

Quelle affirmation est fausse concernant l'inspection de contenu SSL de type "Man-in-the-middle" ?

☐ Le FortiGate établit un tunnel SSL avec le poste client et un autre tunnel SSL avec le serveur web.

☐ Le FortiGate remplace la signature par sa signature dans tous les certificats provenant des serveurs web.

☐ Le FortiGate doit disposer d'un certificat permettant d'émettre des certificats.

☐ Le certificat local du FortiGate (Fortinet\_CA\_SSL) utilisé par défaut pour l'inspection SSL est un certificat auto-signé

Dans une configuration d'authentification "Agentless polling mode", où doit se trouver l'agent collecteur ?

☐ Dans n'importe quel serveur Windows

☐ Il n'y a pas d'agent collecteur, le FortiGate interroge les contrôleurs de domaine AD.

☐ Dans le contrôleur de domaine AD maître

☐ Dans l'un des contrôleurs de domaine AD

Quelle affirmation n'est pas correcte concernant le mode tunnel VPN SSL ?

☐ Le FortiGate attribuera dynamiquement une adresse IP à l'adaptateur réseau SSL VPN coté client.

☐ Le trafic IP dans le tunnel VPN SSL est chiffré.

☐ Un nombre limité d'applications IP sont prises en charge (par exemple : HTTP, FTP, SMB/CIFS)

☐ Le client VPN SSL FortiClient peut être utilisé pour établir un VPN SSL en mode tunnel.

Dans le message Syslog suivant, à quoi correspond terme « LINEPROTO »

```
*Mar 5 16 :447 :34.452 UTC : %LINEPROTO-5-UPDOWN : Line protocol on  
Interface FastEthernet changed state to up
```

☐ La destination syslog

☐ L'horodatage du message syslog

☐ La gravité Syslog

☐ La capacité Syslog

☐ Le numéro de séquence du message syslog

Quel mode d'inspection antivirus n'est pas dans un Fortigate ?

- ☐ Monitor scan flow-based
- ☐ Proxy-based
- ☐ Full scan flow-based
- ☐ Quick scan flow-based

Quelle affirmation concernant IPS est fausse ?

- ☐ La configuration la plus performante pour bloquer les attaques consiste à utiliser l'IPS derrière une interface en mode One-arm sniffer.
- ☐ L'IPS peut bloquer une tentative d'intrusion alors qu'un IDS ne peut pas.
- ☐ L'IPS peut détecter des attaques de type "zero-day".
- ☐ Le moteur IPS est utilisé par l'IPS mais aussi par d'autres fonctions de sécurité du Fortigate.

Quelle affirmation est fausse concernant l'authentification NTLM ?

- ☐ Elle doit être prise en charge (supportée) par les contrôleurs de domaine.
- ☐ Elle permet l'authentification lorsque la communication avec l'agent DC ne fonctionne plus.
- ☐ Elle doit être prise en charge par le navigateur de l'utilisateur.
- ☐ La négociation NTLM s'effectue entre le FortiGate et le navigateur de l'utilisateur.

Quelle méthode réduit le risque d'attaque par inondation d'adresses MAC (MAC flooding) ?

- ☐ Augmenter la vitesse des ports du commutateur.
- ☐ Désactiver la fonction Dynamic Trunking Protocol (DTP).
- ☐ Utiliser une liste de contrôle d'accès (ACL) pour filtrer le trafic de diffusion.
- ☐ Filtrer les VLAN sur les liens trunk.
- ☐ Configurer la sécurité des ports (port-security).
- ☐ Augmenter la taille de la table de commutation.

Sur lequel des types de trafic réseau suivant le moteur antivirus d'un FortiGate ne peut-il pas rechercher des virus ?

O POP3

O SMTP

O **SNMP**

O FTP

Vous êtes chargé de concevoir un nouveau déploiement IPsec en respectant les critères ci-dessous : quelle topologie doit être utilisée pour satisfaire à toutes les exigences ?

- Il y a deux sites centraux auxquels toutes agences doivent se connecter.
- Les agences n'ont pas besoin de communiquer directement les unes avec les autres.
- Aucun routage dynamique ne sera utilisé.
- La conception doit minimiser le nombre de tunnels à devoir configurer.

O Topologie en bus

O Topologie Hub-and-spoke

O **Topologie à maillage partiel**

O Topologie à maillage complet

O Topologie Hub-only

Un administrateur a activé l'analyse antivirus en mode proxy et a configuré les paramètres ci-dessous. Quelle affirmation concernant la configuration est vraie ?

```
Config firewall profile-protocol-options
Edit default
  Config http
    Set oversized-limit 10
    Set options oversize
  End
End
```

O Le FortiGate n'analyse que les 10 premiers Mo d'un fichier.

O Les fichiers de plus de 10 Mo sont envoyés au moteur heuristique pour être analysés.

O **Les fichiers de plus de 10 Mo ne seront pas analysés par l'antivirus et seront bloqués.**

O FortiGate scanne les fichiers par morceaux de 10 MO.

Quelle fonctionnalité UTM envoie une requête UDP aux serveurs FortiGuard chaque fois que FortiGate analyse un paquet (sauf si la réponse est mise en cache localement) ?

O VDOM root

O Antivirus

O IPS

O Contrôle d'application

O Filtrage Web

Parmi les éléments proposés, lequel peut avoir une valeur variable mais néanmoins, Netflow considérera que le trafic appartient au même flux ?

O Le numéro du port de destination

O adresse IP source

O Le de protocole de couche application

O Le marquage TOS (Type Of Service)

Quels agents FSSO sont nécessaires pour implémenter une solution FSSO "Agent based polling mode" ?

O Agents collecteur uniquement (collector agent)

O Agents interrogateur uniquement (polling agent)

O Agents collecteur et agents DC

O Agents DC uniquement (Domain Controller agent)

O Agents interrogateur et agent DC

Quel est l'objectif de la fonction Accounting dans le sigle AAA ?

O Fournir des questions de défi et de réponse

O Demander aux utilisateurs de prouver leur identité

O Déterminer les ressources auxquelles un utilisateur peut accéder

☐ Garder la trace des actions d'un utilisateur

Quelle affirmation est correcte en ce qui concerne l'utilisation du VPN SSL en mode "web-only" ?

☐ Le mode « Web only supporte un nombre limité de protocoles tels que HTTP, FTP, SMB/CIFS, SSH.

☐ Le mode Web only » ne prend en charge que la version 3 du SSL.

☐ Le mode « Web only nécessite un plug-in fourni par Fortinet sur le client web.

☐ L'environnement d'exécution JAVA doit être installé sur le client.

Laquelle des affirmations suivantes est correcte concernant le filtrage des URL sur un FortiGate ?

☐ Dès qu'il y a une correspondance avec un filtre de contournement (filter override), l'action de blocage de la règle de filtrage est remplacée par une action d'autorisation pendant le laps de temps configuré.

☐ Un FortiGate peut filtrer les URL sur la base de motifs (patterns) utilisant du texte et des expressions régulières.

☐ Les deux seules actions disponibles pour le filtrage d'URL sont : Autoriser et Bloquer.

☐ Le mode NGFW permet d'utiliser le filtrage Web par catégories sans devoir contacter les services Fortiguard.

Un administrateur a créé une signature IPS personnalisée. Où la signature IPS personnalisée doit-elle être appliquée ?

☐ Dans un profil de contrôle d'application.

☐ Dans une interface.

☐ Dans une règle DOS.

☐ Dans une sonde IPS.

Un administrateur doit inspecter tout le trafic web (y compris le trafic web sur Internet) provenant des utilisateurs qui se connectent au VPN SSL. Comment cela peut-il être réalisé ?

☐ Utiliser le -web-only

☐ Désactiver le split tunneling

☐ Configurer des signets web (Bookmarks)

☐ Attribuer des adresses IP publiques aux clients VPN SSL

Une société remplace un de ses pare-feu par un FortiGate. Celui-ci doit être capable d'appliquer la redirection de port à leurs serveurs web du back-end tout en bloquant les téléchargements de virus et les inondations TCP SYN des attaquants (SYN flood). Quel mode de fonctionnement est le meilleur choix pour répondre à ces exigences ?

☐ NAT/ Route

☐ NAT/ route avec une interface en One-arm-sniffer

☐ Ce n'est pas possible, un Fortigate ne peut pas effectuer de redirection de ports.

☐ Mode transparent

Quelle pratique permet de réduire les risques d'une attaque par saut de VLAN ?

☐ Le VLAN natif et le VLAN de gestion doivent avoir le même numéro de VLAN.

☐ Configurer les trunks sur tous les ports connectés aux périphériques des utilisateurs de manière statique (switchport mode trunk).

☐ Utiliser SSH pour tous les accès à distance.

☐ Remplacer le VLAN de gestion par un VLAN distinct qui n'est pas accessible aux utilisateurs classiques.

☐ Remplacer le VLAN natif par défaut (VLAN 1) par un VLAN distinct de tous les autres VLAN.

Quel mode de déploiement du SSO n'est pas possible avec Windows AD?

☐ Polling mode

☐ Terminal Server agent mode

☐ Domain Controller agent mode

☐ eDirectory agent mode

Dans une solution FSSO avec agent, comment l'agent collecteur FSSO apprend-il chaque adresse IP ?

☐ L'agent collecteur interroge fréquemment les contrôleurs de domaine AD pour obtenir l'adresse IP de chaque utilisateur.

☐ L'agent DC apprend le nom de la station de travail à partir des journaux d'événements et le DNS est ensuite utilisé pour traduire ces noms en adresses IP.

☐ L'agent collecteur ne connaît pas, et n'a pas besoin de connaître, l'adresse IP de chaque utilisateur. Seuls les noms des postes de travail sont connus de l'agent collecteur,

☐ Les agents DC obtiennent chaque adresse IP d'utilisateur à partir des journaux d'événements et transmettent ces informations à l'agent collecteur.

Quelle fonction de surveillance du réseau est fournie par l'utilisation de SPAN ?

- ☐ Les rapports en temps réel et l'analyse à long terme des événements de sécurité sont activés.
- ☐ Les analystes réseau sont en mesure d'accéder aux fichiers journaux des périphériques réseau et de surveiller le comportement du réseau.
- ☐ SPAN permet de corréler les statistiques sur les paquets circulant dans les routeurs et les commutateurs multicouches afin d'en déduire la présence de trafic anormal.
- ☒ Le trafic sortant et entrant dans un commutateur est copié vers un dispositif de surveillance du réseau.

Quelle proposition n'est pas une technique pouvant être utilisée pour essayer d'empêcher un logiciel antivirus d'identifier un Virus par sa signature ?

- ☐ La compression
- ☐ L'ajout de code mort
- ☐ Le chiffrement
- ☒ La forensique

Une interface d'un commutateur est configurée avec l'option PortFast. Quelle protection permet d'empêcher des problèmes au niveau STP si un autre commutateur était branché sur cette interface ?

- ☐ LLDP
- ☒ BPDU Guard
- ☐ Protector
- ☐ EEE BPDU
- ☐ Watchdog
- ☐ STP Checker

Quel type d'attaque implique de mentir sur l'adresse source d'une trame ou d'un paquet ?

- ☐ Snooping
- ☒ Spoofing
- ☐ Flooding
- ☐ Starvation
- ☐ Sweep scan
- ☐ Denial Of service

Quelle est l'étape nécessaire pour qu'un client VPN SSL puisse accéder à un serveur interne en utilisant le mode « port forward » ?

- ☐ Configurer l'application cliente pour qu'elle transfère le trafic IP vers l'applet Java préalablement installée.
- ☐ Configurer les applications qu'elles utilisent des ports TCP dynamiques.
- ☐ Installer le client VPN SSL FortiClient.
- ☒ Créer un domaine (Realm) VPN SSL réservé aux clients utilisant le mode « port forward »

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

- ☒ Le navigateur doit avoir installé le certificat de l'autorité de certification qui a signé le certificat du serveur web.
- ☐ La clé publique du certificat du serveur web doit être installée dans le navigateur.
- ☐ Le navigateur doit avoir la clé privée du certificat de la CA qui a signé le certificat du navigateur web.
- ☐ Le certificat du serveur web doit être installé dans le navigateur.

Quelle affirmation sur les profils de filtrage DNS est vraie ?

- ☐ Ils permettent de filtrer plus précisément que le filtrage HTTP.
- ☐ Ils peuvent aussi inspecter le trafic HTTPS.
- ☒ Ils peuvent bloquer les requêtes DNS vers des serveurs de commande et de contrôle de botnets connus.
- ☐ Ils peuvent inspecter le trafic HTTP.
- ☐ Ils doivent toujours être appliqués dans les politiques de pare-feu avec l'inspection SSL activée.

Un administrateur a configuré un FortiGate de sorte que les utilisateurs finaux doivent s'authentifier auprès du pare-feu à l'aide de certificats numériques avant de naviguer sur Internet. Les utilisateurs possèdent leur certificat numérique délivré par une CA. Quelle condition doit également être respectée pour que l'authentification soit réussie ?

- ☒ Le Fortigate devra de la clé privée qui a signé les certificats numériques des clients.
- ☐ Les utilisateurs devront fournir un nom d'utilisateur et un mot de passe valides.
- ☐ Le FortiGate devra envoyer un token (un jeton) aux utilisateurs afin de valider leur certificat.
- ☐ Les utilisateurs doivent appartenir à un d'utilisateurs de pare-feu (Firewall user group).



Quelle affirmation est correcte concernant la recherche de virus sur un FortiGate ?

- ☐ La recherche de virus est activée par défaut.
- ☐ L'activation du scan de virus dans un profil de sécurité permet la protection contre les virus pour tout le trafic passant par le FortiGate.
- ☒ Le scan de virus doit être activé dans un profil de sécurité, qui doit être appliqué à une règle de pare-feu.
- ☐ Le support client Fortinet permet de scanner les virus à distance pour vous.

Quel type de trafic et d'attaque ne peut pas être bloqué par un profil de pare-feu d'application web (WAF) ?

- ☐ Attaques par injection SQL
- ☐ Attaques via des scripts de site à site (XSS)
- ☒ Trafic vers les serveurs de botnets
- ☐ Fuites de données relatives aux cartes de crédit de la société

Quelle affirmation décrit le mieux le mécanisme d'inondation TCP SYN (SYN flood) ?

- ☒ L'attaquant envoie de nombreuses demandes de connexions TCP mais ne les finalisent pas.
- ☐ L'attaquant maintient ouvertes de nombreuses connexions avec une transmission de données cliente, de sorte que les autres clients ne peuvent pas démarrer de nouvelles connexions.
- ☐ L'attaquant envoie un paquet malformé spécialement conçu la synchronisation des sessions de la cible.
- ☐ L'attaquant envoie un paquet spécialement conçu pour se synchroniser avec le FortiGate.

Quel est le nom donné à une alerte générée par un agent SNMP ?

- ☒ Trap
- ☐ Syslog message
- ☐ SNMP POST
- ☐ SNMP GET
- ☐ Capture

258.

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

A. Une route statique doit être configurée par l'administrateur en utilisant l'interface racine sei. comme interface sortante.

sortante.

**B. 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.**

C. Une route de retour vers le pool IP SSLVPN est automatiquement créée sur l'unité FortiGate.

D. L'unité FortiGate ajoute une route basée sur l'adresse de destination dans la politique de pare-feu SSL VPN.

259. Lorsque le proxy SSL n'effectue PAS d'interception man-in-the-middle du trafic SSL, quel champ de certificat peut être utilisé pour déterminer le classement d'un site Web ?

A. Unité organisationnelle.

**B. Nom commun.**

C. Numéro de série.

D. Validité.

260.

A. Il prend en charge SSL version 3 uniquement.

En ce qui concerne l'utilisation du VPN SSL en mode Web-only, quelle affirmation est correcte ?

B. Il nécessite un plug-in fourni par Fortinet sur le client Web.

**C. L'utilisateur doit disposer d'un navigateur Web qui prend en charge la longueur de chiffrement de 64 bits.**

D. L'environnement d'exécution JAVA doit être installé sur le client.

261. Lesquels des énoncés suivants sont vrais au sujet de l'inspection du contenu SSL Man-in-the-middle ? (Choisissez-en trois.)

A. Le dispositif FortiGate " re-signe " tous les certificats provenant des serveurs HTTPS.

**B. Le dispositif FortiGate fait office de sous-CA.**

**C. Le certificat de service local du serveur Web doit être installé dans le dispositif FortiGate.**

D. Le dispositif FortiGate effectue une inspection man-in-the-middle.

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

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

**A. Une route vers un sous-réseau de destination correspondant à l'objet d'adresse Internal\_Servers.**

B. Une route vers le sous-réseau de destination configuré dans le widget du mode tunnel.

C. Un itinéraire par défaut.

D. Un itinéraire vers le sous-réseau de destination configuré dans les paramètres globaux du VPN SSL.

263. Lesquels des agents FSSO suivants sont nécessaires pour une solution en mode agent DC ? (Choisissez-en 2)

- A. Agent FSSO
- B. Agent DC**
- C. Agent collecteur**
- D. Serveur Radius

264. Quelle est l'étape requise par un VPN SSL pour accéder à un serveur interne en utilisant le mode de transfert de port ?  
mode forward ?

- A. Configurer les adresses IP virtuelles à attribuer aux utilisateurs du VPN SSL.
- B. Installer le client VPN SSL FortiClient
- C. Créer un royaume VPN SSL réservé aux clients utilisant le mode de transfert de port.
- D. Configurer l'application client pour transférer le trafic IP vers un proxy d'applets Java.**

265. Une entreprise doit fournir un accès VPN SSL à deux groupes d'utilisateurs. L'entreprise doit également afficher des messages de bienvenue différents sur l'écran de connexion VPN SSL pour les deux groupes d'utilisateurs. Qu'est-ce qui est nécessaire dans la configuration VPN SSL pour répondre à ces exigences ?

- A. Deux VPN SSL séparés dans des interfaces différentes du même VDOM.
- B. Des royaumes VPN SSL différents pour chaque groupe**
- C. Des adresses IP SSL VPN virtuelles différentes pour chaque groupe
- D. Deux politiques de pare-feu avec des portails captifs différents

266.

Lorsqu'un utilisateur tente de se connecter à un site HTTPS, quel est le résultat attendu avec cette configuration ? R. L'utilisateur doit s'authentifier avant d'accéder à des sites dont les certificats SSL ne sont pas fiables.  
non fiables.

- B. L'utilisateur reçoit des avertissements relatifs aux certificats lorsqu'il se connecte à des sites dont les certificats SSL ne sont pas fiables.**
- C. L'utilisateur est autorisé à accéder à tous les sites dotés de certificats SSL non fiables, sans avertissement de certificat. fourni).
- D. L'utilisateur est empêché de se connecter aux sites qui ont des certificats SSL non fiables (sans exception).

267. Un administrateur doit inspecter l'ensemble du trafic web (y compris le trafic web Internet)  
provenant d'utilisateurs se connectant à un VPN SSL. Comment cela peut-il être réalisé ?

- A. En désactivant le tunnelage fractionné**
- B. Configurer les signets Web
- C. Attribution d'adresses IP publiques aux clients VPN SSL
- D. Utiliser le mode Web uniquement

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

- A. Le navigateur doit avoir installé le certificat de l'autorité de certification qui a signé le certificat du serveur Web.
- B. Le navigateur doit avoir installé le certificat du serveur Web.
- C. La clé privée du certificat de l'autorité de certification qui a signé le certificat du navigateur Web doit être installée sur le navigateur.
- D. La clé publique du certificat du serveur Web doit être installée sur le navigateur.

269. Lors de la navigation 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 ?

- A. L'adresse IP publique de l'unité FortiGate
- B. L'adresse IP interne de l'unité FortiGate
- C. L'adresse IP virtuelle de l'utilisateur distant
- D. L'adresse IP publique de l'utilisateur distant

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

- A. Le nom de l'adaptateur réseau virtuel requis dans le PC de chaque utilisateur pour le mode Tunnel VPN SSL.
- B. Le nom d'une interface virtuelle dans le VDOM racine d'où provient tout le trafic utilisateur VPN SSL.
- C. Un objet Adresse du pare-feu qui contient les adresses IP attribuées aux utilisateurs VPN SSL.
- D. L'interface virtuelle du VDOM racine à laquelle les tunnels VPN SSL distants se connectent.

271.

Un FortiGate est configuré avec l'adresse 1.1.1.1/24 sur l'interface wan2 et l'accès administratif HTTPS est activé pour l'interface.

L'accès administratif HTTPS, utilisant le port tep par défaut, est activé pour cette interface. Compte tenu des paramètres VPN SSL de la pièce à conviction. Lesquelles des URLs de portail de connexion VPN SSL suivantes sont valides ? (Choisissez-en deux.)

- A. http://1.1.1.1:443/Training
- B. https://1.1.1.1:443/STUDENTS
- C. https://1.1.1.1/login
- D. https://1.1.1.1/

272. Lesquelles des affirmations suivantes sont correctes concernant le mode Web-only du VPN SSL ? (Choisissez-en deux.)

- A. Il ne peut être utilisé que pour se connecter à des services Web.
- B. Le trafic IP est encapsulé sur HTTPS.
- C. L'accès aux ressources du réseau interne est possible à partir du portail VPN SSL.
- D. Le client VPN SSL autonome FortiClient NE PEUT PAS être utilisé pour établir un VPN SSL uniquement sur le Web.
- E. Il n'est pas possible de se connecter à des serveurs SSH via le VPN.

273. Laquelle des méthodes d'authentification suivantes peut être utilisée pour l'authentification VPN SSL ? (Choisissez-en trois.)

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

B. Authentification à deux facteurs

C. Authentification par mot de passe local

D. FSSO

E. RSSO

274. Quelle affirmation décrit le mieux ce que fait la vérification d'intégrité du client VPN SSL ?

A. Bloque les tentatives de connexion VPN SSL des utilisateurs qui ont été mis sur liste noire.

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

C. Valide l'identifiant de l'utilisateur VPN SSL.

D. Vérifie quel portail VPN SSL doit être présenté à chaque utilisateur VPN SSL.

E. Vérifie que le dernier client VPN SSL est installé sur le PC du client.

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

A. Le trafic IP est encapsulé sur HTTPS.

B. Le client VPN SSL autonome FortiClient peut être utilisé pour établir un VPN SSL en mode Tunnel.

C. Un nombre limité d'applications IP est pris en charge.

D. Le dispositif FortiGate attribue dynamiquement une adresse IP à la carte réseau VPN SSL.

276. Lesquels des énoncés suivants décrivent certaines des différences entre la cryptographie symétrique et asymétrique ? (Choisissez-en deux.)  
doit être gardé secret.

A. Dans la cryptographie symétrique, les clés sont accessibles au public. Dans la cryptographie asymétrique, les clés sont accessibles au public.

B. La cryptographie asymétrique permet de chiffrer les données plus rapidement que la cryptographie symétrique.

C. La cryptographie symétrique utilise une clé pré-partagée. La cryptographie asymétrique utilise une paire de clés.

D. Les clés asymétriques peuvent être envoyées à l'homologue distant via des certificats numériques. Les clés symétriques ne peuvent pas

277. Parmi les affirmations suivantes, laquelle décrit le mieux ce qu'est une autorité de publique (CA) ?

A. Un service qui fournit un certificat numérique à chaque fois qu'un utilisateur s'authentifie

B. Une entité qui certifie que les informations contenues dans un certificat numérique sont valides et vraies.

C. Le processus FortiGate chargé de générer des certificats numériques à la volée à des fins d'inspection SSL.

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

278. Lesquels des énoncés suivants sont vrais à propos du certificat SSL Proxy ?

A. Il ne peut pas être signé par une AC privée doit être utilisé pour l'inspection du contenu SSL ? (Choisissez-en deux.)

B. Il doit avoir soit le champ "CA=True", soit le champ "Key Usage=KeyCertSign".

C. Il doit être installé dans le dispositif FortiGate.

D. L'objet déposé doit contenir soit le FQDN, soit l'adresse IP du dispositif FortiGate.

279. Lesquels des énoncés suivants sont vrais au sujet des utilisateurs d'ICP créés dans un dispositif FortiGate ? (Choisissez-en deux.)

A. Ils peuvent être utilisés pour l'authentification par jeton

B. Peut être utilisé pour l'authentification à deux facteurs

C. Sont utilisés pour l'authentification par certificat

D. Ne peuvent pas être membres de groupes d'utilisateurs

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

de signature de certificat (CSR) ?

A. Un message envoyé par l'autorité de certification (CA) qui contient un certificat numérique signé.

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

C. Une demande soumise à une autorité de certification (CA) pour demander un certificat numérique signé.

D. Une demande soumise à une autorité de certification (CA) pour demander une liste de révocation de certificat (CRL).

281. Laquelle des actions suivantes peut être utilisée pour sauvegarder les clés et les certificats numériques d'un dispositif FortiGate ? (Choisissez-en deux.)

A. Effectuer une sauvegarde complète de la configuration de FortiGate.

B. Téléchargement d'un fichier PKCS#10 sur un lecteur USB

C. Téléchargement manuel des informations de certificat vers une autorité de certification (CA)

D. Télécharger un fichier PCS#12 vers un serveur TFTP

282. Lequel des énoncés suivants doit être vrai pour qu'un certificat numérique soit valide ? (Choisissez-en deux.)

A. Il doit être signé par une autorité de certification " fiable ".

B. Il doit être répertorié comme valide dans une liste de révocation de certificats (CRL).

C. Le champ CA doit être "TRUE".

D. Il doit être encore dans sa période de validité

283. Quelle est l'affirmation vraie concernant les temporisateurs VPN SSL ? (Choisissez-en deux.)

- A. Permettent d'atténuer les attaques DoS provenant de requêtes HTTP partielles.
- B. Les paramètres VPN SSL ne comportent pas de temporisateurs personnalisables.
- C. Déconnecter les utilisateurs VPN SSL inactifs lorsqu'un délai d'authentification de la politique de pare-feu se produit.
- D. Empêcher les utilisateurs VPN SSL d'être déconnectés en raison d'une forte latence du réseau.

284. Laquelle des conditions suivantes doit être remplie pour qu'un navigateur Web fasse confiance à un certificat de serveur Web signé par une AC tierce ?

- A. La clé publique du certificat de serveur Web doit être installée sur le navigateur.
- B. Le certificat du serveur Web doit être installé sur le navigateur.
- C. Le certificat de l'autorité de certification qui a signé le certificat du serveur Web doit être installé sur le navigateur.
- D. La clé privée du certificat de l'autorité de certification qui a signé le certificat du navigateur doit être installée sur le navigateur.

285. L'épinglage de la clé publique HTTP (HPKP) peut constituer un obstacle à la mise en œuvre d'une inspection complète de la sst complète. Quelles solutions pourraient résoudre ce problème ? (Choisissez-en deux.)

- A. Activer l'option Autoriser les certificats SSL non valides pour le profil de sécurité concerné.
- B. Modifier les navigateurs Web pour en choisir un qui ne prend pas en charge HPKP.
- C. Exempter les sites Web qui utilisent HPKP de l'inspection SSL complète.
- D. Installer le certificat de l'autorité de certification (requis pour vérifier le certificat du serveur Web) dans les magasins des utilisateurs.

286. Lequel des énoncés suivants est vrai concernant les paramètres SSL VPN pour un portail portail VPN SSL ?

- A. Par défaut, FortiGate utilise des serveurs WINS pour résoudre les noms.
- B. Par défaut, le portail VPN SSL nécessite l'installation du certificat d'un client.
- C. Par défaut, le tunnelage fractionné est activé.
- D. Par défaut, l'interface graphique d'administration et le portail VPN SSL utilisent le même port HTTPS.

287. Quelle est la description correcte d'un résultat de hachage en ce qui concerne les certificats numériques ?

- A. Une valeur unique utilisée pour vérifier les données d'entrée
- B. Une valeur de sortie qui est utilisée pour identifier la personne ou déduire qui a rédigé les données d'entrée.
- C. Une obfuscation utilisée pour masquer les données d'entrée.
- D. Une valeur de sortie chiffrée utilisée pour protéger les données d'entrée.

288. Un administrateur doit créer une connexion SSL-VPN pour accéder à un serveur interne en utilisant le signet Port Forward. Quelle étape est nécessaire pour cette configuration ?

- A. Configurer un royaume VPN SSL pour que les clients utilisent le signet Port Forward.
- B. Configurer l'application client pour transférer le trafic IP via FortiClient.
- C. Configurez l'adresse IP virtuelle à attribuer aux utilisateurs VPN SSL.
- D. Configurez l'application client pour qu'elle transfère le trafic IP vers un proxy d'applets Java.

289. Quels utilisateurs et groupes d'utilisateurs sont autorisés à accéder au réseau via le portail captif ?

- A. Seuls les utilisateurs individuels, et non les groupes, définis dans la configuration du portail captif.
- B. Les groupes définis dans la configuration du portail captif
- C. Tous les utilisateurs
- D. Utilisateurs et groupes définis dans la politique de pare-feu

290. Quelles sont les deux affirmations vraies concernant les VPN IPsec et les VPN SSL ? (Choisissez-en deux.)

- A. Le VPN SSL crée une connexion HTTPS. IPsec ne le fait pas.
- B. Les VPN SSL et les VPN IPsec sont tous deux des protocoles standard.
- C. Un VPN SSL ou un VPN IPsec peut être établi entre deux dispositifs FortiGate.
- D. Un VPN SSL ou un VPN IPsec peut être établi entre une station de travail d'utilisateur final et un dispositif FortiGate.

291. Concernant le VPN SSL en mode tunnel, quelles sont les trois affirmations correctes ? (Choisissez-en trois.)

- A. Le tunnelage fractionné est pris en charge
- B. Il nécessite l'installation d'un client VPN.
- C. Il nécessite l'utilisation d'un navigateur Internet.
- D. Il ne prend pas en charge le trafic provenant d'applications réseau tierces.
- E. Une adresse IP VPN SSL est attribuée dynamiquement au client par l'unité FortiGate.

292. Quelles tâches relèvent de la responsabilité du proxy SSL dans une connexion HTTPS typique ? (Choisissez-en deux.)

- A. La poignée de main SSL du client Web.
- B. La poignée de main SSL du serveur Web.
- C. La mise en mémoire tampon des fichiers.
- D. La communication avec le processus de filtrage des URL.

293. Un client peut créer une connexion sécurisée à un dispositif FortiGate en utilisant le VPN SSL en mode web uniquement. Lequel des énoncés suivants est correct concernant l'utilisation du VPN SSL en mode Web-only ?

- A. Le mode Web-only prend en charge SSL version 3 uniquement.
- B. Un plug-in fourni par Fortinet est nécessaire sur le client Web pour utiliser le mode SSL VPN Web-only.
- C. Le mode Web-only nécessite que l'utilisateur dispose d'un navigateur Web qui prend en charge la longueur de chiffrement de 64 bits.



D. L'environnement d'exécution JAVA doit être installé sur le client pour pouvoir se connecter à un VPN SSL en mode Web uniquement.

294. Un client peut établir une connexion sécurisée à un réseau d'entreprise en utilisant le VPN SSL en mode tunnel. Lesquelles des affirmations suivantes sont correctes concernant l'utilisation du VPN SSL en mode tunnel ? (Sélectionnez toutes les réponses applicables.)

A. La tunnelisation fractionnée peut être activée lors de l'utilisation du VPN SSL en mode tunnel.

B. Un logiciel client est nécessaire pour pouvoir utiliser un VPN SSL en mode tunnel.

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

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

295. Un problème pourrait potentiellement se produire lorsque l'on clique sur Connecter pour démarrer le mode tunnel

VPN SSL. Le tunnel démarre pendant quelques secondes, puis s'arrête. Lequel des énoncés suivants décrit le mieux la façon de résoudre ce problème ?

A. Cet utilisateur n'a pas la permission d'activer le mode tunnel.

Assurez-vous que le widget du mode tunnel a été ajouté au portail Web de cet utilisateur.

B. Cette unité FortiGate peut disposer de plusieurs connexions Internet.

Pour éviter ce problème, utilisez la commande CLI appropriée pour lier la connexion VPN SSL à l'interface entrante d'origine.

C. Vérifiez l'adaptateur SSL sur la machine hôte.

Si nécessaire, désinstallez et réinstallez l'adaptateur à partir du portail en mode tunnel.

D. Assurez-vous que seul Internet Explorer est utilisé. Tous les autres navigateurs ne sont pas pris en charge.

296. Une unité FortiGate peut créer une connexion sécurisée à un client utilisant SSL VPN en mode tunnel. Lesquelles des affirmations suivantes sont correctes concernant l'utilisation du VPN SSL en mode tunnel ? (Sélectionnez toutes les réponses applicables.)

A. La tunnelisation fractionnée peut être activée lors de l'utilisation du mode tunnel SSL VPN.

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

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

D. Le VPN SSL en mode tunnel nécessite que le logiciel FortiClient soit installé sur l'ordinateur de l'utilisateur.

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

297. L'utilisateur final de l'air se connecte au portail VPN SSL et sélectionne l'option Mode Tunnel

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

- A. photo
- B. photo
- C. photo
- D. photo

298. L'inspection du contenu SSL est activée sur l'unité FortiGate. Laquelle des étapes suivantes est nécessaire pour empêcher un utilisateur de recevoir un avertissement du navigateur Web lorsqu'il accède à un site Web crypté par SSL ?  
le poste de travail de l'utilisateur.

- A. Le certificat racine du proxy SSL de FortiGate doit être importé dans le magasin de certificats local sur le poste de travail de l'utilisateur.
- B. Désactivez la vérification stricte du certificat de serveur dans le navigateur Web sous Options Internet.
- C. Activez le mode proxy transparent sur l'unité FortiGate.
- D. Activez l'authentification NTLM sur l'unité FortiGate. L'authentification NTL\_M supprime les messages d'avertissement du certificat dans le navigateur Web.

299. Systeri Examinez l'illustration ci-dessous et répondez à la question qui suit. Dans les options UTM Proxy, le certificat CA Fortinet\_CA\_SSLProxy définit lequel des éléments suivants :

- A. Le certificat de cryptage de l'unité FortiGate utilisé par le proxy SSL.
- B. Le certificat de signature de l'unité FortiGate utilisé par le proxy SSL.
- C. Le certificat de signature de FortiGuard utilisé par le proxy SSL.
- D. Le certificat de cryptage de FortiGuard utilisé par le proxy SSL.

300. Lesquels des énoncés suivants sont corrects en ce qui concerne la configuration d'une unité FortiGate en tant que passerelle VPN SSL ? (Sélectionnez tous ceux qui s'appliquent.)

- A. Le mode tunnel ne peut être utilisé que si les groupes d'utilisateurs VPN SSL ont au moins une option de contrôle des hôtes activée.
- B. Les routes spécifiques nécessaires pour accéder aux ressources internes via une connexion VPN SSL en mode tunnel à partir de l'ordinateur client sont définies dans le widget de routage associé au portail VPN SSL.
- C. Pour appliquer un portail à un utilisateur, ce dernier doit appartenir à un groupe d'utilisateurs VPN SSL.
- D. Les paramètres du portail spécifient si la connexion fonctionnera en mode Web uniquement ou en mode tunnel.

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

- A. Nom commun
- B. Organisation
- C. Unité organisationnelle
- D. Numéro de série
- E. Validité

302. Dans le widget Tunnel Mode du portail Web, l'administrateur a configuré un pool IP et a activé le tunnelage fractionné.

Lequel des énoncés suivants est vrai concernant l'adresse IP utilisée par le client VPN SSL ?

- A. Le pool IP spécifié dans les options du widget Mode tunnel SSL-VPN remplacera la plage d'adresses IP définie dans les paramètres SSL-VPN.
- B. Le tunnelage fractionné étant activé, aucune adresse IP ne doit être attribuée pour que le tunnel VPN SSL soit établi.
- C. La plage d'adresses IP spécifiée dans les Paramètres SSL-VPN remplacera la plage d'adresses IP dans les Options du Widget Mode Tunnel SSL-VPN.

303. La fonction de vérification de l'hôte peut être activée sur l'unité FortiGate pour les connexions VPN SSL. Lorsque cette fonction est activée, l'unité FortiGate sonde l'ordinateur hôte distant pour vérifier qu'il est "sûr" avant d'accorder l'accès.

Lequel des éléments suivants n'est PAS une option de la fonction de vérification de l'hôte ?

- A. Le logiciel antivirus FortiClient
- B. Le logiciel de pare-feu Microsoft Windows
- C. Le logiciel de pare-feu FortiClient
- D. Logiciel antivirus tiers

304. Qu'est-ce qui est nécessaire dans une configuration FortiGate pour avoir plusieurs VPN VPN IPsec utilisant le mode agressif ?

- A. Tous les VPN dialup en mode agressif DOIVENT accepter les connexions provenant du même ID de pair.
- B. Chaque ID d'homologue DOIT correspondre au FQDN de chaque homologue distant.
- C. Chaque VPN commuté en mode agressif DOIT accepter les connexions provenant d'ID d'homologues différents.
- D. Le paramètre peer ID ne doit PAS être utilisé.

305. Un utilisateur final se connecte au portail VPN SSL à accès complet et sélectionne l'option Tunnel Mode en cliquant sur le bouton "Connect". L'administrateur a activé le tunnelage fractionné.

Étant donné que l'utilisateur s'authentifie par rapport à la politique VPN SSL présentée dans l'image ci-dessous, quelle affirmation ci-dessous identifie la route qui est ajoutée à la table de routage du client.

- A. Une route vers la destination correspondant à l'objet adresse 'WIN2K3'.
- B. Une route vers la destination correspondant à l'objet d'adresse 'all'.
- C. Une route par défaut.
- D. Aucune route n'est ajoutée.

306. Avec le mode agent DC de FSSO, un utilisateur de domaine peut s'authentifier soit auprès du contrôleur de domaine exécutant l'agent collecteur et l'agent contrôleur de domaine, soit auprès d'un contrôleur de domaine exécutant uniquement l'agent contrôleur de domaine. Si vous tentez de vous authentifier auprès d'un contrôleur de domaine exécutant uniquement l'agent de contrôleur de domaine, quelles sont les affirmations correctes ? (Choisissez-en deux.)

- A. L'événement de connexion est envoyé à un agent collecteur par l'agent DC.
- B. L'événement de connexion est envoyé à la FortiGate par l'agent DC.
- C. L'agent collecteur de domaine peut effectuer une recherche DNS pour l'adresse IP du client authentifié.
- D. L'utilisateur ne peut pas être authentifié auprès du FortiGate de cette manière car chaque agent de contrôleur de domaine nécessite un agent collecteur dédié.

307. Quelle affirmation décrit l'utilité de la commande CLI `diagnose debug authd fssolist` ?

- A. Surveille les communications entre l'agent collecteur FSSO et l'unité FortiGate.
- B. Affiche les utilisateurs actuellement connectés à l'aide de FSSO.
- C. Affiche la liste de tous les agents collecteurs FSSO connectés.
- D. Affiche la liste de tous les agents DC installés sur tous les contrôleurs de domaine.

308. Quel énoncé décrit le mieux ce qu'est `SSL.root` ?

- A. Le nom de l'adaptateur réseau virtuel requis dans le PC de chaque utilisateur pour le mode Tunnel VPN SSL.
- B. Le nom d'une interface virtuelle dans le VDOM racine d'où provient tout le trafic utilisateur VPN SSL.
- C. Un objet Adresse du pare-feu qui contient les adresses IP attribuées aux utilisateurs VPN SSL.
- D. L'interface virtuelle du VDOM racine à laquelle les tunnels VPN SSL distants se connectent.

309. Un FortiGate est configuré avec l'adresse 1.1.1.1/24 sur l'interface wan2 et l'accès administratif HTTPS.

L'accès administratif HTTPS, utilisant le port supérieur par défaut, est activé pour cette interface. Compte tenu des paramètres VPN SSL de la pièce à conviction. Lesquelles des URLs de portail de connexion VPN SSL suivantes sont valides ? (Choisissez-en deux.)

- A. <http://1.1.1.1:443/Training>
- B. <https://1.1.1.1:443/STUDENTS>
- C. <https://1.1.1.1/login>
- D. <https://1.1.1.1/>

310. Quel énoncé décrit le mieux la fonction de vérification de l'intégrité du client VPN SSL ?

- A. Bloque les tentatives de connexion VPN SSL des utilisateurs figurant sur la liste noire.
- B. [Détection des applications de sécurité du client Windows exécutées sur les PC du client VPN SSL.](#)
- C. Valide l'identifiant de l'utilisateur VPN SSL.
- D. Vérifie quel portail VPN SSL doit être présenté à chaque utilisateur VPN SSL.
- E. Vérifie que le dernier client VPN SSL est installé sur le PC du client.

311. Quels sont les avantages du mode FSSO DC par rapport au mode polling ?

- A. Redondance de l'agent collecteur.
- B. Permet une authentification transparente.
- C. Les agents DC ne sont pas nécessaires dans les contrôleurs de domaine AD.
- D. [Évolutivité](#)

312. Lesquelles des affirmations suivantes sont correctes concernant l'authentification NTLM ?

(Choisissez-en trois)

- A. [La négociation NTLM commence entre le dispositif FortiGate et le navigateur de l'utilisateur.](#)
- B. [Elle doit être prise en charge par le navigateur de l'utilisateur.](#)
- C. [Elle doit être prise en charge par les contrôleurs de domaine.](#)
- D. Elle ne nécessite pas d'agent collecteur.
- E. [Il ne nécessite pas d'agents DC.](#)

313. Lequel des énoncés suivants décrit le mieux comment l'agent collecteur apprend qu'un utilisateur s'est déconnecté du réseau ?

- A. [La station de travail ne répond pas aux sondages fréquemment effectués par l'agent collecteur.](#)
- B. L'agent DC capture l'événement de déconnexion dans les journaux d'événements, qu'il transmet à l'agent collecteur.
- C. Le poste de travail notifie à l'agent DC que l'utilisateur s'est déconnecté.
- D. L'agent collecteur reçoit les événements de déconnexion lorsqu'il interroge le contrôleur de domaine correspondant.

314. Laquelle des affirmations suivantes décrit le mieux le rôle d'un agent DC dans un DC FSSO ?

DC FSSO ?

- A. Capture les événements de connexion et les transmet à l'agent collecteur.
- B. Capture l'adresse IP et le nom du poste de travail de l'utilisateur et transmet ces informations aux dispositifs FortiGate.
- C. Capture les événements de connexion et de déconnexion et les transmet à l'agent collecteur.
- D. Capture les événements de connexion et les transmet aux dispositifs FortiGate.

315. Lequel des modes FSSO suivants doit être utilisé pour les réseaux Novell Directory ?

- A. Polling sans agent
- B. Agent LDAP
- C. Agent d'annuaire
- D. Agent DC

316. Dans une solution FSSO en mode interrogation sans agent, où doit se trouver l'agent collecteur ?

- A. Dans n'importe quel serveur Windows
- B. Dans l'un des contrôleurs de domaine AD
- C. Dans le contrôleur de domaine AD maître
- D. Le dispositif FortiGate interroge les contrôleurs de domaine AD.

317. Lesquels des énoncés suivants sont des caractéristiques d'une solution FSSO utilisant le mode d'accès avancé ? (Choisissez-en trois.)

- A. Les profils de protection peuvent être appliqués à la fois aux utilisateurs individuels et aux groupes d'utilisateurs.
- B. Les groupes imbriqués ou hérités sont pris en charge
- C. Les noms d'utilisateur suivent la convention LDAP : CN=User, OU=Nom, DC=Domaine
- D. Les noms d'utilisateur suivent la convention Windows : Domaine - nom d'utilisateur
- E. Les profils de protection ne peuvent être appliqués qu'à des groupes d'utilisateurs.

318. Lesquels des agents FSSO suivants sont nécessaires pour une solution en mode agent DC ? (Choisissez-en deux.)

- A. Agent FSSO
- B. Agent DC
- C. Agent collecteur
- D. Serveur Radius

319. Dans une solution en mode agent de FSSO, comment l'agent collecteur de FSSO apprend-il chaque adresse IP ?

- A. Les agents DC obtiennent chaque adresse IP d'utilisateur à partir des journaux d'événements et transmettent ces informations à l'agent collecteur.
- B. L'agent collecteur ne connaît pas, et n'a pas besoin de connaître, l'adresse IP de chaque utilisateur. Seuls les noms des postes de travail sont connus de l'agent collecteur.
- C. L'agent collecteur interroge fréquemment les contrôleurs de domaine AD pour obtenir l'adresse IP de chaque utilisateur.
- D. L'agent DC apprend le nom de la station de travail à partir des journaux d'événements et le DNS est ensuite utilisé pour traduire ces noms en adresses IP respectives.

320. Quels agents FSSO sont nécessaires pour une solution de mode d'interrogation basée sur des agents FSSO ?

- A. Agent collecteur et agents DC
- B. Agent d'interrogation uniquement
- C. Agent collecteur uniquement
- D. Agents DC uniquement

321. Quel protocole ne peut pas être utilisé avec le type d'authentification active ?

- A. Local
- B. RADIUS
- C. LDAP
- D. RSSO

322. Lesquels des énoncés suivants concernant l'authentification NTLM sont corrects ? (Choisissez-en deux.)

- A. Elle est utile lorsque les utilisateurs se connectent à des DC qui ne sont pas surveillés par un agent collecteur.
- B. Elle prend la place de la méthode d'authentification principale lorsqu'elle est configurée avec FSSO.
- C. Les environnements multi-domaines nécessitent des agents DC sur chaque contrôleur de domaine.
- D. Les navigateurs Web compatibles avec NTLM sont nécessaires.

323. Comment FortiGate vérifie-t-il les informations d'identification d'un utilisateur LDAP distant ?

- A. FortiGate envoie les informations d'identification saisies par l'utilisateur au serveur LDAP pour authentification.
- B. FortiGate génère à nouveau l'algorithme en fonction des informations d'identification de connexion et le compare à l'algorithme stocké sur le serveur LDAP.
- C. FortiGate interroge sa propre base de données pour obtenir des informations d'identification.
- D. FortiGate recherche les informations d'identification sur le serveur LDAP.

324. Lesquelles des affirmations suivantes concernant le mode d'accès AD avancé pour l'agent collecteur FSSO sont vraies ? (Choisissez-en deux.)

A. Il n'est pris en charge que si des agents DC sont déployés.

B. FortiGate peut agir comme un client LDAP pour configurer les filtres de groupe.

C. Il prend en charge la surveillance des groupes imbriqués.

D. Elle utilise la convention Windows pour l'attribution de noms, c'est-à-dire Domain\Username.

325. Lesquels des énoncés suivants décrivent le mode d'interrogation WMI pour l'agent collecteur FSSO ? (Choisissez-en deux.)

A. L'agent collecteur n'a pas besoin de rechercher les journaux d'événements de sécurité.

B. L'interrogation WMI peut augmenter l'utilisation de la bande passante sur les grands réseaux.

C. La fonction NetSessionEnum est utilisée pour suivre les déconnexions des utilisateurs.

D. L'agent collecteur utilise une API Windows pour interroger les DC sur les connexions des utilisateurs.

Quel schéma d'authentification n'est pas pris en charge par l'implémentation RADIUS sur le FortiGate ?

326. sur FortiGate ?

A. CHAP

B. MSCHAP2

C. PAP

D. FSSO

327.

FSSO est une solution d'authentification unique permettant d'authentifier les utilisateurs de manière transparente sur une unité FortiGate à l'aide des informations d'identification stockées dans le répertoire actif de Windows.

Lesquels des énoncés suivants sont corrects concernant FSSO dans un environnement de domaine Windows lorsque le mode DC-agent est utilisé ? (Choisissez-en deux.)

A. Un agent collecteur FSSO doit être installé sur chaque contrôleur de domaine.

B. Un agent contrôleur de domaine FSSO doit être installé sur chaque contrôleur de domaine.

C. L'agent contrôleur de domaine FSSO met régulièrement à jour les informations de connexion des utilisateurs sur l'unité FortiGate sur l'unité FortiGate.

D. L'agent collecteur FSSO reçoit les informations de connexion des utilisateurs de l'agent du contrôleur de domaine et les envoie à l'unité FortiGate.



328. Quelle est la meilleure description du délai d'authentification ?

A. La durée pendant laquelle FortiGate attend que l'utilisateur saisisse ses informations d'identification.

B. La durée pendant laquelle un utilisateur est autorisé à envoyer et à recevoir du trafic avant de devoir s'authentifier à nouveau.

C. La durée pendant laquelle un utilisateur authentifié peut rester inactif (sans envoyer de trafic) avant de devoir s'authentifier à nouveau.

D. Combien de temps une session authentifiée par un utilisateur peut exister sans devoir s'authentifier à nouveau.

329. Quelles sont les réponses valides d'un serveur RADIUS à un paquet ACCESS-REQUEST provenant d'une FortiGate ? (Choisissez-en deux.)

A. ACCESS-CHALLENGE

B. ACCESS-RESTRICT

C. ACCÈS EN ATTENTE

D. ACCESS-REJECT

330. Quel protocole ne peut pas être utilisé avec le type d'authentification active ?

A. Local

B. RADIUS

C. LDAP

D. RSSO

331. Lors de la configuration de LDAP sur le FortiGate comme base de données distante pour les utilisateurs, qu'est-ce qui ne fait pas partie de la configuration ?

A. Le nom de l'attribut qui identifie chaque utilisateur (Common Name Identifier).

B. Les noms des éléments du compte utilisateur ou du groupe (DN utilisateur).

C. Le secret du serveur pour permettre les requêtes à distance (secret du serveur primaire).

D. Les informations d'identification d'un administrateur LDAP (mot de passe).

332. Quelles méthodes d'authentification FortiGate prend-il en charge pour l'authentification du pare-feu ? (Choisissez-en deux.)

A. Service d'authentification à distance des utilisateurs (RADIUS)

B. Protocole d'accès aux annuaires légers (LDAP)

C. Authentification par mot de passe local

D. POP3

E. Authentification par mot de passe à distance

333. Quelles méthodes FortiGate peut-il utiliser pour envoyer un mot de passe à usage unique (OTP) aux utilisateurs de l'authentification à deux facteurs ? (Choisissez-en trois.)

A. FortiToken matériel

B. Portail Web

C. Courriel

D. Token USB

E. Logiciel FortiToken

334. Quels types de groupes d'utilisateurs FortiGate prend-il en charge pour l'authentification du pare-feu ?  
(Choisissez-en trois.)

- A. RSSO
- B. Pare-feu
- C. LDAP
- D. NTLM
- E. FSSO

335. Quelles sont les deux affirmations vraies concernant les clauses de non-responsabilité des politiques de pare-feu ? (Choisissez-en deux.)

- A. Ils ne peuvent pas être utilisés en combinaison avec l'authentification des utilisateurs.
- B. Ils ne peuvent être appliqués qu'aux interfaces sans fil.
- C. Les utilisateurs doivent accepter la clause de non-responsabilité pour continuer.
- D. La page de déni de responsabilité est personnalisable.

336. Lesquelles des affirmations suivantes sont vraies à propos des utilisateurs PKI créés dans un dispositif FortiGate ? (Choisissez-en deux.)

- A. Ils peuvent être utilisés pour l'authentification par jeton
- B. Peut être utilisé pour l'authentification à deux facteurs
- C. Sont utilisés pour l'authentification par certificat
- D. Ne peuvent pas être membres de groupes d'utilisateurs

337. Laquelle des affirmations suivantes concernant les temporisations de l'agent collecteur FSSO est vraie ?

- A. L'intervalle de vérification de la station de travail est utilisé pour vérifier périodiquement si une station de travail est toujours membre du domaine.
- B. L'intervalle de vérification de changement d'adresse IP surveille l'adresse IP du serveur où l'agent collecteur est installé et met à jour la configuration de l'agent collecteur si elle change.
- C. L'expiration du cache du groupe d'utilisateurs est utilisée pour faire vieillir les groupes surveillés.
- D. L'intervalle de temporisation des entrées mortes est utilisé pour faire vieillir les entrées dont l'état n'est pas vérifié.

338. Quel est l'inconvénient de l'utilisation du mode d'interrogation de FSSO NetAPI par rapport à FSSO Security Event Log (WinSecLog) ?

- A. Il nécessite l'installation d'un agent DC dans certains des DC Windows.
- B. Il est plus lent.
- C. Elle peut manquer certains événements de connexion.
- D. Elle nécessite l'accès à un serveur DNS pour la résolution des noms des stations de travail.

339. Quelles sont les deux conditions requises pour que le mode DC-agent FSSO fonctionne correctement dans un environnement Windows AD ?

AD ? (Choisissez-en deux.)

- A. Le serveur DNS doit résoudre correctement tous les noms de postes de travail.
- B. Le service de registre distant doit être exécuté sur tous les postes de travail.
- C. L'agent collecteur doit être installé dans l'un des contrôleurs de domaine Windows.
- D. Un même utilisateur ne peut pas être connecté à deux postes de travail différents en même temps.

340. Quelles sont les affirmations vraies concernant l'authentification des utilisateurs locaux ? (Choisissez-en deux.)

- A. L'authentification à deux facteurs peut être activée sur une base par utilisateur.
- B. Les utilisateurs locaux sont réservés aux comptes d'administration et ne peuvent pas être utilisés pour authentifier les utilisateurs du réseau.
- C. Les administrateurs peuvent créer les comptes d'utilisateur sur un serveur distant et stocker les mots de passe des utilisateurs localement dans la FortiGate.
- D. Les noms d'utilisateur et les mots de passe peuvent être stockés localement sur la FortiGate.

341. Le port1 de la FortiGate est connecté à l'Internet. Le port FortiGate est connecté au réseau interne. Examinez la configuration du pare-feu illustrée dans la pièce à conviction, puis répondez à la question ci-dessous. D'après la configuration du pare-feu illustrée dans la pièce, quelle affirmation est correcte ?

- A. Un utilisateur qui ne s'est pas authentifié peut accéder à Internet en utilisant n'importe quel protocole qui ne déclenche pas de demande d'authentification.
- B. Un utilisateur qui n'est pas authentifié peut accéder à Internet en utilisant n'importe quel protocole, à l'exception de HTTP, HTTPS, Telnet et FTP, Telnet et FTP.
- C. Un utilisateur doit s'authentifier à l'aide des protocoles HTTP, HTTPS, SSH, FTP ou Telnet avant de pouvoir accéder à tous les services Internet.
- D. L'accès Internet DNS est toujours autorisé, même pour les utilisateurs qui ne se sont pas authentifiés.

342. Lorsque l'authentification de la politique de pare-feu est activée, quels sont les protocoles qui peuvent déclencher un défi d'authentification ? (Choisissez-en deux)

- A. SMTP
- B. POP3
- C. HTTP
- D. FTP

343. Quelle affirmation concernant le délai d'authentification de la politique de pare-feu est vraie ?

- A. Il s'agit d'un délai d'inactivité. Le FortiGate considère qu'un utilisateur est " inactif " s'il ne voit pas de paquets provenant de l'IP source de l'utilisateur.
- B. Il s'agit d'un hard timeout. Le FortiGate supprime la stratégie temporaire pour l'adresse IP source d'un utilisateur après l'expiration de ce délai.
- C. Il s'agit d'un délai d'inactivité. Le FortiGate considère qu'un utilisateur est "inactif" s'il ne voit pas de paquets provenant du MAC source de l'utilisateur.
- D. Il s'agit d'un hard timeout. Le FortiGate supprime la politique temporaire pour l'adresse MAC source d'un utilisateur après l'expiration de ce délai.

344. Lorsque l'authentification de la politique de pare-feu est activée, seul le trafic sur les protocoles supportés sera

- A. SMTP déclenche un défi d'authentification. Sélectionnez tous les protocoles pris en charge parmi les suivants :
- B. SSH
- C. HTTP
- D. FTP
- E. SCP

345. toutes les réponses applicables.

Parmi les types d'authentification suivants, lesquels sont pris en charge par les unités FortiGate ? (Sélectionnez

- A. Kerberos
- B. LDAP
- C. RADIUS
- D. Utilisateurs locaux

346. Lesquels des éléments suivants sont des types de groupes d'utilisateurs d'authentification valides sur une unité FortiGate ? (Sélectionnez toutes les réponses applicables.)

- A. Pare-feu
- B. Service d'annuaire
- C. Local
- D. LDAP
- E. ICP

347. Un administrateur a configuré une unité FortiGate de sorte que les utilisateurs finaux doivent s'authentifier auprès du pare-feu à l'aide de certificats numériques avant de naviguer sur Internet.

De quoi l'utilisateur doit-il disposer pour que l'authentification soit réussie ? (Sélectionnez toutes les réponses applicables.)

- A. Une entrée dans un annuaire LDAP pris en charge.
- B. Un certificat numérique émis par un serveur CA.
- C. Un nom d'utilisateur et un mot de passe valides.
- D. Un certificat numérique émis par l'unité FortiGate.
- E. L'appartenance à un groupe d'utilisateurs du pare-feu.

348. L'unité FortiGate peut être configurée pour permettre l'authentification auprès d'un serveur RADIUS. Le serveur RADIUS peut utiliser plusieurs protocoles d'authentification différents au cours du processus d'authentification. Lesquels des protocoles d'authentification suivants sont valides et peuvent être utilisés lorsqu'un utilisateur s'authentifie auprès du serveur RADIUS ? (Sélectionnez toutes les réponses applicables.)

- A. MS-CHAP-V2 (protocole d'authentification Microsoft Challenge-Handshake v2)
- B. PAP (Protocole d'authentification par mot de passe)
- C. CHAP (Challenge-Handshake Authentication Protocol)
- D. MS-CHAP (Microsoft Challenge-Handshake Authentication Protocol V1)
- E. FAP (FortiGate Authentication Protocol)

349. Lesquels des éléments suivants sont des composants valides de Fortinet Server Authentication Extensions (FSAE) ?

Extensions (FSAE) ? (Sélectionnez toutes les réponses applicables.)

- A. Agent de sécurité local du domaine.
- B. Collector Agent.
- C. Agent Active Directory.
- D. Agent d'authentification de l'utilisateur.
- E. Domain Controller Agent.

350. Le paramètre Idle Timeout d'une unité FortiGate s'applique aux éléments suivants ?

- A. La navigation sur le Web
- B. Les connexions FTP
- C. Authentification des utilisateurs
- D. Accès administrateur
- E. Remplacement du filtrage Web

351. Avec FSSO, un utilisateur de domaine peut s'authentifier soit auprès du contrôleur de domaine exécutant l'agent collecteur et l'agent de contrôleur de domaine, soit auprès d'un contrôleur de domaine exécutant uniquement l'agent de contrôleur de domaine.

Si vous tentez de vous authentifier auprès du contrôleur de domaine secondaire exécutant uniquement l'agent de contrôleur de domaine, laquelle des affirmations suivantes est correcte ?

(Sélectionnez toutes les réponses applicables.)

- A. L'événement de connexion est envoyé à l'agent collecteur.
- B. L'unité FortiGate reçoit les informations utilisateur de l'agent de contrôleur de domaine du contrôleur secondaire.
- C. L'agent collecteur effectue la recherche DNS de l'adresse IP du client authentifié.
- D. L'utilisateur ne peut pas être authentifié auprès de l'appareil FortiGate de cette manière car chaque agent de contrôleur de domaine nécessite un agent collecteur dédié.

352. Lequel des énoncés suivants est correct en fonction de la configuration du pare-feu illustrée dans la pièce à conviction ? A. Un utilisateur peut accéder à Internet en utilisant uniquement les protocoles pris en charge par l'authentification de l'utilisateur.  
B. Un utilisateur peut accéder à Internet en utilisant n'importe quel protocole, à l'exception de HTTP, HTTPS, Telnet et FTP. Ces protocoles nécessitent une authentification avant que l'utilisateur ne soit autorisé à accéder.  
C. Un utilisateur doit s'authentifier en utilisant le protocole HTTP, HTTPS, SSH, FTP ou Telnet avant de pouvoir accéder à des services.  
d'accéder à un service.

D. Un utilisateur ne peut pas accéder à Internet à l'aide d'un quelconque protocole, à moins qu'il n'ait passé l'authentification du pare-feu.

353. Parmi les agents FSSO suivants, lesquels sont requis pour une solution en mode agent DC ?

pour une solution en mode agent DC ? (Choisissez-en 2)

- A. Agent FSSO
- B. Agent DC
- C. Agent collecteur
- D. Serveur Radius

354. Les fichiers signalés comme "suspects" ont été soumis à quel contrôle Antivirus ?

- A. Grayware
- B. Virus
- C. Bac à sable
- D. Heuristique

355. Quelles options de mise à jour des définitions d'antivirus et d'attaques sont prises en charge par les unités FortiGate ? (Choisissez-en deux.)

- A. Mise à jour manuelle en téléchargeant les signatures depuis le site d'assistance.
- B. Mises à jour automatiques FortiGuard.
- C. Pousser les mises à jour depuis le réseau de distribution FortiGuard.
- D. Exécutez la commande fortiguard-AV-AS à partir de l'interface CLI.

356. Quelle affirmation est correcte concernant l'analyse antivirus sur une unité FortiGate ?

- A. L'analyse antivirus est activée par défaut.
- B. Le support client Fortinet active l'analyse antivirus à distance pour vous.
- C. L'analyse antivirus doit être activée dans un profil de sécurité, qui doit être appliqué à une politique de pare-feu.
- D. L'activation de l'analyse antivirus dans un profil de sécurité permet d'activer la protection antivirus pour l'ensemble du trafic transitant par la FortiGate.

357. Quel mode d'inspection antivirus doit être utilisé pour analyser les protocoles SMTP, FTP, POP3 et SMB ?

- A. Basé sur un proxy
- B. Basé sur le DNS
- C. Basé sur le flux
- D. Man-in-the-middle.

358. Laquelle des options suivantes pouvez-vous utiliser pour mettre à jour les définitions de virus sur une unité FortiGate ? (Sélectionnez toutes les options applicables.)

- A. Mise à jour par poussée.
- B. Mise à jour planifiée
- C. Mise à jour manuelle
- D. Mise à jour FTP

359. Parmi les fonctions suivantes de mise à jour des définitions d'antivirus et d'attaques, lesquelles sont prises en charge par les unités FortiGate ? (Sélectionnez toutes les réponses applicables.)

- A. Mises à jour manuelles, à l'initiative de l'utilisateur, à partir du réseau de distribution FortiGuard.
- B. Mises à jour des définitions d'antivirus et d'attaques et des moteurs antivirus programmées toutes les heures, tous les jours ou toutes les semaines à partir du réseau de distribution FortiGuard.
- C. Mises à jour push du réseau de distribution FortiGuard.
- D. État des mises à jour, y compris les numéros de version, les dates d'expiration et les dates et heures des mises à jour les plus récentes.

Une unité FortiGate peut rechercher des virus sur quels types de trafic réseau ? (Sélectionnez toutes les réponses applicables.)

360. tous ceux qui s'appliquent).

- A. POP3
- B. FTP
- C. SMTP
- D. SNMP
- E. NetBios

361. Quels sont les trois différents types de mode de conservation qui peuvent se produire sur un dispositif FortiGate ? (Choisissez-en trois.)

- A. Proxy
- B. Système d'exploitation
- C. Noyau
- D. Système
- E. Dispositif

362.

Un dispositif FortiGate est configuré pour effectuer une mise à jour AV & IS programmée toutes les heures. Compte tenu des informations de la pièce à conviction, quand la prochaine mise à jour aura-t-elle lieu ?

- A. 01:00
- B. 02:05
- C. 11:00
- D. 11:08

363. Un administrateur a activé l'analyse antivirus basée sur le proxy et a configuré les paramètres suivants : Quelle affirmation concernant la configuration ci-dessus est vraie ?

```
config firewall profile-protocol-options
edit default
config http
set oversize-limit
10 set options oversize
fin
fin
```

- A. Les fichiers de plus de 10 Mo ne sont pas analysés pour détecter les virus et seront bloqués.
- B. La FortiGate analyse uniquement les 10 premiers Mo d'un fichier.
- C. Les fichiers de plus de 10 Mo sont envoyés au moteur heuristique pour être analysés.
- D. FortiGate analyse les fichiers par morceaux de 10 Mo.

fin

Exa

364. Quelle est la durée la plus longue autorisée sur un dispositif FortiGate pour que l'analyse antivirus se termine ?

- A. 20 secondes
- B. 30 secondes
- C. 45 secondes
- D. 10 secondes

365. Les fichiers dont la taille dépasse la limite de surdimensionnement sont soumis à quel contrôle Antivirus ?

- A. Grayware
- B. Virus
- C. Bac à sable
- D. Heuristique

366. Quel type de mode de conservation écrit un message de journal immédiatement, plutôt que lorsque le périphérique quitte le mode de conservation ?

- A. Noyau
- B. Proxy
- C. Système
- D. Dispositif

367. Quel est le nombre maximum de bases de données virales différentes qu'un FortiGate peut avoir ?

- A. 5
- B. 2
- C. 3
- D. 4



368. Lesquelles des affirmations suivantes sont vraies concernant le certificat SSL Proxy qui doit être utilisé pour l'inspection du contenu SSL ? (Choisissez-en deux.)

- A. Il ne peut pas être signé par une autorité de certification privée
- B. Il doit comporter soit le champ "CA=True", soit le champ "Key Usage-KeyCertSign".
- C. Il doit être installé dans le dispositif FortiGate.
- D. L'objet déposé doit contenir soit le FQDN, soit l'adresse IP du dispositif FortiGate.

369. Lesquels des énoncés suivants concernant le mode conversationnel sont vrais ? (Choisissez-en deux.)

- A. FortiGate cesse d'envoyer des fichiers à FortiSandbox pour inspection.
- B. FortiGate cesse d'effectuer des vérifications RPF sur les paquets entrants.
- C. Les administrateurs ne peuvent pas modifier la configuration.
- D. Les administrateurs peuvent accéder à la FortiGate uniquement via le port console.

370. Examinez cette configuration de la FortiGate :

```
config system global
set av-failopen pass
end
```

Examinez la sortie de la commande de débogage suivante :

```
# diagnose hardware sysinfo conserve
mode de conservation de la mémoire : on
RAM totale : 3040 Mo
```

Mémoire utilisée : 2948 Mo 97% de la RAM totale

mémoire libérable : 92 Mo 38 % de la RAM totale

mémoire utilisée + seuil de libération extrême : 2887 MB 95% de la RAM totale

mémoire utilisée seuil rouge : 2675 Mo 88% de la mémoire RAM totale

seuil de mémoire utilisée vert : 2492 MB 82% de la RAM totale

D'après les résultats du diagnostic ci-dessus, comment le FortiGate gère-t-il le trafic des nouvelles sessions qui nécessitent une inspection ?

- A. Il est autorisé, mais sans inspection
- B. Il est autorisé et inspecté tant que l'inspection est basée sur le flux
- C. Il est abandonné.
- D. Il est autorisé et inspecté, à condition que la seule inspection requise soit celle de l'antivirus.

371. Laquelle des fonctions suivantes de filtrage du spam n'est PAS prise en charge par une unité FortiGate ?

- A. Vérification de l'en-tête des Multipurpose Internet Mail Extensions (MIME)
- B. Recherche DNS HELO
- C. Greylisting
- D. Mot banni

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

Voir la pièce à conviction.

A. L'utilisateur doit s'authentifier avant d'accéder à des sites dont les certificats SSL ne sont pas fiables.

**B. L'utilisateur reçoit des avertissements relatifs aux certificats lorsqu'il se connecte à des sites dont les certificats SSL ne sont pas fiables.**

C. L'utilisateur est autorisé à accéder à tous les sites dotés de certificats SSL non fiables, sans avertissement de certificat.

D. L'utilisateur ne peut pas se connecter aux sites qui ont des certificats SSL non fiables (aucune exception n'est prévue).

373. Une politique de pare-feu a été configurée pour que le serveur de messagerie interne reçoive des courriers électroniques de parties externes via SMTP. Les figures A et B montrent les profils d'antivirus et de filtre de messagerie appliqués à cette politique. Quel est le comportement correct lorsque la pièce jointe d'un e-mail est détectée comme un virus par le moteur antivirus de FortiGate ?

A. L'unité FortiGate supprime le fichier infecté et envoie l'e-mail avec un message de remplacement pour avertir le destinataire que la pièce jointe d'origine était infectée.

**B. L'unité FortiGate rejette l'e-mail infecté et l'expéditeur reçoit un message d'échec de livraison.**

C. L'unité FortiGate supprime le fichier infecté et ajoute un message de remplacement.

D. L'expéditeur et le destinataire sont tous deux informés que le fichier infecté a été supprimé.

E. L'unité FortiGate rejette

374. Quelles déclarations concernant le processus de mise à niveau du micrologiciel sur un cluster haute disponibilité (HA) actif-actif sont vraies ? (Choisissez-en deux.)

A. L'image du micrologiciel doit être téléchargée manuellement sur chaque FortiGate.

**B. Seuls les périphériques FortiGate secondaires sont redémarrés.**

C. La mise à niveau ininterrompue est activée par défaut.

**D. L'équilibrage de la charge de trafic est temporairement désactivé pendant la mise à niveau du firmware.**

375. Laquelle des séquences suivantes décrit l'ordre correct des critères utilisés pour la sélection d'une unité maître au sein d'un cluster FortiGate à haute disponibilité (HA) lorsque la priorité est désactivée ?

A. 1. moniteur de port, 2. priorité de l'unité, 3. temps de fonctionnement, 4. numéro de série.

**B. 1. moniteur de port, 2. temps de fonctionnement, 3. priorité de l'unité, 4. numéro de série.**

C. 1. priorité de l'unité, 2. temps de fonctionnement, 3. moniteur de port, 4. numéro de série.

D. 1. temps de fonctionnement, 2. priorité de l'unité, 3. moniteur de port, 4. numéro de série.

376. Lesquels des énoncés suivants sont corrects concernant la commande HA diagnose sys ha reset- uptime ? (Choisissez-en deux.)

- A. Le dispositif sur lequel cette commande est exécutée est susceptible de passer du statut de maître à celui d'esclave si la fonction de neutralisation est désactivée.
- B. Le dispositif sur lequel cette commande est exécutée est susceptible de passer du statut de maître à celui d'esclave si la priorité est activée.
- C. Cette commande n'a aucun impact sur l'algorithme HA.
- D. Cette commande réinitialise la variable uptime utilisée dans l'algorithme HA ; elle peut donc provoquer l'élection d'un nouveau maître.

377. Quelles sont les conditions requises pour qu'un cluster HA maintienne les connexions TCP après un basculement de périphérique ou de liaison ? (Choisissez-en deux.)

- A. Activer la reprise de session.
- B. Activer le contournement.
- C. Les connexions doivent être UDP ou ICMP.
- D. Les connexions ne doivent pas être gérées par un proxy.

378. Dans HA, l'option Réserver le port de gestion pour le membre du cluster est sélectionnée comme indiqué dans l'illustration ci-dessous. Quelles sont les affirmations correctes concernant ce paramètre ? (Choisissez-en deux.)

- A. Les paramètres d'interface du port 7 ne seront pas synchronisés avec les autres membres du cluster.
- B. L'adresse IP attribuée à cette interface ne doit pas chevaucher le sous-réseau d'adresses IP attribué à une autre interface.
- C. Lorsque vous vous connectez au port7, vous vous connectez toujours à l'appareil maître.
- D. Une adresse de passerelle peut être configurée pour le port7.

379. La pièce montre la commande Disconnect Cluster Member dans une unité FortiGate faisant partie d'un cluster HA avec deux membres HA. Quel est l'effet de la commande Disconnect Cluster Member telle qu'elle est présentée dans l'illustration ? (Choisissez-en deux.)

- A. Le port 3 est configuré avec une adresse IP pour l'accès à la gestion.
- B. Les règles de pare-feu sont purgées sur l'unité déconnectée.
- C. Le mode HA passe à standalone.
- D. Le nom d'hôte du système est défini sur le numéro de série de l'unité.

380. Deux périphériques sont dans un cluster HA, les noms d'hôte des périphériques sont STUDENT et REMOTE. La pièce A montre la sortie de commande de diagnose sys session stat pour le dispositif STUDENT. La pièce B montre la sortie de la commande diagnose sys session stat pour le dispositif REMOTE. Pièce A et B : Compte tenu des informations fournies dans les pièces, laquelle des affirmations suivantes est correcte ? (Choisissez-en deux.)

- A. STUDENT est probablement le périphérique maître.
- B. La collecte de session est probablement activée.
- C. Le mode de cluster est actif-passif.
- D. Il n'y a pas assez d'informations pour déterminer le mode de cluster.

381. Un administrateur a formé un cluster de haute disponibilité impliquant deux unités FortiGate. [Plusieurs commutateurs de couche 2 en amont] -- [ Cluster FortiGate HA ] -- [ Plusieurs commutateurs de couche 2 en aval ].

L'administrateur souhaite s'assurer qu'une seule défaillance de lien aura un impact minimal sur le débit global du trafic à travers ce cluster.

Laquelle des options suivantes décrit la meilleure mesure que l'administrateur peut prendre ? L'administrateur doit

A. Augmenter le nombre d'unités FortiGate dans le cluster et configurer HA en mode actif-actif.

B. Activer la surveillance de toutes les interfaces actives.

**C. Configurez une conception à maillage complet qui utilise des interfaces redondantes.**

D. Configurez la fonction de serveur ping HA pour permettre le basculement HA en cas d'interruption d'un chemin.

382. Dans un cluster haute disponibilité fonctionnant en mode actif-actif, laquelle des propositions suivantes décrit correctement le chemin emprunté par le paquet SYN d'une session HTTP qui est déchargé sur une unité esclave ?

A. Demande : hôte interne ; FortiGate esclave ; FortiGate maître ; Internet ; serveur Web.

B. Demande : hôte interne ; FortiGate esclave ; Internet ; serveur web.

C. Demande : hôte interne ; FortiGate esclave ; FortiGate maître ; Internet ; serveur Web.

**D. Demande : hôte interne ; FortiGate maître ; FortiGate esclave ; Internet ; serveur web.**

383. Lequel des énoncés suivants décrit correctement le fonctionnement d'une unité FortiGate en mode Transparent ?

A. Pour gérer l'unité FortiGate, l'une des interfaces doit être désignée comme interface de gestion. Cette interface ne doit pas être utilisée pour le transfert de données.

**B. Une adresse IP est utilisée pour gérer l'unité FortiGate mais cette adresse IP n'est pas associée à une interface spécifique.**

C. L'unité FortiGate doit utiliser des adresses IP publiques sur les réseaux interne et externe.

D. L'unité FortiGate utilise des adresses IP privées sur le réseau interne mais les cache en utilisant la traduction d'adresse.

384. Quelles sont les conditions requises pour qu'un cluster maintienne les connexions TCP après un basculement de périphérique ou de liaison ? (Sélectionnez toutes les réponses applicables.)

**A. Activer la reprise de session.**

B. S'applique uniquement aux connexions gérées par un proxy.

C. S'applique uniquement aux connexions UDP et IMP.

**D. Les connexions ne doivent pas être gérées par un proxy.**

385. Two FortiGate devices fail to form an HA cluster, the device hostnames are STUDENT and REMOTE. Exhibit A shows the command output of show system ha for the STUDENT device. Exhibit B shows the command output of show system ha for the REMOTE device. Which one of the following is the most likely reason that the cluster fails to form?

A. Password

**B. HA mode**

C. Heartbeat

D. Override

Laquelle des raisons suivantes est la plus probable pour laquelle le cluster ne parvient pas à se former ?

386. Lequel des énoncés suivants décrit correctement l'utilisation de la commande "diagnose sys ha reset-uptime" ?

**A. Pour forcer un basculement HA lorsque le paramètre HA override est désactivé.**

B. Pour forcer un basculement HA lorsque le paramètre de remplacement HA est activé.

C. Pour effacer les compteurs HA.

D. Pour redémarrer une unité FortiGate qui fait partie d'un cluster HA.

387. Quels sont les éléments qui doivent être identiques pour que deux unités FortiGate forment un cluster HA ? (Choisissez-en deux)

**A. Firmware.**

**B. Modèle.**

C. Nom d'hôte.

D. Fuseau horaire du système.

388. Lequel des énoncés suivants décrit les objectifs des paquets ARP gratuits envoyés par un cluster HA ?

A. Pour synchroniser les tables ARP dans toutes les FortiGate Unis qui font partie du cluster HA.

**B. Pour notifier aux commutateurs du réseau qu'une nouvelle unité maître HA a été élue.**

C. Pour notifier à l'unité maître que les dispositifs esclaves sont toujours en marche et vivants.

D. Pour notifier à l'unité maître les adresses MAC physiques des unités esclaves.

389.

Lesquels des énoncés suivants sont corrects concernant une unité HA maître ? (Choisissez-en deux)

**A. Il ne doit y avoir qu'une seule unité maîtresse dans chaque grappe vitale HA.**

**B. Le maître synchronise la configuration du cluster avec le stree**

C. Seul le maître dispose d'une interface HA de gestion réservée.

D. Les interfaces Heartbeat ne sont pas nécessaires sur une unité maître. 83

390. Quelle affirmation décrit la manière dont le trafic circule dans les sessions gérées par une unité esclave dans un cluster HA actif-actif ?

A. Les paquets sont envoyés directement à l'unité esclave en utilisant l'adresse MAC physique de l'esclave.

B. Les paquets sont envoyés directement à l'unité esclave en utilisant l'adresse MAC virtuelle HA.

C. Les paquets arrivent aux deux unités simultanément, mais seule l'unité salve transmet la session.

**D. Les paquets sont d'abord envoyés à l'unité maître, qui les transmet ensuite à l'unité esclave.**

391. Lesquelles des affirmations suivantes sont correctes concernant le protocole de support de vie de session de FortiGate ? (Choisissez-en deux)

- A. Par défaut, les sessions UDP ne sont pas synchronisées.
- B. Jusqu'à quatre dispositifs FortiGate en mode autonome sont pris en charge.
- C. seule l'unité maître gère le trafic.
- D. Permet la synchronisation des sessions par VDOM.

392. Quels sont les critères par défaut pour la sélection de l'unité maître HA dans un cluster HA ?

- A. surveillance des ports, priorité, temps de fonctionnement, numéro de série
- B. Surveillance des ports, temps de fonctionnement, priorité, numéro de série.
- C. Priorité, temps de fonctionnement, surveillance des ports, numéro de série
- D. uptime, priorité, moniteur de port, numéro de série

393. Quelles informations sont synchronisées entre deux unités FortiGate qui appartiennent au même cluster HA ? (Choisissez-en trois)

- A. Adresses IP attribuées à l'interface activée par DHCP.
- B. Le nom d'hôte du dispositif maître.
- C. Routage configuré et état
- D. Configuration IP de l'interface de gestion HA réservée.
- E. Politiques et objets du pare-feu.

394. Visualisez la pièce à conviction. D'après cette sortie, quelles sont les affirmations correctes ?

(Choisissez-en deux.)

- A. Le VDOM a11 n'est pas synchronisé entre les dispositifs FortiGate primaire et secondaire.
- B. Le VDOM racine n'est pas synchronisé entre les dispositifs FortiGate primaire et secondaire.
- D. Les dispositifs FortiGate ont trois VDOM.
- C. La configuration globale est synchronisée entre les dispositifs FortiGate primaire et secondaire.

395. Examinez l'exposition d'une configuration de politique de proxy explicite.

En cas de tentative de connexion par proxy provenant de l'adresse IP 10.0.1.5 et d'un utilisateur qui

ne s'est pas encore authentifié, quelle action le proxy FortiGate entreprend-il ?

- A. L'utilisateur est invité à s'authentifier. Le trafic de l'utilisateur Student sera autorisé par la politique #1. Le trafic de tout autre utilisateur sera autorisé par la politique n°2.
- B. L'utilisateur n'est pas invité à s'authentifier. La connexion est autorisée par la politique de proxy #2
- c. L'utilisateur n'est pas invité à s'authentifier. La connexion sera autorisée par la politique de proxy #1
- D. L'utilisateur est invité à s'authentifier. Seul le trafic de l'utilisateur Student est autorisé. Le trafic de tout autre utilisateur sera bloqué.

396. Quelle est la raison valable pour utiliser l'authentification basée sur la session au lieu de

l'authentification basée sur l'IP dans une solution de proxy web FortiGate ?

A. Les utilisateurs doivent saisir manuellement leurs informations d'identification chaque fois qu'ils se connectent à un autre site web.

B. Les utilisateurs proxy sont authentifiés via FSSO.

**C. Plusieurs utilisateurs partagent la même adresse IP.**

D. Les utilisateurs du proxy sont authentifiés via RADIUS.

397. Examinez la configuration suivante du proxy Web FortiGate, puis répondez à la question cidessous :

```
config web-proxy explicit set pac-file-server-status enable set pac-file-server-port 8080 set pac-filename wad.dat end
```

En supposant que l'adresse IP du proxy FortiGate est 10.10.1.1, quelle URL un navigateur Internet

doit-il utiliser pour télécharger le fichier PAC ?

A. https://10.10.1.1:8080

B. https://10.10.1.1:8080/wpad.dat

C. http://10.10.1.1:8080/

**D. http://10.10.1.1:8080/wpad.dat**

398. Quelles sont les affirmations vraies concernant l'utilisation d'un fichier PAC pour configurer les

paramètres du proxy web dans un navigateur Internet ? (Choisissez-en deux.)

A. Un seul proxy est pris en charge.

B. Peut être importé manuellement dans le navigateur.

**C. Le navigateur peut le télécharger automatiquement depuis un serveur web.**

**D. Peut inclure une liste de sous-réseaux IP de désanation auxquels le navigateur peut se connecter directement sans passer par le réseau de l'entreprise.**

399.

Quelles sont les deux méthodes prises en charge par le protocole de découverte automatique du proxy

Web ?

**A. DHCP**

**WPAD) pour apprendre automatiquement l'URL où se trouve un fichier PAC ? (Choisissez-en deux.)**

B. BOOTP

? - Aujourd'hui à 18:51

**C. DNS**

D. Configuration automatique d'IPv6

400. Quelle est une raison valable pour utiliser l'authentification basée sur la session au lieu de

l'authentification basée sur l'IP dans une solution de proxy web FortiGate ?

A. Les utilisateurs doivent saisir manuellement leurs informations d'identification chaque fois qu'ils se

connectent à un autre site web.

B. Les utilisateurs proxy sont authentifiés via FSSO.

**C. Plusieurs utilisateurs partagent la même adresse IP.**

D. Les utilisateurs du proxy sont authentifiés via RADIUS.

401. Un navigateur Internet utilise la méthode WAD DNS pour discovaddresPAC fles.

URL. Le serveur DNS répond à la demande du navigateur avec l'adresse IP 10.100.1.10.

Quelle URL le

navigateur utilisera-t-il pour télécharger le fichier PAC ?

A. http://10.100.1.10/proxy.pac

B. https://10.100.1.10/

**C. http://10.100.1.10/wpad.dat**

D. https://10.100.1.10/proxy.pac

402. Quel protocole un navigateur Internet peut-il utiliser pour télécharger le fichier PAC avec

la configuration du proxy web ?

A. HTTPS

B. FTP

C. TFTP

**D. HTTP**

403. Lequel des éléments suivants doit être configuré sur une unité FortiGate pour rediriger les

demandes de contenu vers des serveurs de cache Web distants ?

**A. WCCP doit être activé sur l'interface faisant face au cache Web.**

B. Vous devez activer le Web-proxy explicite sur l'interface entrante.

C. WCCP doit être activé en tant que paramètre global sur l'unité FortiGate.

D. WCCP doit être activé sur toutes les interfaces de l'unité FortiGate par lesquelles le trafic HTTP passe.

404. Lorsque vous utilisez la méthode WAD DNS, quel est le format FQDN que les navigateurs

utilisent pour interroger le serveur DNS ?

**A. wad. <domaine local>**

B. srv\_tep.wpad. <domaine local>

C. srv\_proxy. <domaine local>/wad.dat

D. proxy. <domaine-local>.wpad

405. Quelles déclarations concernant l'authentification proxy explicite basée sur IP sont vraies ?

(Choisissez-en deux.)

A. L'authentification basée sur l'IP est la plus adaptée pour authentifier les utilisateurs derrière un dispositif NAT.

**B. Les sessions provenant de la même adresse source sont traitées comme un seul utilisateur.**

**C. L'authentification basée sur l'IP consomme moins de mémoire du FortiGate que l'authentification basée sur la session.**

D. FortiGate mémorise les sessions authentifiées à l'aide de cookies de navigateur.

406. Laquelle des affirmations suivantes est vraie concernant les paquets TCP SYN qui vont d'un

client, via un proxy web implicite (proxy transparent), à un serveur web écoutant le port TCP 80 ?

(Choisissez-en trois.)

**A. L'adresse IP source correspond à l'adresse IP du client.**

B. L'adresse IP source correspond à l'adresse IP du proxy.

C. L'adresse IP de destination correspond à l'adresse IP du proxy.

**D. L'adresse IP de destination correspond aux adresses IP du serveur.**



E. Le numéro du port TCP de destination est 80.

407. Laquelle des affirmations suivantes est vraie concernant l'utilisation d'un fichier PAC pour Plus d'un proxy est supporté.

configurer les paramètres du proxy web dans un navigateur Internet ? (Choisissez-en deux.)

B Peut contenir une liste de destinations qui seront exemptées de l'utilisation de tout proxy.

C. Peut contenir une liste d'URLs qui seront exemptées de l'inspection du filtrage web de FortiGate.

D. Peut contenir une liste d'utilisateurs qui seront exemptés de l'utilisation de tout proxy.

408. Lesquels des points suivants sont des avantages de l'utilisation de la mise en cache web ?

(Choisissez-en trois.)

A. Diminution de l'utilisation de la bande passante

B. Réduire la charge du serveur

C. Réduire l'utilisation du CPU de FortiGate

D. Réduire l'utilisation de la mémoire de FortiGate

E. Réduire les délais de circulation

409.

Un administrateur souhaite bloquer les téléchargements HTTP. Examinez la pièce à conviction, qui

contient l'adresse proxy créée à cette fin.

Où l'adresse proxy doit-elle être utilisée ?

A. Comme la source dans une politique de pare-feu.

B. Comme la source dans une politique de proxy.

C. Comme destination dans une politique de pare-feu.

D. Comme destination dans une politique de proxy.

410. Lesquels des énoncés suivants sont vrais lors de l'utilisation de WAD avec la méthode de

découverte DHCP ? (Choisissez-en deux.)

A. Si la méthode DHCP échoue, les navigateurs essaieront la méthode DINS.

B. le navigateur doit être préconfiguré avec l'adresse IP des serveurs DHCP.

C. Le navigateur envoie une requête DHCPINFORM au serveur DHCP.

D. Le serveur DHCP fournit le fichier PAC à télécharger.

411. Examinez la configuration de ce fichier PAC.

fonction FindProxyForURL (url, host) 1 if (shExpMatch (url,

, ".fortinet.com/)) t

return "DIRECT" ; }

si (isInNet (host, "172.25.120.04, "255.255.255.0 )) | return "PROXY" altproxy.corp.com : 8060" ; )

return "PROXY proxy.corp.com : 8090" ;

}

Lesquels des énoncés suivants sont vrais ? (Choisissez-en deux.)

A. Les navigateurs peuvent être configurés pour récupérer ce fichier PAC depuis le FortiGate.

B. Toute requête web vers le 172.25. 120. 0/24 est autorisée à contourner le proxy.

C. Toutes les demandes qui ne sont pas faites à Fortinet.com ou au sous-réseau 172.25. 120.0/24, doivent passer par altproxy.corp.com : 8060.

D. Toute requête web fortinet.com est autorisée à contourner le proxy.

412. Dans la sortie de la table de session de FortiOS, quel est le numéro correct de l'état du proto

pour une connexion TCP établie et non proxyée ?

A. 00

B. 11

C. 01

D. 05

413. Lesquels des énoncés suivants sont corrects concernant les configurations de VPN dialup

IPsec pour les dispositifs FortiGate ? (Choisissez-en deux)

A. Le mode principal doit être utilisé lorsqu'il n'y a pas plus d'un VPN dialup IPsec configuré sur

le même appareil FortiGate.

B. Un appareil FortiGate avec un VPN IPsec configuré comme dialup peut initier la connexion du

tunnel à n'importe quelle adresse IP distante.

C. Peer ID doit être utilisé lorsqu'il y a plus d'un VPN dialup IPsec en mode agressif sur le même

dispositif FortiGate.

D. Le FortiGate ajoutera automatiquement une route statique à l'adresse source du sélecteur

de mode rapide reçue de chaque pair distant.

414. Vous êtes chargé d'architecturer un nouveau déploiement IPsec avec les critères suivants :

- Il existe deux sites du siège social auxquels tous les bureaux satellites doivent se connecter.

- Les bureaux satellites n'ont pas besoin de communiquer directement avec d'autres bureaux satellites.

- Aucun routage dynamique ne sera utilisé.

- La conception doit minimiser le nombre de tunnels à configurer. Quelle topologie doit être utilisée pour satisfaire toutes les exigences ?

A. Redondant

B. Hub-and-spoke

C. Maille partielle

D. Entièrement maillé

415. Lesquels des énoncés suivants sont corrects ? (Choisissez-en deux.)

A. C'est une configuration IPsec redondante.

B. La route Tunnel est la route principale pour la recherche du site distant. La route Tunnel est

utilisée uniquement si le VPN TunnelB est en panne.

C. Cette configuration nécessite au moins deux politiques de pare-feu dont l'action est définie sur

IPsec.

D. La détection des pairs morts doit être désactivée pour prendre en charge ce type de configuration

IPsec.

416. Quels énoncés décrivent le mieux le VPN à découverte automatique (ADVPN).  
(Choisissez-en deux.)

A. Il nécessite l'utilisation de protocoles de routage dynamique afin que les rayons puissent apprendre les routes vers d'autres rayons.

B. ADVPN n'est pris en charge qu'avec IKEv ?

C. Les tunnels sont négociés dynamiquement entre les rayons.

D. Chaque rayon nécessite la configuration d'un tunnel statique vers les autres rayons afin que les propositions de phase 1 et de phase 2 soient définies à l'avance.

417. Quels avantages y a-t-il à utiliser une configuration VPN IPSec en étoile au lieu d'un ensemble

de tunnels IPSec entièrement maillés ? (Sélectionnez toutes les réponses qui s'appliquent.)

A. L'utilisation d'une topologie en étoile est nécessaire pour obtenir une redondance complète.

B. L'utilisation d'une topologie en étoile simplifie la configuration car moins de tunnels sont nécessaires.

C. L'utilisation d'une topologie en étoile permet un cryptage plus fort.

D. Le routage au niveau d'un rayon est plus simple, comparé à un nœud maillé.

Quels énoncés sont des propriétés correctes d'un déploiement VPN à maillage partiel.  
(Choisissez 418. deux.)

A. Les tunnels VPN s'interconnectent entre chaque site.

B. Les tunnels VPN ne sont pas configurés entre chaque site.

C. Certains sites sont accessibles via un site central.

D. Il n'y a pas d'emplacement de hub dans un maillage partiel

419. Examinez la configuration spanning tree suivante sur un FortiGate en mode transparent : Quel

énoncé est correct pour la configuration ci-dessus ?  
config system interface edit <interface name>

set stp-forward enable end

A. Le FortiGate participe à l'arborescence (spanning tree)

B. Le dispositif FortiGate transmet les messages spanning tree reçus.

C. Des boucles de la couche 2 d'Ethernet sont susceptibles de se produire.

D. Le FortiGate génère des trames BPDU de spanning tree.

420. Quels avantages y a-t-il à utiliser une configuration VPN IPSec entièrement maillée au lieu d'un

ensemble de tunnels IPSec en étoile ?

A. L'utilisation d'une topologie en étoile est nécessaire pour obtenir une redondance complète.

B. L'utilisation d'une topologie à maillage complet simplifie la configuration.

C. L'utilisation d'une topologie à maillage complet permet un cryptage plus fort.

D. La topologie à maillage complet est la configuration la plus tolérante aux pannes.

421. Lesquels des énoncés suivants sont corrects concernant la configuration du mode IKE ? (Choisissez-en deux)

A. Il peut attribuer dynamiquement des adresses IP aux clients VPN IPsec.

B. Il peut attribuer dynamiquement des paramètres DNS aux clients VPN IPsec.

C. Il utilise le protocole ESP.

D. Il peut être activé dans la configuration de la phase 2.

422. Qu'est-ce qui est nécessaire dans une configuration FortiGate pour avoir plus d'un VPN IPsec dialup utilisant le mode agressif ?

A. Tous les VPN dialup en mode agressif DOIVENT accepter des connexions provenant du même ID de

pair.

B. Chaque ID d'homologue DOIT correspondre au FQDN de chaque homologue distant.

C. Chaque dialup en mode agressif DOIT accepter des connexions provenant de différents peer ID.

D. Le paramètre peer ID ne doit PAS être utilisé.

423. Un administrateur réseau doit mettre en œuvre une redondance de route dynamique entre

une unité FortiGate située dans un bureau distant et une unité FortiGate située dans le bureau

central.

Le bureau distant accède aux ressources centrales en utilisant des tunnels VPN IPSec via deux

fournisseurs d'accès Internet différents.

Quelle est la meilleure méthode pour permettre au bureau distant d'accéder aux ressources via

l'unité FortiGate utilisée au bureau central ?

A. Utilisez deux ou plusieurs tunnels VPN IPSec basés sur les routes et activez OSPF sur l'interface

virtuelle IPSec.

B. Utilisez deux ou plusieurs tunnels VPN IPSec basés sur des règles et activez OSPF sur les interfaces

virtuelles IPSec.

C. Utilisez des VPN basés sur les routes sur l'unité FortiGate du bureau central pour annoncer les

routes avec un protocole de routage dynamique et utilisez un VPN basé sur les politiques sur le

bureau distant avec deux ou plusieurs routes statiques par défaut.

D. Les protocoles de routage dynamique ne peuvent pas être utilisés sur les tunnels VPN IPSec.

424. Quels énoncés décrivent correctement le fonctionnement en mode transparent ?

(Choisissez-en

trois.)

A. La FortiGate agit comme un pont transparent et transmet le trafic au niveau de la couche 2.

B. Les paquets Ethernet sont transférés en fonction des adresses MAC de destination, et NON des adresses IP.

C. La FortiGate transparente est clairement visible pour les hôtes du réseau dans une route de traçage

IP.

D. Permet l'inspection du trafic en ligne et la mise en place de pare-feu sans modifier le schéma IP du réseau.

E. Toutes les interfaces de l'appareil FortiGate en mode transparent doivent être sur des sous-réseaux IP différents.

425. Examinez la configuration suivante de spanning tree sur un FortiGate en mode transparent : config system interface edit <interface name> set stp-forward enable end. Quelle affirmation est correcte pour la configuration ci-dessus ?

- A. Le FortiGate participe au spanning tree.
- B. Le dispositif FortiGate transmet les messages spanning tree reçus.
- C. Des boucles de la couche 2 d'Ethernet sont susceptibles de se produire.
- D. Le FortiGate génère des trames BPDU de spanning tree.

426. Parmi les affirmations suivantes, quelles sont les différences correctes entre le mode NAT/route et le mode transparent ? (Choisissez-en deux.)

- A. En mode transparent, les interfaces n'ont pas d'adresse IP.
- B. Les polices de pare-feu ne sont utilisées qu'en mode NAT/route.
- C. Les routeurs statiques ne sont utilisés qu'en mode NAT/route.
- D. Seul le mode transparent permet l'inspection du trafic en ligne au niveau de la couche 2.

427. Laquelle des affirmations suivantes est vraie concernant un dispositif FortiGate fonctionnant en mode transparent ? (Choisissez-en trois.)

- A. Il agit comme un pont de couche 2
- B. Il agit comme un routeur de niveau 3
- C. Il transmet les trames en utilisant l'adresse MAC de destination.
- D. Il transmet les paquets en utilisant l'adresse IP de destination.
- E. Il peut effectuer une inspection du contenu (antivirus, filtrage web, etc.)

428. Examinez la topologie du réseau dans la pièce à conviction.

La station de travail, 172.16.1.1/24, se connecte au port2 du dispositif FortiGate, et le routeur du

FAI, 172.16.1.2, se connecte au port. Sans modifier l'adressage IP, quels changements de configuration sont nécessaires pour transférer correctement le trafic des utilisateurs vers Internet ?

(Choisissez-en deux)

- A. Au moins une politique de pare-feu du port2 au port1 pour autoriser le trafic sortant.
- B. Une route par défaut configurée dans les dispositifs FortiGuard pointant vers le routeur du FAI.
- C. Adresses IP statiques ou dynamiques dans les deux interfaces FortiGate port1 et port2.
- D. Les dispositifs FortiGate configurés en mode transparent.

429. Lesquelles des affirmations suivantes sont correctes concernant les domaines de diffusion de couche 2 dans les VDOM en mode transparent ? (Choisissez-en deux)

- A. L'ensemble du VDOM est un domaine de diffusion unique, même lorsque plusieurs VLAN sont utilisés.
- B. Chaque VLAN est un domaine de diffusion distinct.
- C. Les interfaces configurées avec le même ID VLAN peuvent appartenir à des domaines de diffusion différents.
- D. Toutes les interfaces du même domaine de diffusion doivent utiliser le même ID de VLAN.

430. Laquelle des affirmations suivantes est correcte concernant les interfaces FortiGate et le

protocole spanning tree ? (Choisissez-en deux)

- A. Seules les interfaces du commutateur FortiGate participent à l'arbre de spanning.
- B. Les interfaces All FortiGate dans les VDOMs en mode transparent participent au spanning tree.**
- C. Toutes les interfaces FortiGate en mode NAT/route VDOMs Participent au spanning tree.
- D. Toutes les interfaces FortiGate dans les VDOMs en mode transparent peuvent bloquer ou transmettre les BPDUs.**

431. Lequel des énoncés suivants décrit correctement le fonctionnement d'une unité FortiGate en mode Transparent ?

- A. Pour gérer l'unité FortiGate, l'une des interfaces doit être désignée comme interface de gestion. Cette interface ne doit pas être utilisée pour le transfert de données.
- B. Une adresse IP est utilisée pour gérer l'unité FortiGate mais cette adresse IP n'est pas associée à une interface spécifique.**
- C. L'unité FortiGate doit utiliser des adresses IP publiques sur les réseaux interne et externe.
- D. L'unité FortiGate utilise des adresses IP privées sur le réseau interne mais les cache en utilisant la traduction d'adresse.

432. Quelle fonction de FortiGate peut être utilisée pour bloquer un balayage ping d'un attaquant ?

- A. Pare-feu d'application Web (WAF)
- B. Signatures IPS basées sur le taux
- C. Renifleur à un bras
- D. Politiques de DoS**

433. Votre serveur de messagerie Linux fonctionne sur un numéro de port non standard, le port

2525. Quelle affirmation est vraie ?

- A. IPS ne peut pas analyser ce trafic pour des anomalies SMTP à cause du numéro de port non standard. Vous devez donc J'ai reconfiguré le serveur pour qu'il fonctionne sur le port 2.
- B. Pour appliquer l'IPS au trafic vers ce serveur, vous devez configurer le proxy SMTP de FortiGate pour qu'il écoute sur le port 2525.
- C. IPS appliquera toutes les signatures SMTP, qu'elles s'appliquent aux clients ou aux serveurs.

**D. Les décodeurs de protocole détectent automatiquement le SMTP et recherchent les correspondances avec la signature IPS appropriée.**

434. Examinez le message de journal suivant pour IPS et identifiez les réponses valides ci-dessous.

(Sélectionnez toutes les réponses qui s'appliquent.)

- A. La cible est 192.168.3. 168.
- B. La cible est 192.168.3.170.**
- C. L'attaque a été détectée et bloquée.
- D. L'attaque a été détectée seulement**
- E. L'attaque était basée sur le protocole TCP.

435. Identifiez l'énoncé qui décrit correctement la sortie de la commande suivante :

diagnose ips anomaly list

A. Liste la politique DoS configurée.

**B. Liste les compteurs en temps réel pour la politique DoS configurée.**

C. Liste des erreurs capturées lors de la compilation de la politique DoS.

D. Liste les correspondances des signatures IPS.

436. Examinez la configuration du filtre du capteur IPS illustrée dans la pièce ; En fonction des

informations de la pièce, quelles sont les affirmations correctes concernant le filtre ?

(Choisissez-en deux.)

A. Il n'enregistre pas les attaques visant les serveurs Linux.

B. Il correspond à tout le trafic vers les serveurs Linux.

**C. Son action bloquera le trafic correspondant à ces signatures.**

**D. Il ne prend effet que lorsque le capteur est appliqué à une police.**

437. Par défaut, le système de protection contre les intrusions (IPS) d'une unité FortiGate est

configuré pour effectuer quelle action ?

A. Bloquer toutes les attaques du réseau.

B. Bloquer les attaques réseau les plus courantes.

**C. Autorise tout le trafic**

D. Autoriser et enregistrer tout le trafic

438. Dans lequel des modèles de rapport suivants devez-vous configurer les graphiques à inclure

dans le rapport ?

**A. Modèle de mise en page**

B. Modèle de filtre de données

C. Modèle de sortie

D. Modèle d'horaire

439. Un administrateur examine les journaux d'attaques et remarque l'entrée suivante :

D'après les informations affichées dans cette entrée, lesquelles des affirmations suivantes sont

correctes ? (Cochez toutes les réponses qui s'appliquent.)

A. C'est une attaque du serveur HTTP.

B. L'attaque a été détectée et bloquée par l'unité FortiGate.

**C. L'attaque visait une unité FortiGate à l'adresse IP 192.168. 1. 100.**

**D. L'attaque a été détectée et passée par l'unité FortiGate**

440. Examinez la configuration CLI ci-dessous pour un capteur IPS et identifiez les affirmations correctes concernant cette configuration parmi les choix ci-dessous.

(Sélectionnez toutes les réponses qui appliquer.

A. Le capteur enregistrera toutes les attaques de serveurs pour tous les systèmes d'exploitation.

**B. Le capteur inclura un fichier PCAP avec une trace des paquets correspondants dans le message**

**de journal de toute signature correspondante.**

C. Le capteur correspondra à tout le trafic provenant de l'objet d'adresse 'LINUX\_SERVER'.

D. Le capteur réinitialisera toutes les connexions qui correspondent à ces signatures.

**E. Le capteur filtre uniquement les signatures IPS à appliquer à la politique de pare-feu sélectionnée.**

441. Laquelle des propositions suivantes décrit la meilleure signature personnalisée pour détecter

l'utilisation du mot "Fortinet" dans les applications de chat ?

A. L'exemple de trace de paquet illustré dans la pièce fournit des détails sur le paquet qui doit

être détecté. F-SBID(--protocol tcp ; --flow from\_client ; --pattern "X-MMS-IM-Format" ; --pattern "fortinet",  
- no\_case ;)

B. F-SBID ( --protocole tcp ; -flow from\_client ; --pattern "fortinet" ; --no\_case ;)

C. F-SBID(--protocole tcp ; -flow from\_client ; --pattern "X-MMS-IM-Format" ; --pattern "fortinet", - within  
20 ; --no\_case ; )

D. F-SBID(--protocole tcp ; -flow from\_client ; --pattern "X-MMS-IM-Format" ; -pattern "fortinet", - within  
20 ; )

442. Lequel des modèles de rapport suivants doit être utilisé lors de la planification de la génération de rapports ?

A. Modèle de mise en page

B. Modèle de filtre de données

C. Modèle de sortie

D. Modèle de graphique

443. Lesquelles décrivent le mieux le mécanisme d'une inondation TCP SYN ?

A. L'attaquant maintient ouvertes de nombreuses connexions avec une transmission lente des

données, de sorte que les autres clients ne peuvent pas établir de nouvelles connexions.

B. L'attaquant envoie un paquet conçu pour se "synchroniser" avec le FortiGate.

L'attaquant envoie un paquet malformé spécialement conçu, destiné à faire tomber la cible en

faisant exploser son analyseur syntaxique.

D. L'attaquant commence de nombreuses connexions, mais ne reconnaît jamais les former complètement.

444. Acme Web Hosting remplace l'un de ses pare-feu par un FortiGate. Il doit être capable d'appliquer le transfert de port à ses serveurs Web dorsaux tout en bloquant les téléchargements

de virus et les inondations TCP SYN des attaquants. Quel mode de fonctionnement est le meilleur

choix pour répondre à ces exigences ?

A. NAT/route

B. Mode NAT avec une interface en mode renifleur à un bras

C. Mode transparent

D. Il n'existe pas de mode de fonctionnement approprié

445. Quelle affirmation est correcte concernant la création d'une signature personnalisée ?

A. Il doit commencer par le nom

B. Il doit indiquer si le flux de trafic provient du client ou du serveur.

C. Il doit spécifier le protocole. Sinon, elle pourrait accidentellement correspondre à des protocoles de couche inférieure.

D. Il n'est pas pris en charge par le support technique de Fortinet.



446. Quelle vulnérabilité du système d'exploitation pouvez-vous protéger lors de la sélection des

signatures à inclure dans un capteur IPS ? (Choisissez-en trois)

A. Irix

B. ONIX

C. Linux

D. Mac OS

E. BSD

447. Quelle affirmation concernant l'IPS est fausse ?

A. Les paquets IPS contiennent un moteur et des signatures utilisés à la fois par IPS et d'autres scans

basés sur le flux.

B. La topologie à un bras avec le mode renifleur améliore les performances de blocage de l'IPS.

C. IPS peut détecter les attaques de type "zero-day".

D. Le statut de la dernière tentative de mise à jour de service de FortiGuard IPS est indiqué sur System>Config>FortiGuard et dans la sortie de 'diag autoupdate version'.

448. Lequel des énoncés suivants est correct en ce qui concerne la fonction de quarantaine NAC ?

A. Avec la quarantaine NAC, les fichiers peuvent être mis en quarantaine non seulement à la suite

d'une analyse antivirus, mais aussi pour d'autres formes d'inspection du contenu telles que IPS et

DLP.

B. La quarantaine NAC effectue un contrôle client sur les postes de travail avant qu'ils ne soient autorisés à avoir un accès administratif à FortiGate.

C. La quarantaine NAC permet aux administrateurs d'isoler les clients dont l'activité sur le réseau

présente un risque pour la sécurité.

D. Si vous avez choisi l'action de quarantaine, vous devez décider si le type de quarantaine est une quarantaine NAC ou une quarantaine de fichiers.

449. Une organisation souhaite protéger son serveur SIP contre les attaques

par inondation d'appels. unité pour répondre à cette exigence ?

Parmi les modifications de configuration suivantes, lesquelles peuvent être effectuées sur le serveur

FortiGate® ?

A. Appliquer une liste de contrôle d'application qui contient une règle pour SIP et dont l'option

"Limiter les demandes INVITE" est configurée.

B. Activez la mise en forme du trafic pour la politique de pare-feu SIP appropriée.

C. Réduisez la valeur du temps de survie de la session pour le protocole SIP en exécutant la commande CLI configure system session- ttl.

D. Exécutez la commande CLI set udp-idle-timer et définissez une valeur de temps inférieure.

450. Sur votre FortiGate 60D, vous avez configuré des politiques de pare-feu. Elles transfèrent le

trafic vers votre serveur web Linux Apache. Sélectionnez la meilleure façon de protéger votre serveur web en utilisant le moteur IPS.

A. Activer les signatures IPS pour les serveurs Linux avec les protocoles HTTP, TCP et SSL et les applications Apache. Configurer DLP pour bloquer les requêtes HTTP GET avec les numéros de cartes de crédit.

B. Activer les signatures IPS pour les serveurs Linux avec les protocoles HIT, TCP et SSL et les applications Apache. Configurez DLP pour bloquer HTTP GET avec des numéros de carte de crédit.

Configurez également une politique Dos pour empêcher les floods TCP SYN et les scans de port.

C. Aucun. Le FortiGate 60D est un modèle de bureau, qui ne prend pas en charge l'IPS.

**D. Activez les signatures IPS pour les serveurs Linux et Windows avec les protocoles FTP, HTTP, TCP, et SSL et les applications Apache et PHP.**

451. Une administration souhaite limiter le volume total de sessions SMTP sur son serveur de messagerie. Lequel des capteurs DoS suivants peut être utilisé à cette fin ?

A. top port\_scan

**B. ip\_dst\_session**

C. udp\_flood

D. ip\_src\_session

452. Quels sont les changements apportés à IPS qui réduiront l'utilisation des ressources et amélioreront les performances ? (Choisissez-en trois)

**A. Dans la signature personnalisée, supprimez les mots-clés inutiles afin de réduire la longueur de**

**l'arborescence de la signature que FortiGate doit comparer pour déterminer si le paquet est conforme.**

**B. Dans les capteurs IPS, désactivez les signatures et les statistiques basées sur le taux (détection des anomalies) pour les protocoles, les applications et les directions de trafic qui ne**

**sont pas pertinents.**

C. Dans les filtres IPS, passez de "Advanced" à "Basic" pour n'appliquer que les signatures les plus essentielles.

**D. Dans les politiques de pare-feu où l'IPS n'est pas nécessaire, désactivez l'IPS.**

E. Dans les politiques de pare-feu où IPS est utilisé, activez les journaux de début de session.

453. Quel profil le moteur IPS peut-il utiliser sur une interface qui est en mode renifleur ? (Choisissez-en trois)

**A. Antivirus (basé sur le flux)**

**B. Filtrage du Web (basé sur la PROXY)**

C. Protection contre les intrusions

**D. Contrôle des applications**

E. Contrôle des points de terminaison

454. Vous créez une signature personnalisée. Laquelle a une syntaxe incorrecte ?

- A. F-SBID(--attack\_id 1842,--name "Ping. Mort";--protocole imp ; --data\_size>32000 ;
- B. F-SBID(--name "Block.SMTP. VRFY.CMD",-pattern "Vrfy" - service SMTP ; --no\_case;-context header ;
- C. F-SBID(--name "Ping.Death";-protocol icmp;--data\_size>32000 ;)
- D. F-SBID(--name "Block".HTTP.POST" ; --protocol top;-- service HI TP;-- flow from\_client, -pattern 'POST' ; -- context uri;--within 5, context ;)

455. Un administrateur a créé une signature IPS personnalisée. Où la signature IPS personnalisée doit-elle être appliquée ?

- A. Dans un capteur IPS
- B. Dans une interface.
- C. Dans une politique de DoS.
- D. Dans un profil de contrôle d'application.

456. Lequel des processus suivants est impliqué dans la mise à jour de l'IPS de FortiGuard ?

- A. Les demandes de mise à jour du FortiGate IPS sont envoyées en utilisant le port UDP 443.
- B. Les demandes de mise à jour du décodeur de protocole sont envoyées à service.fortiguard.net.
- C. Les demandes de mise à jour des signatures IPS sont envoyées à update.fortiguard.net.
- D. Les mises à jour du moteur IPS ne peuvent être obtenues qu'en utilisant les mises à jour push.

457. Examinez la configuration du capteur IPS présentée dans l'illustration, puis répondez à la question ci-dessous.

Un administrateur a configuré le capteur IPS WINDOS\_SERVERS afin de déterminer si l'afflux de

trafic HTTPS est une tentative d'attaque ou non. Après avoir appliqué le capteur IPS, FortiGate ne

génère toujours pas de journaux IPS pour le trafic HTTPS.

Quelle est la raison possible de ce phénomène ?

- A. Le filtre IPS n'a pas l'option Protocol : HTTPS.
- B. Les signatures HTTPS n'ont pas été ajoutées au capteur.
- C. Une politique DoS devrait être utilisée, au lieu d'un capteur IPS.
- D. Une politique DoS devrait être utilisée, au lieu d'un capteur IPS.
- E. La politique de pare-feu n'utilise pas un profil d'inspection SSL complet.

458. Quels types de trafic et d'attaques peuvent être bloqués par un profil de pare-feu d'application Web (WAF) ? (Choisissez-en trois.)

- A. Trafic vers les serveurs de botnets
- B. Trafic vers des sites web inappropriés
- C. Attaques de divulgation d'informations sur les serveurs
- D. Fuites de données de cartes de crédit
- E. Attaques par injection SQL

459. Vous configurez le FortiGate racine pour mettre en œuvre la structure de sécurité.

Vous

configurez le port 10 pour communiquer avec un FortiGate en aval. Affichez la configuration par défaut

Modifier l'interface dans la pièce ci-dessous :

Lors de la configuration du FortiGate racine pour communiquer avec un FortiGate en aval, quels

paramètres doivent être configurés ? (Choisissez-en deux.)

A. Détection du dispositif activée.

**B. Accès administratif : FortiTelemetry.**

**C. IP/Masque de réseau.**

D. Rôle : Sécurité Fabric.

460. Quelle affirmation décrit le mieux la tâche principale des processeurs d'accélération matérielle

de FortiGate ?

**A. Décharger les tâches de traitement du trafic de l'unité centrale principale.**

B. Décharger les tâches de gestion de l'unité centrale principale.

C. Compresser et optimiser le trafic réseau.

D. Augmenter la bande passante maximale disponible dans une interface FortiGate.

461. Quelle affirmation décrit le mieux l'objectif de la fonction de proxy SYN disponible dans les processeurs SP ?

A. Accélérer la poignée de main tridimensionnelle de TCP

B. Collecter des statistiques sur les sessions de trafic

C. Analyser le paquet SYN pour décider si la nouvelle session peut être transférée au processeur SP.

**D. Protection contre les attaques SYN flood.**

462. Pour les dispositifs FortiGate équipés de puces Network Processor (NP), quelles sont les

réponses vraies ? (Choisissez-en trois.)

**A. Pour chaque nouvelle session IP, le premier paquet va toujours à l'unité centrale.**

B. Le noyau n'a pas besoin de programmer la NPU. Lorsque le NPU voit le trafic, il détermine lui-même s'il peut le traiter.

**C. Une fois déchargé, sauf en cas d'erreur, le NP transmet tous les paquets suivants. L'unité centrale ne les traite pas.**

D. Lorsque le dernier paquet est envoyé ou reçu, tel qu'un signal TCP FIN ou TCP RST, le NP renvoie

cette session à l'unité centrale pour qu'elle soit détruite.

E. Les sessions des politiques pour lesquelles un profil de sécurité est activé peuvent être déchargées

par NP.

463. Deux unités FortiGate avec des processeurs NP6 forment un cluster actif-actif. Le cluster

effectue une inspection du profil de sécurité (UTM) sur tout le trafic utilisateur.

Quelles sont les affirmations vraies concernant les sessions que l'unité maître délègue à l'unité

esclave pour inspection ? (Choisissez-en deux.)

A. Ils sont déchargés sur le NP6 dans l'unité maître.

**B. Ils ne sont pas déchargés sur le NP6 dans l'unité maître.**

**C. Ils sont déchargés sur le NP6 dans l'unité esclave.**

D. Elles ne sont pas déchargées sur le NP de l'unité esclave.

464. Lequel des accélérateurs matériels Fortinet suivants peut être utilisé pour décharger

l'inspection antivirus basée sur les flux ? (Choisissez-en deux.)

- A. SP3
- B. CP8
- C. NP4
- D. NP6

465. Quelles fonctions d'inspection du trafic peuvent être exécutées par un processeur de sécurité (SP) ? (Choisissez-en trois.)

- A. proxy TCP SYN
- B. Aide à la session SIP
- C. Antivirus basé sur un proxy
- D. Correspondance des signatures d'attaque
- E. Filtrage web basé sur le flux

466. Un administrateur utilise le renifleur intégré de FortiGate pour capturer le trafic HTTP entre un

client et un serveur. Cependant, la sortie du renifleur ne montre que les paquets liés à l'établissement et à la déconnexion des sessions TCP. Pourquoi ?

- A. L'administrateur fait tourner le renifleur sur l'interface interne uniquement.
- B. Le filtre utilisé dans le renifleur ne correspond au trafic que dans une seule direction.
- C. Le FortiGate effectue une inspection du contenu.
- D. Le trafic TCP est déchargé sur un NP6.

467. Parmi les énoncés suivants, lesquels décrivent le mieux les principales exigences pour qu'une

session de trafic soit éligible au délestage vers un processeur NP6 ? (Choisissez-en trois.)

- A. Les paquets de session n'ont PAS de balise VLAN 802.1Q.
- B. Il ne s'agit PAS de trafic multicast.
- C. Il ne nécessite PAS d'inspection par proxy
- D. Le protocole de la couche 4 doit être UP, TCP, SCTP ou ICMP,
- E. Il ne nécessite PAS d'inspection basée sur le flux.

468.

Quelle affirmation décrit le mieux ce qu'est un système sur puce (SoC) Fortinet ?

- A. Puce à faible consommation qui fournit une puissance de traitement d'usage général.
- B. Une puce qui combine la puissance de traitement générale avec la technologie ASIC personnalisée de Fortinet.
- C. Puce version allégée (avec moins de fonctionnalités) d'un processeur SP
- D. Puce version légère (avec moins de fonctionnalités) d'un processeur CP

469. Lesquelles des affirmations suivantes sont vraies concernant le trafic accéléré par un processeur NP ? (Choisissez-en deux.)

- A. Les paquets TCP SYN sont toujours traités par le processeur NP.
- B. Les paquets initiaux sont envoyés au processeur NP, où une décision est prise pour savoir si la session peut être déchargée ou non.
- C. Les paquets pour une terminaison de session sont toujours traités par le CPU.
- D. Les paquets initiaux vont à l'unité centrale, où une décision est prise pour savoir si la session peut être déchargée ou non.

470. Quelle est l'une des conditions à remplir pour décharger le chiffrement et le déchiffrement du trafic IPsec sur un processeur NP6 ?

A. aucun profil de protection ne peut être appliqué sur le trafic IPsec.

B. L'anti-répétition de phase 2 doit être désactivée.

**C. La phase 2 doit avoir un algorithme de cryptage supporté par le NP6.**

D. Le trafic IPsec ne doit pas être inspecté par un assistant de session FortiGate.

471. Quelle affirmation décrit le mieux l'objectif de la fonction de proxy SYN disponible dans les processeurs SP ?

A Accélérer la poignée de main tridimensionnelle de TCP

B. Collecter des statistiques sur les sessions de trafic

C. Analyser le paquet SYN pour décider si la nouvelle session peut être transférée au processeur SP.

**D. Protéger contre les attaques SYN flood.**

472. Parmi les fonctions de mise en forme du trafic suivantes, lesquelles peuvent être déchargées

sur un processeur NF ? (Choisissez-en deux.)

A. Priorité aux quais

B. Plafonnement du trafic (limite de la bande passante)

**C. Services différenciés - réécriture sur le terrain**

**D. Garantie de la bande passante**

473. Quelle affirmation décrit le mieux ce qu'est un système sur puce (SoC) Fortinet ?

A. Puce à faible consommation qui fournit une puissance de traitement d'usage général.

**B. Une puce qui combine la puissance de traitement générale avec la technologie ASIC personnalisée de Fortinet.**

C. Puce version allégée (avec moins de fonctionnalités) d'un processeur SP

D. Puce version légère (avec moins de fonctionnalités) d'un processeur CP

474. Quelles sont les affirmations vraies concernant le déchargement de l'inspection antivirus vers un processeur de sécurité (SP) ? (Choisissez-en deux.)

A. L'inspection basée sur le proxy et l'inspection basée sur le flux sont toutes deux prises en charge.

**B. Un message de remplacement ne peut pas être présenté aux utilisateurs lorsqu'un virus a été détecté.**

**C. Il permet d'économiser les ressources du processeur,**

D. Les interfaces d'entrée et de sortie peuvent se trouver dans des SP différents.

475. Quels paquets IP peuvent être accélérés matériellement par un processeur NP6 ? (Choisissez-en deux.)

A. Paquets fragmentés.

**B. Paquet multicast.**

**C. Paquet SCTP.**

D. Paquet

GRE. 476.

Lesquelles des affirmations suivantes sont vraies concernant l'équilibrage de la charge des liaisons WAN ? (Choisissez-en deux).

**A. Il ne peut y avoir qu'un seul lien WAN virtuel par VDOM.**

B. FortiGate peut mesurer la qualité de chaque lien en fonction de la latence, de la gigue ou du pourcentage de paquets.

**C. Les vérifications de l'état des liaisons peuvent être effectuées sur chaque membre de la liaison si l'interface WAN virtuelle.**

D. Les valeurs de distance et de priorité sont configurées dans chaque membre de la liaison si l'interface WAN virtuelle

477. Lors de l'utilisation de SD-WAN, comment configurer l'adresse de passerelle du prochain saut

pour une interface membre afin que FortiGate puisse transférer le trafic Internet ?

A. Il doit être configuré dans une route statique en utilisant l'interface virtuelle swan.

**B. Il doit être fourni dans la configuration de l'interface membre du SD-WAN.**

C. Il doit être configuré dans un policy-route en utilisant l'interface virtuelle swan.

D. Il doit être appris automatiquement par un protocole de routage dynamique.

478. Examinez cette sortie d'un flux de débogage :

Quelles sont les affirmations correctes concernant la sortie ? (Choisissez-en deux.)

A. Le paquet a été autorisé par la politique du pare-feu avec l'ID 00007£cO.

**B. La FortiGate a acheminé le paquet par le port3.**

C. FortiGate a reçu un paquet TCP SYN/ACK.

**D. L'adresse IP source du paquet a été traduite en 10.0.1.10.**

479 Visualisez la pièce à conviction. Pourquoi l'administrateur obtient-il l'erreur montrée dans la pièce jointe ?

A. L'administrateur admin ne dispose pas des privilèges nécessaires pour configurer les paramètres globaux.

**B. Les paramètres globaux ne peuvent pas être configurés à partir du contexte du VDOM racine.**

C. La commande config system global n'existe pas dans FortiGate.

D. L'administrateur doit d'abord entrer la commande edit global

480. Dans quels états du processus est-il impossible d'interrompre un processus ?

(Choisissez

A. S-Sleep

B. R-Running

C. D-Sommeil ininterrompu

D. Z-Zombie

481. Examinez la sortie suivante de la commande diagnose sys session list :

Quelles sont les affirmations vraies concernant la session ci-dessus ?

(Choisissez-en deux.)

A. Le Time-To-Live (TTL) de la session a été configuré à 9 secondes.

B. La FortiGate effectue la NAT des adresses IP source et destination sur tous les paquets provenant

de l'adresse 192.168.1. 110.

**C. L'adresse IP 192.168.1.110 est traduite en 172.17.87.16.**

**D. Le FortiGate ne traduit pas les numéros de port TCP des paquets de cette session.**

482. La pièce à conviction montre une partie de la sortie de la commande de diagnostic

'diagnose debug application ike 255', prise pendant l'établissement d'un VPN. Laquelle des affirmations suivantes est correcte concernant cette sortie ? (Choisissez-en deux)

A. Les sélecteurs de mode rapide négociés entre les deux pairs VPN IPsec sont 0.0.0.0/32 pour les

adresses source et destination.

B. La sortie correspond à une négociation de phase 2

C. NAT-T activé et il y a un troisième dispositif sur le chemin qui effectue le NAT du trafic entre les

deux peers VPN IPsec.

D. L'adresse IP du peer VPN IPsec distant est 172.20.187.114

483. Un administrateur réseau connecte son PC à l'interface INTERNAL d'une unité FortiGate.

L'administrateur tente d'établir une connexion HTTPS avec l'unité FortiGate sur l'interface VLAN1 à

l'adresse IP de 10.0.1.1, mais n'obtient aucune connectivité.

Les commandes de dépannage suivantes sont exécutées à partir de l'invite DOS du PC et de la CLI.

D'après les résultats de ces commandes, laquelle des explications suivantes est une cause possible

du problème ?

A. L'unité Fortigate n'a pas de route de retour vers le PC.

B. Le PC a une adresse IP dans le mauvais sous-réseau.

C. Le PC utilise une adresse IP de passerelle par défaut incorrecte.

D. Le service HTTPS n'est pas configuré sur l'interface VLAN1 de l'unité FortiGate.

E. Il n'y a pas de politique de pare-feu permettant le trafic de INTERNAL-> VLAN1

484. Quelles sont les sorties de la commande 'diagnose hardware deviceinfo nic' ? (Choisissez-en deux.)

A. Cache ARP

B. Adresse MAC physique

C. Erreurs et collisions

D. Ports TCP à l'écoute

485. Quels sont les exemples de syntaxe correcte pour la commande de diagnostic des tables de

session ? (Choisissez-en deux.)

A. diagnose s sys filtre de session clair

B. diagnose sys session sc 10.0.1.254

C. diagnostiquer le filtre de session sys

D. diagnostiquer sys session filter list dst.

486. La commande diag sys session list est exécutée dans l'interface CLI. La sortie de cette commande est illustrée dans la pièce.

D'après le résultat de cette commande, laquelle des affirmations suivantes est correcte ?

A. Il s'agit d'une session UDP.

B. La mise en forme du trafic est appliquée à cette session.

C. Il s'agit d'une session ICMP

D. Ce trafic a été authentifié.

E. Cette session correspond à une politique de pare-feu avec l'ID 5.

487. Dans la sortie de la commande de débogage présentée dans l'illustration, lequel des éléments



suivants décrit le mieux l'adresse MAC 00:09:0:69:03:7e ?

§ diagnostic de la liste ip arp

index=2 1fnamemportl 172.20.187.150 00:09:0:69:03:7e state 00000004 use=4589 confirm 4589

update=2422 ref=1

A. C'est l'une des adresses MAC secondaires de l'interface port1.

B. Il s'agit de l'adresse MAC primaire de l'interface du port.

C. Il s'agit de l'adresse MAC d'un autre périphérique réseau situé dans le même segment de réseau local que l'interface du port 1 de l'unité FortiGate.

D. Il s'agit de l'adresse MAC virtuelle HA.

488. Regardez la pièce à conviction. Le client ne peut pas se connecter au serveur Web HTTP.

L'administrateur exécute le renifleur intégré de FortiGate et obtient le résultat suivant :

FortiGate # diagnose sniffer packet any "port 80" 4 interfaces= [any] filter= [port 80]

11.510058 port3 in 10.0.1.10.49255 -> 10.200.1.254.80 : syn 697263124

11.760531 port dans 10.0.1.10.49255 -> 10.200.1.254.80 : gyn 868017830

14.505371 port3 dans 10.0.1.10.49255 -> 10.200.1.254.80 : n 697263124

14.755510 port3 dans 10.0.1.10.49255 -> 10.200.1.254.80 : gyn 868017830

Que faut-il faire ensuite pour résoudre le problème ?

A. Exécutez un autre sniffer dans le FortiGate, cette fois-ci avec le filtre "host 10.0.1.10".

B. Lancez un sniffer dans le serveur web.

C. Capturez le trafic en utilisant un renifleur externe connecté au port 1.

D. Exécuter un flux de débogage.

489. Examinez cette sortie de la commande diagnose sys top :

Quelles affirmations concernant la sortie sont vraies ? (Choisissez-en deux.)

A. sshd est le processus qui consomme le plus de mémoire

B. ssh est le processus qui consomme le plus de CPU

C. Tous les processus listés sont en état de sommeil

D. Le processus ssh utilise 123 pages de mémoire.

490. Un administrateur utilise le renifleur intégré de FortiGate pour capturer le trafic HTTP entre un

client et un serveur. Cependant, la sortie du renifleur ne montre que les paquets liés à l'établissement et à la déconnexion des sessions TCP. Pourquoi ?

A. L'administrateur fait tourner le renifleur sur l'interface interne uniquement.

B. Le filtre utilisé dans le renifleur ne correspond au trafic que dans une seule direction.

C. Le FortiGate fait une inspection du contenu

D. Le trafic TCP est déchargé sur un NP6.

491. Revoir l'article

Examinez la sortie des diagnostics IPsec de la commande diagnose vpn tunnel 11st montrée dans

l'illustration ci-dessous.

Quelles sont les affirmations correctes concernant cette sortie (Choisissez-en deux.)

A. L'adresse 172.20.1.1 a été attribuée au client qui se connecte.

B. Dans les paramètres de la phase 1, la détection des pairs morts est activée. 7 C. Le tunnel est inactif.

• D. L'adresse 10.200.3.1 a été attribuée au client qui se connecte.

492. Quels sont les composants de la FortiGate qui sont testés lors du test matériel ? (Choisissez-en

trois.)

- A. Accès administratif
- B. Battement de cœur HA

**C. CPU**

**D. Disque dur**

**E. Interfaces réseau**

493. Examinez cette sortie d'un flux de débogage :

```
id=20085 trace_id=1 func=print_pkt_detail line=5363 msg="vd-root a reçu un paquet  
(proto=1,  
10.0.1.10:1->10.200.1.254:2048)
```

```
du port3. type=8, code=0, id=1, seg=33."
```

```
id=20085 trace id=1 func=init_ip_session_common line=5519 msg="allouer une nouvelle  
session=00000340
```

```
id=20085 trace id=1 func=vf_ip_route_input_common line=2583 msg="trouver une route :  
flag=04000000 gw=10.200.1.254
```

```
portin
```

```
id=20085 trace_id=1 func=fk_forward_handler line=586 msg="Refusé par la vérification de  
la
```

```
politique de transmission (politique 0)*.
```

Pourquoi le FortiGate a-t-il laissé tomber le paquet ?

- A. L'adresse IP du prochain saut est inaccessible.
- B. Il a échoué à la vérification RPF.
- C. Il correspondait à une politique de pare-feu explicitement configurée avec l'action DENY.

**D. Il correspondait à la politique implicite du pare-feu par défaut.**

494. Examinez la pièce à conviction, qui contient une sortie de diagnostic de session.

Laquelle des affirmations suivantes concernant la sortie de diagnostic de la session est vraie ?

**A. La session est dans l'état ESTABLISHED.**

- B. La session est en état LISTEN.
- C. La session est en état d'ATTENTE DE TEMPS.
- D. La session est en état d'ATTENTE FERMÉE.

495. Lesquelles des affirmations suivantes concernant la sauvegarde des journaux à partir de

l'interface CLI et le téléchargement des journaux à partir de l'interface graphique sont vraies ?

(Choisissez-en deux.)

**A. Les téléchargements de journaux à partir de l'interface graphique sont limités à la vue du filtre en cours.**

**B. Les sauvegardes de journaux effectuées à partir de l'interface CLI ne peuvent pas être restaurées sur un autre FortiGate.**

C. Les sauvegardes de journaux à partir de l'interface CLI peuvent être configurées pour être téléchargées sur FTP à une heure programmée.

D. Les téléchargements de journaux depuis l'interface graphique sont stockés dans des fichiers compressés LZ4.

Quelles commandes sont appropriées pour enquêter sur les CPU élevées ?  
(Choisissez-en deux.) 496.

A. diag sys top

B. diag hardware s sysinfo mem

C. diag debug flow

D. obtenir l'état des performances du système

497. Dans le journal d'un Crash, qu'indique un statut de 0 ?

A. Arrêt anormal d'un processus

B. Un processus fermé pour une raison quelconque

C. Le processus Scanunitd s'est écrasé

D. Arrêt normal sans anomalie

E. Le processus DHCP s'est planté

498. Examinez la pièce à conviction, qui montre la sortie partielle d'un débogage

IKE en temps réel Laquelle des affirmations suivantes concernant la sortie est vraie ?

A. Le VPN est configuré pour utiliser l'authentification par clé pré-partagée.

B. L'authentification étendue (XAuth) a réussi.

C. Remote est le nom d'hôte de l'homologue IPsec distant.

D. La phase 1 est tombée.

499. Quelle affirmation décrit correctement la sortie de la commande diagnose ips anomaly list ?

A. Liste la politique DoS configurée.

B. Liste les compteurs en temps réel pour la politique DoS configurée.

C. Liste les erreurs capturées lors de la compilation de la politique DoS.

D. Liste les correspondances des signatures IPS.

500. Examinez la sortie de débogage IKE pour IPsec présentée dans l'illustration ci-dessous. Quelle

est l'affirmation correcte concernant cette sortie ?

A. Le résultat est une négociation de phase 1.

B. Le résultat est une négociation de phase 2.

C. La sortie capture les messages de détection des pairs morts.

D. La sortie capture les paquets de détection de passerelle morte.

501. Comment configurer un FortiGate pour appliquer la mise en forme du trafic au trafic P2P, tel que BitTorrent ?

A. Appliquer une mise en forme du trafic à une entrée Bit Torrent dans une liste de contrôle des

applications, qui est ensuite appliquée à une politique de pare-feu.

B. Activez l'option de forme dans une politique de pare-feu dont le service est réglé sur BitTorrent.

C. Définissez une règle DLP qui correspond au trafic Bit Torrent et incluez la règle dans un capteur DLP avec la mise en forme du trafic activée.

D. Appliquer une mise en forme du trafic à un profil d'options de protocole.

502. La figure ci-dessous est une capture d'écran d'un profil de contrôle d'application. Les différents

paramètres sont entourés et numérotés. Sélectionnez le numéro identifiant le paramètre qui fournira des informations supplémentaires sur l'accès à YouTube, comme le nom de la vidéo regardée.

- A. 1
- B. 2
- C. 3
- D. 4**
- E. 5

503. Comment les signatures de contrôle des applications sont-elles mises à jour sur un appareil FortiGate ?

- A. Grâce aux mises à jour de FortiGuard.**
- B. Mettez à niveau le micrologiciel FortiOS vers une version plus récente.
- C. En exécutant la fonction d'apprentissage automatique du Contrôle des applications.
- D. Les signatures sont codées en dur sur l'appareil et ne peuvent pas être mises à jour.

504. Quelle réponse décrit le mieux ce qu'est une "application inconnue" ?

- A. Tout le trafic qui correspond à la signature interne pour les applications inconnues.
- B. Le trafic qui ne correspond pas au modèle RFC pour son protocole.

**C. Tout trafic qui ne correspond pas à une signature de contrôle d'application**

D. Un paquet qui échoue au contrôle CRC.

505. A. Avertissez

**B. Autoriser**

**C. Bloc**

D. Modélisation du trafic

**E. Quarantaine**

Quelles actions sont possibles avec le Contrôle des applications ? (Choisissez-en trois.)

506. Un utilisateur derrière la FortiGate essaie d'aller sur (Addicting.Games). Sur la base de cette

configuration, quelle affirmation est vraie ?

Jeux addictifs

Jeux - Jeux gratuits en ligne sur Addicting Games

Jouez à des milliers de jeux en ligne gratuits : jeux d'arcade, jeux de réflexion, jeux amusants, jeux

de sport, jeux de tir, et plus encore. De nouveaux jeux gratuits tous les jours sur AddictingGames.

**A. Addicting. Games est autorisé en fonction de la configuration de l'Application Overrides.**

B. Addicting.Games est bloqué en fonction de la configuration de Filter Overrides.

C. Addicting.Games ne peut être autorisé que si l'action Filter Overrides est définie sur Exempt.

D. Addicting.Games est autorisé en fonction de la configuration des catégories.

507. Quelles déclarations concernant le contrôle des applications sont vraies ? (Choisissez-en deux.)

A. L'activation du profil de contrôle des applications dans un profil de sécurité permet le contrôle des applications pour tout le trafic passant par la FortiGate.

B. Il ne peut pas agir sur des demandes inconnues.

**C. Il peut inspecter le trafic crypté.**

**D. Il peut identifier le trafic d'applications connues, même lorsqu'elles utilisent des ports TCP/UDP**

**non standard.**

508. Quelles sont les affirmations vraies concernant la mise en forme du trafic qui est appliquée dans un capteur d'application et associée à une politique de pare-feu ? (Choisissez-en deux.)

- A. La mise en forme du trafic partagé ne peut pas être utilisée.
- B. Seul le trafic correspondant à la signature de contrôle des applications est mis en forme.
- C. Peut limiter l'utilisation de la bande passante des applications à fort trafic.
- D. La mise en forme du trafic par IP ne peut pas être utilisée.

509. Lesquels des énoncés suivants sont vrais concernant le contrôle des applications ? (Choisissez-en deux.)

- A. Le contrôle des applications est basé sur les numéros de port de destination TCP.
- B. Le contrôle des applications est basé sur le proxy.
- C. Le trafic crypté peut être identifié par le contrôle des applications.
- D. La mise en forme du trafic peut être appliquée au trafic d'application détecté.

510. La figure ci-dessous est une capture d'écran d'un profil de contrôle d'application. Les différents paramètres sont entourés et numérotés. Sélectionnez le numéro identifiant le paramètre qui fournira des informations supplémentaires sur l'accès à YouTube, comme le nom de la vidéo regardée.

- A. 1
- B. 2
- C. 3
- D. 4
- E. 5

511. Quelle action peut être appliquée à chaque filtre du profil de contrôle des applications ?

- A. Blocage, surveillance, alerte et mise en quarantaine
- B. Autoriser, surveiller, bloquer et apprendre
- C. Autoriser, bloquer, authentifier et avertir
- D. Autoriser, surveiller, bloquer et mettre en quarantaine.

512. Visualisez la pièce à conviction. Sur la base de la configuration présentée dans la pièce,

quelles sont les affirmations vraies concernant le comportement du contrôle des applications ? (Choisissez-en deux.)

- A. L'accès à toutes les applications inconnues sera autorisé.
- B. L'accès aux applications Social.Media basées sur un navigateur sera bloqué.
- C. L'accès aux applications mobiles de médias sociaux sera bloqué.
- D. L'accès à toutes les applications de la catégorie Social. Media sera bloqué.

## 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 ?

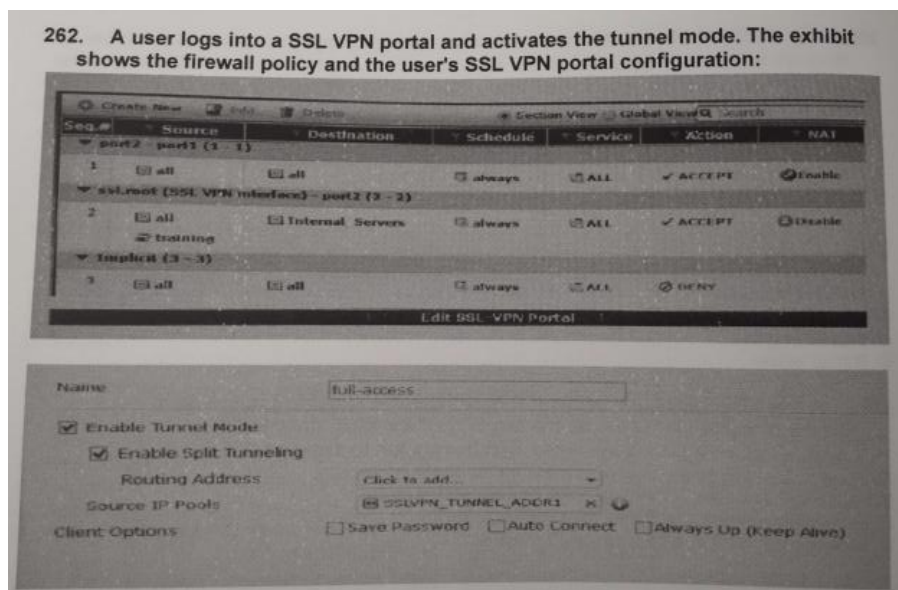
L'appareil FortiGate agit comme une sous-autorité de certification

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.

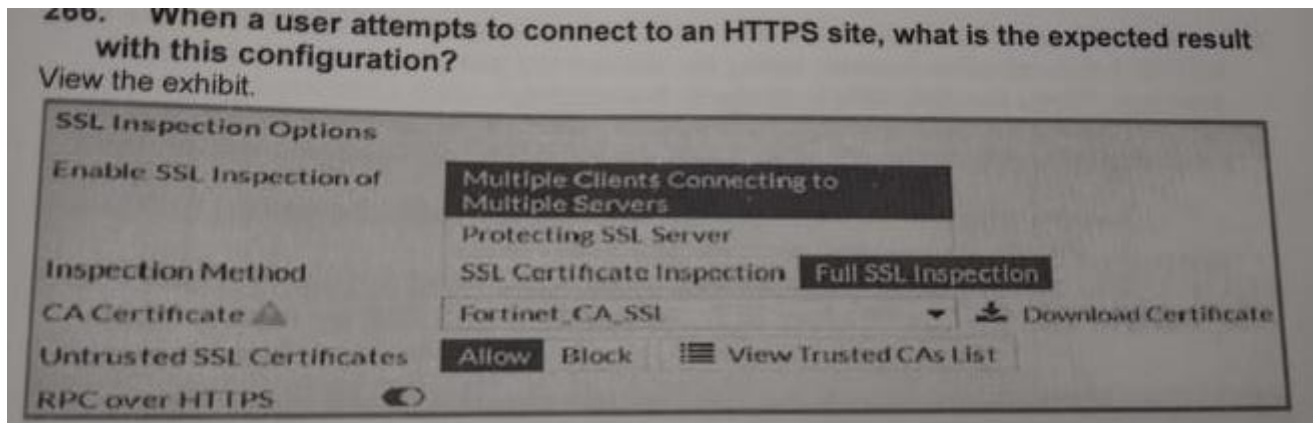
264. Lesquels des agents FSSO suivants sont requis pour une solution en mode agent DC ?

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 ?

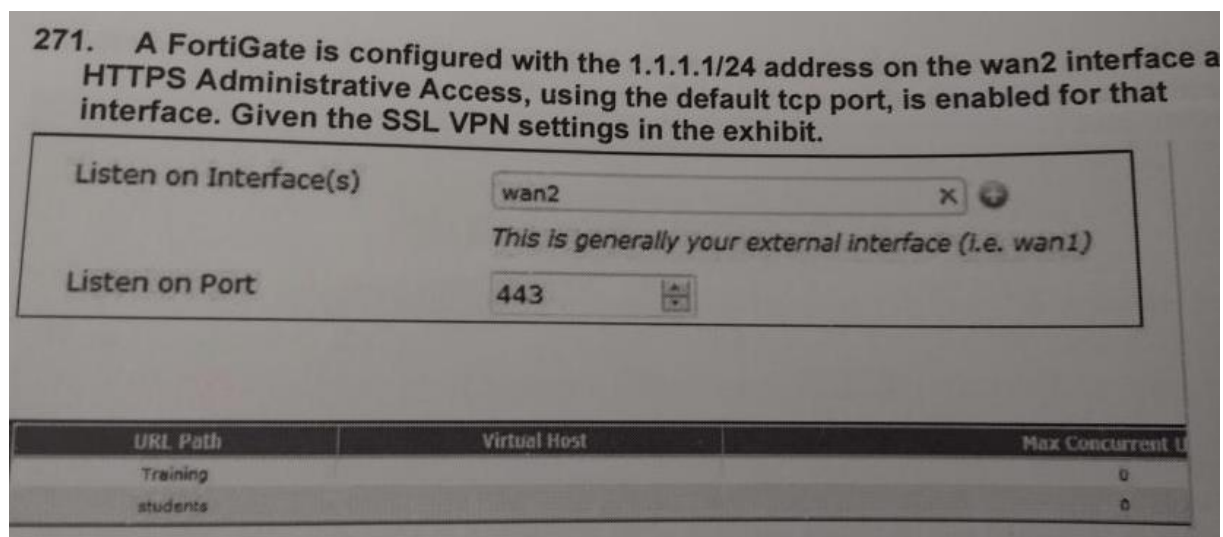
L'adresse IP interne de l'unité FortiGate.

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

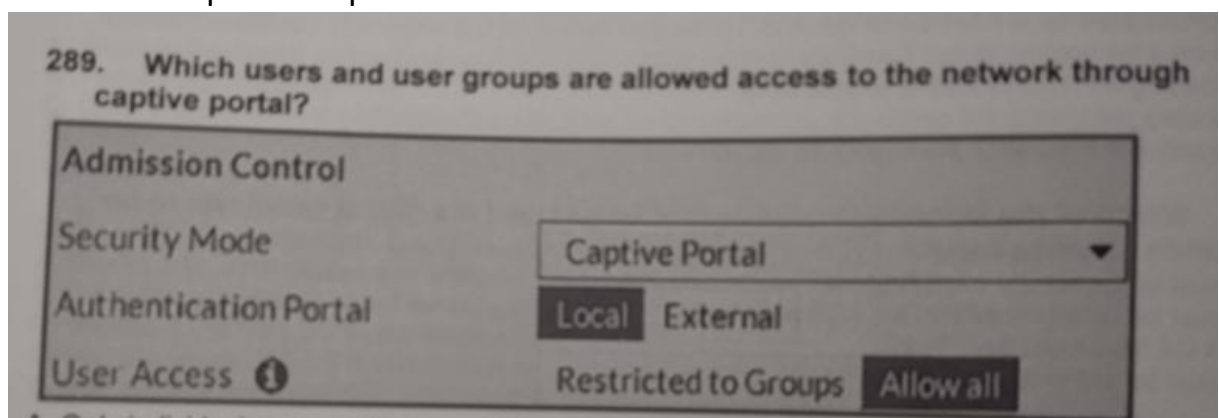
Téléchargement d'un fichier PKCS#12 sur un serveur TFTP

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 checked="" type="checkbox"/>	2	all	all	always	ANY	ACCEPT
ssl.root -> wan1 (1)	<input checked="" type="checkbox"/>	3	all	all	always	ANY	ACCEPT
wan1 -> internal (1)	<input checked="" type="checkbox"/>	1	all	all	always	ANY	SSL-VPN
Implicit (1)							

**B.**

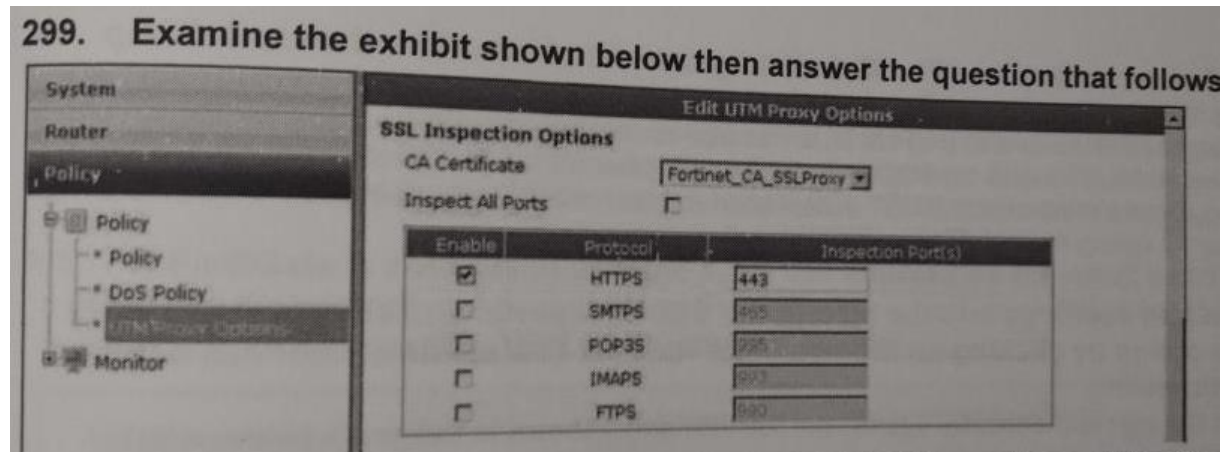
	Status	ID	Source	Destination	Schedule	Service	Action
ssl.root -> internal (1)	<input checked="" type="checkbox"/>	2	all	all	always	ANY	ACCEPT
ssl.root -> wan1 (1)	<input checked="" type="checkbox"/>	3	all	all	always	ANY	ACCEPT
wan1 -> internal (1)	<input checked="" type="checkbox"/>	1	all	all	always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

**C.**

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

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

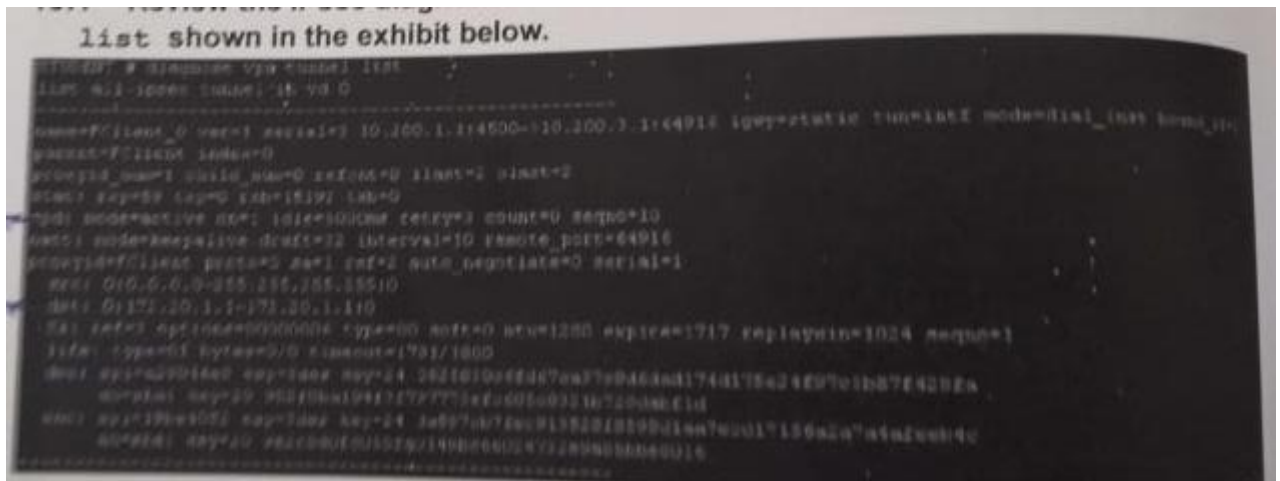
statement below identifies the route that is added to the client's routing table.

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".



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

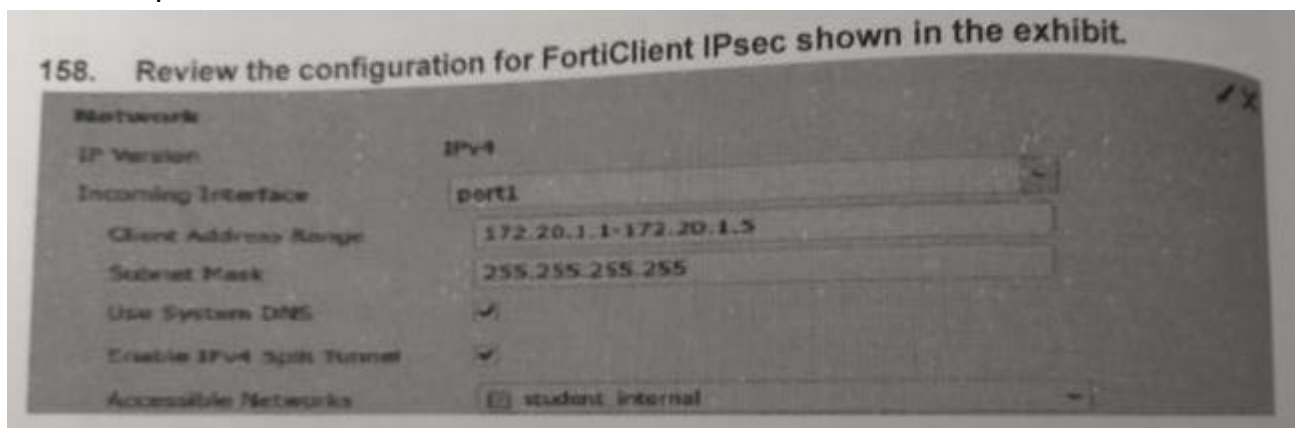


Quelles déclarations sont correctes concernant cette sortie ?

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 pare-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 ?

176. Which of the following statements are correct concerning the IPsec phase 1 and phase 2, shown in the exhibit? (choose two)

Peer Options

Accept Types: This peer ID

Peer ID: fortinet

Phase 1 Proposal

Encryption: 3DES Authentication: SHA1

Diffie-Hellman Groups: 21, 20, 19, 18, 17, 16, 15, 14, 5, 2, 1

Key Lifetime (seconds): 86400

Local ID:

XAUTH

Type: Disabled

Phase 2 Selectors

Name	Local Address	Remote Address
	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0

A. The quick mode selector in the remote site must also be 0.0.0.0/0 for the source and destination

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 ?

181. View the exhibit. Which of the following statements are correct? (Choose two.)

The screenshot shows two IPsec tunnel configurations. TunnelB has a destination of 172.13.24.0/255.255.255.0 and an administrative distance of 5. TunnelA has a destination of 172.13.24.0/255.255.255.0 and an administrative distance of 10. Both tunnels are enabled.

Destination	Subnet	Named Address	Internet Service
Device	172.13.24.0/255.255.255.0		
Administrative Distance	5		
Comments			
Status	Enabled	Disabled	
Advanced Options			
Priority	30		

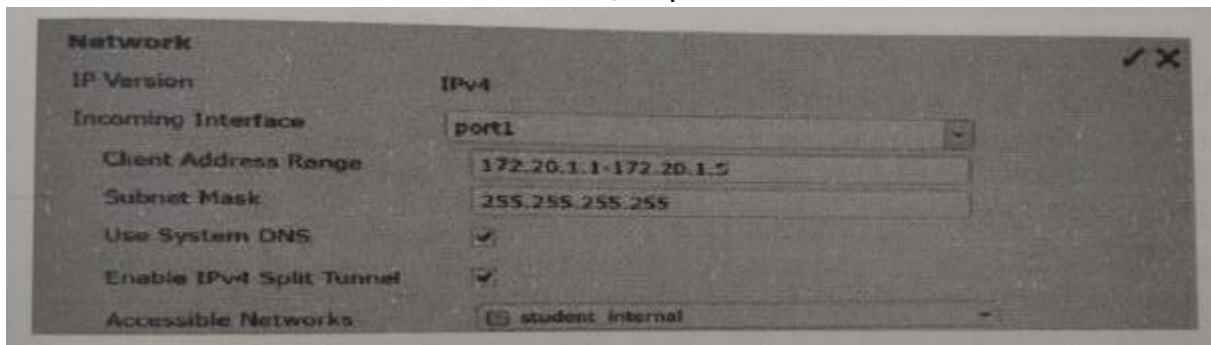
  

Destination	Subnet	Named Address	Internet Service
Device	172.13.24.0/255.255.255.0		
Administrative Distance	10		
Comments			
Status	Enabled	Disabled	
Advanced Options			
Priority	0		

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 ?

Créer 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 ?

question following is related to the configuration? (Select all that apply).

New Phase 1

Name: Remote\_1

Comments: [Empty] 0/255

Remote Gateway: Static IP Address

IP Address: 10.200.3.1

Local Interface: port1

Mode: ☐ Aggressive ☒ Main (ID protection)

Authentication Method: Preshared Key

Pre-shared Key: [Empty]

Peer Options: ☒ Accept any peer ID

Advanced... (XAUTH, NAT Traversal, DPD)

☒ Enable IPsec Interface Mode

IKE Version: ☒ 1 ☐ 2

Local Gateway IP: ☒ Main Interface IP ☐ Specify [Empty]

P1 Proposal

1 - Encryption: AES192 Authentication: SHA1

DH Group: 1 ☐ 2 ☐ 5 ☒ 14 ☐

Keylife: 65500 (120-172800 seconds)

Local ID: [Empty] (optional)

XAUTH: ☒ Disable ☐ Enable as Client ☐ Enable as Server

NAT Traversal: ☒ Enable

Keepalive Frequency: 10 (10-900 seconds)

Dead Peer Detection: ☒ Enable

A. The phase 1 is for a route-based VPN.

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

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

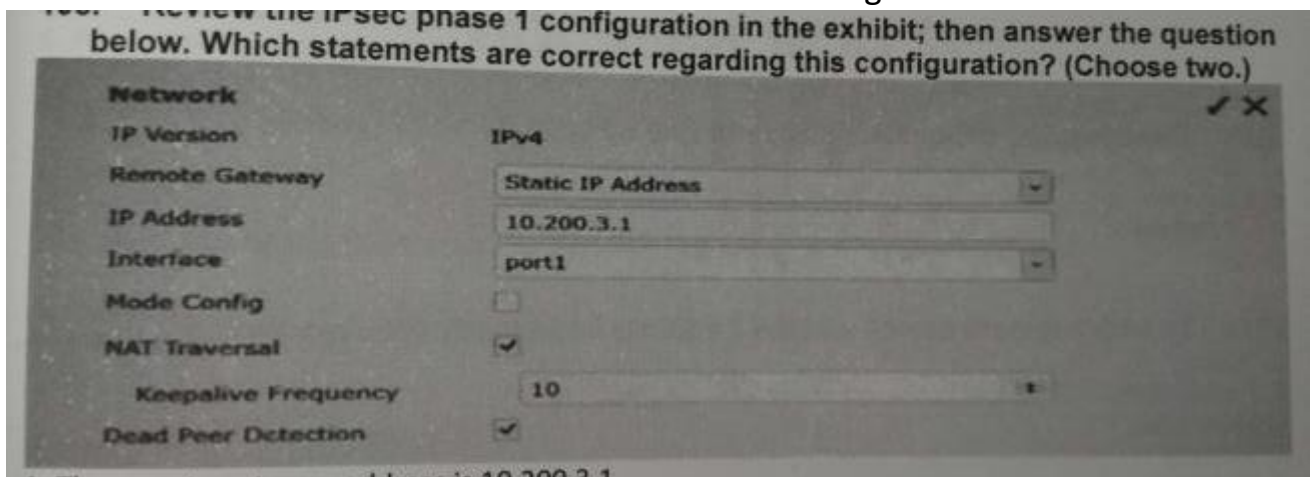


197. Passez en revue la configuration de route statique pour IPsec présentée dans l'image au-dessus ; puis répondez à la question ci-dessous. Quelles affirmations sont correctes concernant cette configuration ?

L'interface distante est une interface IPsec.

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

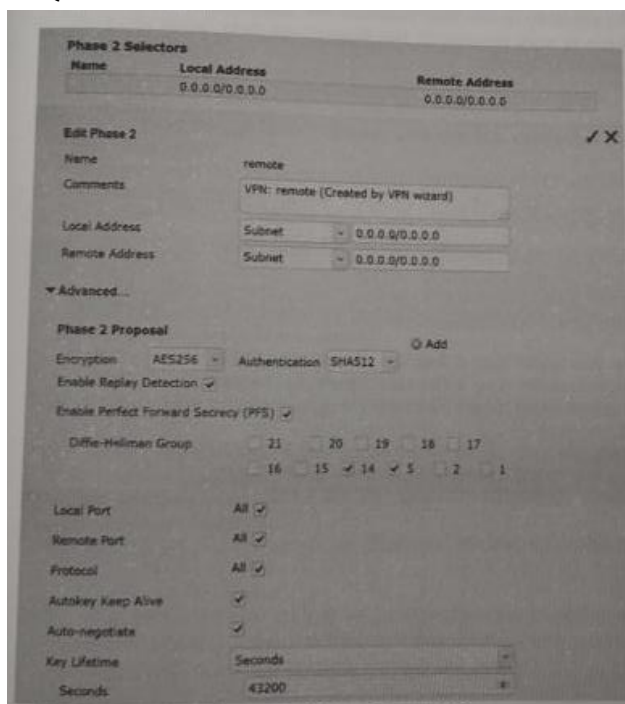
198. Passez en revue la configuration IPsec phase 1 dans l'image. Quelles déclarations sont correctes concernant cette configuration ?



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.



# Cybersec-exam-juin22

## Question 1

*L'administrateur d'un FortiGate avec le profil super\_admin configure un domaine virtuel (VDOM) pour un nouveau client. Après avoir créé le VDOM, l'administrateur ne peut pas réaffecter l'interface dmz au nouveau VDOM car l'option est grisée dans l'interface graphique du VDOM de gestion. Quelle serait la cause possible de ce problème ?*

L'interface dmz est référencée dans la configuration d'un autre VDOM.

## Question 2

*Lors de la configuration de la NAT, quelle affirmation est vraie au sujet d'un pool IP de type « One-to-One » ?*

Il n'utilise pas la Port Address Translation (PAT).

## Question 3

*Quelle mesure est prise par le FortiGate à l'expiration du minuteur lié au « link health monitor » ?*

Toutes les routes utilisant la passerelle (next-hop) configurée dans le « link health monitor » sont supprimées de la table de routage.

## Question 4

*Quelle proposition peut correspondre au paramètre « Services » d'une règle de pare-feu ?*

DNS

## Question 5

*Un fichier de sauvegarde commence par la ligne affichée ci-dessous.*

*#config-version=FGVM64-5.02-FW-build589-140613*

*Pouvez-vous le restaurer sur un FortiWifi 60D ?*

Modèle de périphérique – Version du Firmware – N° build

Non

### Question 6

*Quelle affirmation ne correspond pas à la Fortinet Security Fabric*

Diminue les risques notamment grâce à la corrélation des menaces et aux échanges d'alertes.

Réservée aux équipements Fortinet.

Capable de couvrir l'ensemble de la surface d'attaque du réseau, de l'IoT jusqu'au Cloud.

Permet d'avoir une vue d'ensemble de tous les points d'infiltration potentiels et de coordonner les défenses.

### Question 7

*Laquelle des affirmations suivantes est correcte en ce qui concerne les fichiers journaux (log) ?*

La section « en-tête » aura les mêmes champs pour chaque log ;

La section « corps » d'un log changent en fonction du type de log

### Question 8

*Quelle protocole faut-il utiliser pour l'accès administratif à un FortiGate ?*

SSH

### Question 9

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

ESP

### Question 10

*Quelle affirmation est fausse concernant le routage basé sur des règles (Policy-based routing)*

Les règles ne sont pas lues selon l'ordre séquentiel mais selon la meilleure correspondance.

### Question 11

*Quel élément est utilisé pour signer un certificat serveur ?*

La clé privée d'une autorité de certification.

## Question 12

*Quelle affirmation est fausse en ce qui concerne les domaines virtuels FortiGate (VDOM) ?*

S'il y a des VDOM, on peut sauvegarder leur configuration individuellement.

Tout le trafic généré par le FortiGate lui-même provient du VDOM de gestion.

**Le même compte administrateur doit être utilisé pour la gestion des différents VDOM d'un FortiGate.**

Chaque interface est membre d'un seul VDOM.

## Question 13

*Quelle affirmation est fausse en ce qui concerne les domaines virtuels FortiGate (VDOM) ?*

L'interface sur laquelle un paquet arrive détermine quel VDOM traite le trafic.

En mode multi-ldom, n'importe quel VDOM peut être configuré pour être le VDOM de gestion.

**Des règles de pare-feu ne sont pas nécessaires pour autoriser le trafic entrant par les liens inter-ldom.**

Des comptes administrateurs différents peuvent être attribués à la gestion de différents VDOM.

## Question 14

*Quelle affirmation est fausse en ce qui concerne les domaines virtuels FortiGate (VDOM) ?*

Le mode Split-ldom contient 2 VDOM prédéfinis : VDOM Root et VDOM FG-Traffic.

Pour interconnecter deux VDOM à l'aide d'un VDOM-link, au moins un des VDOM doit fonctionner en mode NAT/route.

Par défaut le VDOM racine joue le rôle de VDOM de gestion.

**Le mode multi-VDOM permet d'allouer les ressources de telle sorte que le Fortigate peut utiliser plus de quantité de mémoire que la quantité de mémoire physiquement disponible.**

### Question 15

*Quel est le processus de récupération de mot de passe sur un FortiGate ?*

Se connecter en mode console en utilisant le compte « maintenir » dans les quelques secondes qui suivent la mise sous tension physique du FortiGate, puis entrer les commandes de réinitialisation du mot de passe administrateur.

### Question 16

*D'après les informations fournies, quelle affirmation est fausse si la protection contre l'usurpation d'adresse IP (Reverse Path Forwarding Check, RPF) est configurée en **mode loose** ?*

*Mode loose : Paquet accepté tant qu'il y a une route active vers IP source via interface entrante.*

*Mode stricte : Route active vers IP source vers interface entrante et si route = meilleur chemin possible*

*Le paquet IP dont l'IP source est 150.142.15.73 et l'IP destination est 10.0.3.17 arrivant sur l'interface Wan2 est bloqué par la fonction RPF.*

### Question 17

*Quelle proposition n'est pas une fonction d'un FortiGate ?*

Contrôle d'application

Inspection SSL/SSH

**Audit d'une base de données**

Prévention de la fuite de données (DLP, data leak prevention)

Prévention des intrusions

Antivirus

### Question 18

*Quel type de VPN est utilisé pour connecter des télétravailleurs à un intranet ?*

Dial-up VPN

### Question 19

*Quelle méthode de translation d'adresse n'existe pas en mode Firewall Policy NAT ?*

*IP pool type : One-to-many*

### Question 20

*Quelle proposition est une caractéristique du mode « Firewall Policy NAT »*  
SNAT et DNAT doivent être configurés pour chaque règle du pare-feu.

### Question 21

*Laquelle des combinaisons suivantes de deux configurations de FortiGate (côté A et côté B), peut être utilisée pour établir avec succès un VPN IPsec entre elles ?*

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.

### Question 22

*Un administrateur veut créer un tunnel VPN IPsec entre 2 périphériques FortiGate. Quelle proposition n'est pas une étape de configuration qui doit être effectuée sur les 2 périphériques ?*

Configurer le mode de fonctionnement en mode VPN IPsec.

### Question 23

*Quelle proposition n'est pas un type de journal utilisé sur un Fortigate ?*

Event Log

Security Log

Traffic Log

Syslog

#### Question 24

*Quelle affirmation est fausse concernant la correspondance des sources dans une règle de pare-feu ?*

Un périphérique source **doit** nécessairement être sélectionné dans une règle de pare-feu (il ne doit pas, il peut, pareil pour user)

#### Question 25

*Quel champ d'en-tête peut être utilisé dans une règle de pare-feu pour la correspondance du trafic ?*

Le type et le code ICMP

#### Question 26

*En sécurité informatique, quel terme signifie que les informations contenues dans un système informatique ne peuvent être modifiées que par les personnes autorisées ?*

L'intégrité

#### Question 27

*Quelle affirmation n'est pas un des objectifs d'une signature électronique ?*

Garantir la confidentialité d'un message.

#### Question 28

Toutes les autres routes par défaut doivent avoir une distance administrative inférieure ?

#### Question 29

*Parmi les niveaux de gravité présentés qui indiquent que l'importance d'un événement journalisé, quel est le niveau de gravité le moins sévère ?*

Debugging.

#### Question 30

*Quelle proposition n'est pas une méthode ECMP (Equal Cost Multi-Path) ?*

Priority

### Question 31

*Un FortiGate possède plusieurs VDOM en mode NAT/route avec plusieurs interfaces VLAN dans chaque VDOM. Laquelle des affirmations suivantes est correcte concernant les adresses IP attribuées à chaque interface VLAN ?*

Différents VLAN peuvent utiliser la même adresse IP tant qu'ils se trouvent dans des VDOM différents.

### Question 32

*Quel type de journal contient les informations relatives au trafic qui a été autorisé ou bloqué par le FW ?*

Forward : Contient des informations sur le trafic qui a été autorisé ou bloqué par le FW.

Local : Contient des informations sur le trafic de et vers l'IP de gestion de l'UTM

Sniffer : Enregistre tout le trafic passant par l'interface configurée en One-Arm Sniffer.

### Question 33

*Parmi les propositions suivantes, laquelle est une méthode de configuration de la NAT sur un FortiGate ?*

NAT 64 mode

NAT inspection

Transparent NAT Mode

NAT/Route mode

Firewall Policy NAT mode

### Question 34

*Quelle fonction permet d'obtenir l'empreinte numérique d'un fichier*

NAT

EIGRP

AES

Diffie-Hellman

SHA

RSA

### Question 35

*Quelle affirmation correspond à la notion d'identification des périphériques (Device identification) ?*

FortiClient peut être utilisé comme technique d'identification de périphériques.

### Question 36

*Quel est l'objectif de la phase 1 de IKE ?*

Créer un tunnel sécurisé temporaire pour protéger l'ensemble des échanges IKE phase 2.

### Question 37

*Quelle affirmation est vraie concernant les interfaces entrantes et sortantes dans les règles d'un pare-feu FortiGate ?*

Les interfaces sources et destinations sont obligatoires.

### Question 38

*Que faut-il configurer pour équilibrer la charge sur deux routes statiques menant vers la même destination dans la table de routage ?*

La même distance administrative et la même priorité

### Question 39

*Quel champ d'en-tête peut être utilisé dans une règle de pare-feu pour la correspondance du trafic ?*

Les types et les codes ICMP

### Question 40

*Parmi les choix suivants, lequel est un mode de fonctionnement pris en charge par un périphérique FortiGate ?*

Nat/route



# QCM NSE4 500 PAGES

## 1) Bases

### Question 1

*Examine la configuration ST suivante sur un FortiGate en mode transparent :*

```
config system interface
edit <interface name>
set stp-forward enable
end
```

*Quelle proposition est correcte à propos de la configuration ci-dessus ?*

Le périphérique fortigate transfère les messages ST reçu.

### Question 2

*Quelle sont les exemples de syntaxes correctes pour la commande diagnostics de session de table. (2 choix possibles)*

Diagnose sys sessions filter clear

Diagnose sys sessions filter list dst

### Question 3

*Dans quel ordre sont exécuté les règles de firewall d'un FortiGate Unit ?*

De haut en bas, selon leur numéros de séquences (Sequence number)

### Question 4

*Quel champ d'en-tête peut être utilisé dans une règle de pare-feu pour la correspondance du trafic ?*

Le type et le code ICMP

### Question 5

*Quel proposition est vrai à propos des avertissements règles de pare-feu.*

Les utilisateurs doivent accepter les avertissements avant de continuer

La page d'avertissement est modifiable

### Question 6

*Quelle proposition décrit l'indicateur de statut vert qui apparaît près des différents services de réseaux de distribution FortiGuard ?*

Ils indiquent que le FortiGate est capable de se connecter au réseau de distribution FortiGuard

### Question 7

*Quels protocoles de réseau sont supportés pour l'accès administratif à un FortiGate Unit ?*

SSH – Telnet - HTTP

### Question 8

*Quel est le processus de récupération de mot de passe sur un FortiGate ?*

Se connecter en mode console en utilisant le compte « maintenir » dans les quelques secondes qui suivent la mise sous tension physique du FortiGate, puis entrer les commandes de réinitialisation du mot de passe administrateur.

### Question 9

*Quels sont les méthodes pouvant être utilisé pour délivrer un jeton token à un utilisateur utilisant l'authentification à 2 facteurs ?*

Message d'un téléphone SMS – FortiToken - Email

### Question 10

*Un admin a besoin de télécharger le journal de log d'un FortiAnalyser depuis un FortiGate avec un disque dur interne. Quelle proposition est correcte ?*

Les message de logs sont transmis en tant que texte brut compressé au format LZ4

FortiGate peut encrypter les communications utilisant SSL encrypted OFTP trafic.

### Question 11

*Un admin observe que l'interface Port1 ne peut être configuré avec une adresse IP. Quels peuvent être les raisons ? (3 choix possibles)*

L'interface a été configuré en « one-arm sniffer »

L'interface est un membre d'un virtual wire pair

Le mode d'opération est transparent

### Question 12

*Quelle proposition décrit correctement le mode d'opération transparent ?*

Elle permet l'inspection du trafic interne et le pare-feu sans changer le schéma IP du réseau.

Les paquets Ethernet sont transmis selon l'adresse MAC de destination, et non l'adresse IP.

Le FortiGate agit en tant que pont transparent et transmet du trafic à la couche Layer-2.

### Question 13

*Quand le rôle est configuré en tant qu' « Undefined », quelle proposition est correcte ?*

L'interface graphique (GUI) fournit toutes les options de configuration valable pour l'interface port1.

### Question 14

*Quelle proposition est correcte selon le number ID policy des règles de pare-feu ?*

Ils sont nécessaires pour modifier les règle de pare-feu depuis le CLI.

### Question 15

*Quelle proposition est correcte selon le timeout d'authentification des règles de pare-feu ?*

C'est un timeout d'inactivité. Le FortiGate considère les utilisateurs à être inactif s'ils ne voient aucun paquet venir depuis l'adresse IP source de l'utilisateur.

### Question 16

*Quels protocoles et paramètres peuvent être utilisé pour garantir la sécurité l'accès administratif restrict à un FortiGate ?*

Trusted host – HTTPS - SSH

### Question 17

*Quel antivirus et options de mise à jour de définition d'attaque sont prises en charge par FortiGate units ?*

Mise à jour manuel en téléchargeant les signatures depuis le site de support.  
FortiGuard Pull updates.

### Question 18

*Dans quel états de processus est-il impossible d'interrompre/tuer un processeur ?*

D – Uninterruptable Sleep

Z - Zombie

### Question 19

*Quel est le processus de récupération de mot de passe sur un FortiGate ?*

Se connecter en mode console en utilisant le compte « maintenir » dans les quelques secondes qui suivent la mise sous tension physique du FortiGate, puis entrer les commandes de réinitialisation du mot de passe administrateur.

### Question 20

*Quelle proposition n'est pas une fonction d'un FortiGate ?*

Audit d'une base de données

Prevention des intrusions

Filtrage Web

Contrôle d'application

### Question 21

*Quand un administrateur tente de diriger un FortiGate puis une adresse IP qui n'est pas un trusted host, que se passe-t-il ? FortiGate va mettre en sujet le trafic de cet personne dans les règles de pare-feu, il ne va pas le contourner.*

## Question 22

*Un fichier de sauvegarde commence par la ligne affichée ci-dessous.*

*#config-version=FGVM64-5.02-FW-build589-140613*

*Pouvez-vous le restaurer sur un FortiWifi 60D ?*

*Modèle de périphérique – Version du Firmware – N° build*

Non

## Question 23

## Question 24

*Tu as configuré le serveur DHCP sur l'interface Port1 du FortiGate, afin d'offrir des IP dans un range de 192.168.1.65-192.168.1.253*

*Quand le premier hôte enverra une requête DHCP, quel IP le DHCP va lui offrir ?*

192.168.1.65

## Question 25

*Tu as créé un nouveau compte administrateur et assigné le profil prof\_admin. Qu'est-ce qui est faux à propos des permissions de comptes ?*

Il peut reset les mots de passe oubliés des autres comptes administrateurs comme les « admin »

## Question 26

*Quel fonctionnalité UTM envoie un UDP query aux serveurs FortiGuard serveur chaque fois que FortiGate scan un paquet (à moins que la réponse soit dans le cache)*

Web Filtering

### Question 27

*Une nouvelle version du logiciel FortiOS vient de sortir. Quand vous le mettez à jour, quel proposition est correcte ?*

Si on met à jour via le menu boot loader depuis un serveur TFTP, il ne sauvegardera pas la configuration actuelle. Mais si on le fait depuis l'interface graphique GUI ou CLI, FortiOS va tenter de convertir et sauvegarder la config actuelle dans la nouvelle version de FortiOS

### Question 28

*Si vous avez oublié votre mdp pour le compte Admin de votre FortiGate, comment devez-vous le reset ?*

Il faut éteindre le FortiGate. Après plusieurs secondes, le redémarrer. Se connecter au compte « maintenir » dans les quelques secondes qui suivent la mise sous tension physique du FortiGate, puis entrer les commandes de réinitialisation du mot de passe administrateur.

### Question 29

*Qu'est-ce qui définit l'identification de périphérique ?*

Activer un périphérique source dans une règle de pare-feu active  
l'identification du périphérique dans l'interface source de cette règle.  
FortiClient peut être utilisé en tant qu'agent basé sur l'identification technique de périphérique.

### Question 30

*Quelle proposition est vraie à propos de la table de session FortiGate.*

Elle renseigne les états de connexion TCP

### Question 31

*Quel méthodes permet à Fortigate d'envoyer a One Time Password (OTP) pour l'authentification à 2 facteurs.*

Hardware FortiToken – Email – Software FortiToken

### Question 32

*Laquelle des propositions permet à FortiToken d'utiliser comme input quand il génère un code token.*

Temps et Nom d'utilisateur

### Question 33

*Quelle proposition est fausse à propos des configurations d'avertissements sur le FortiGate ?*

L'avertissement peut être contourné à travers une liste d'exemption de sécurité.

### Question 34

*Quel type de mode de conservation écrit un message log immédiatement, plutôt que lorsque le périphérique quitte le mode conservation ?*

Kernel ou Proxy ?

### Question 35

*Laquelle des modes d'opérations suivants sont supporté par les périphérique FortiGate ?*

Transparent – NAT/route

### Question 36

*Quel type d'erreur pouvez-vous avoir quand vous uploadez un logiciel ?*

Logiciel corrompu – Historique de configuration

### Question 37

*Quel est la sortie pour la commande « diagnose hardware deviceinfo nic » ?*

Mac address physique – Erreurs et collisions

### Question 38

*Dans la sortie de table de session FortiOS, quel est le correct « proto\_sate » numéro pour un établi, non-proxy connection TCP ? 01*

### Question 39

*Que commande est approprié pour l'enquête de haut CPU ?*

Diag sys top – get system performance status

### Question 40

*Quel statut TCP fait les paramètres globaux « tcp-half-open-timer » appliquer ?*

SYN SENT – TIME WAIT ?

### Question 41

*Dans une sortie de table de session FortiOS, quel sont les 2 possibilités de valeur « proto\_state » pour une session UDP ?*

00 - 05

### Question 42

*Qu'est ce qui définit correctement « Section View » et « Global View » pour les règles de pare-feu ?*

Section View listes les règles de pare-feu primaire par leurs couple d'interface  
Global View listes les règles de pare-feu primaire par leurs numéros de séquence de règle.

### Question 43

*Un administrateur veut configurer un FortiGate en tant que serveur DNS. Le FortiGate doit utiliser sa base de données DNS d'abord, et ensuite relayer toutes les requêtes irrésolvable à un serveur DNS externe. Lequel de ces méthodes DNS devez-vous utiliser ?*

Recursive

### Question 44

*Lequel des produits Fortigate suivants peut recevoir une MAJ depuis le FortiGuard Distribution Network ?*

FortiGate – FortiClient - FortiMail



#### Question 45

*Un FortiGate est configuré pour recevoir des notifications de maj depuis le FortiGuard Distribution Network, cependant les maj ne sont pas reçus, quels sont les problèmes qui empêchent cela ?*

Il y a un périphérique NAT entre le FortiGate et le FortiGuard Distribution Network et il n'y a pas d'IP override push configuré

L'interface externe du FortiGate est configuré pour recevoir l'IP adresse d'un serveur DHCP

#### Question 46

*Lesquels des protocoles suivants sont supportés pour un accès administratif depuis un unit FortiGate*

HTTPS, http, SSH, TELNET, PING, SNMP

#### Question 47

*Lequel des propositions suivantes est correcte à propos de l'unit FortiGate opérant en mode NAT/Route ?*

Le FortiGate unit fonctionne en tant que périphérique Layer 3

#### Question 48

*Lequel des propositions suivantes est correcte à propos de l'unit FortiGate opérant en mode NAT/Route ?*

Le Fortigate unit utilise couramment des IP adresses privés depuis le réseau interne mais les caches en utilisant le NAT.

#### Question 49

*Un FortiGate unit peut fournir quel fonctionnalité ?*

Filtre email – Firewall – VPN gateway

### Question 50

*Quelle méthode peut être utilisé pour accéder au CLI ?*

- En utilisant directement une connexion serial
- En utilisant la fenêtre de console CLI depuis l'interface GUI
- En utilisant une connexion SSH
- En utilisant une connexion Telnet

### Question 51

*Remplis le blanc :*

*La commande CLI EXECUTE est utilisé sur l'unit FortiGate pour exécuter la commande static tel que ping ou pour reset l'unit FortiGate to factory defaults.*

### Question 52

*Lors de sauvegardes de fichier de configuration sur un unit FortiGate, le contenu peut être encryptés en activant l'option encrypt and demandant un mot de passe. Si on a oublié le mdp, le fichier de configuration peut toujours être restauré en utilisant quel méthode ?*

Si le mot de passe est oublié, il n'y a aucun moyen d'utiliser le fichier

### Question 53

*Lorsqu'on crée un user admin, lequel des config suivantes d'objets détermine les droits d'accès depuis l'unit FortiGate ?*

Le profile

### Question 54

Trop de choix

### Question 55

Trop de choix

### Question 56

*Les fonctionnalité UTM peut être appliqué à quel groupe d'objet ?*

Les règles de pare-feu.

### Question 57

*Chaque fonctionnalité UTM a des objets UTM configurable comme les sensors, profile ou liste qui définissent comment la fonctionnalité va fonctionner. Comment sont les fonctionnalités UTM appliqué au trafic ?*

Un ou plusieurs UTM features sont autorisés dans les règles de pare-feu

### Question 58

*Si aucune règle de pare-feu n'est spécifié entre 2 interfaces FortiGate et les zones sont inutilisé, quelle action va être prise à propos du trafic entre ces interfaces ?*

Le trafic sera bloqué

### Question 59

Pas étudier

### Question 60

*Qu'est ce qui est faux à propos des paramètres pour un type d'IP pool port block allocation ?*

Le block par user définit le nombre de connexion de block pour chaque user.

### Question 61

*Quel proposition est vrai à propos des services FortiGuard pour Fortigate ?*

L'antivirus signature est dl localement sur le FortiGate.

### Question 62

Trop de choix

### Question 63

Trop de choix

#### Question 64

*Quels options valide pour les requêtes DNS envoyé directement depuis une interface IP de Fortigate.*

Forward-only et non recursive

#### Question 65

*Quel proposition est vrai à propos des avertissements règles de pare-feu.*

Les utilisateurs doivent accepter les avertissements avant de continuer

La page d'avertissement est modifiable

#### Question 66

*Qu'est ce qui définit correctement « Section View » et « Global View » pour les règles de pare-feu ?*

Section View listes les règles de pare-feu primaire par leurs couple d'interface

Global View listes les règles de pare-feu primaire par leurs numéros de séquence de règle.

#### Question 67

*Dans la sortie « diag debug flow », vous voyez le message « Allowed by Policy-1 : SNAT », quelle proposition est vraie ?*

Le paquet correspond à la règle de pare-feu dont l'ID de règle (policy) est 1.

#### Question 68

*Quel proposition est vraie à propos des interfaces entrantes et sortante dans les règles de pare-feu ?*

La source et destination de l'interface sont obligatoire.

#### Question 69

*Quel trafic correspond au règle de pare-feu des paramètres « Services »*

DNS – http – HTTPS

### Question 70

*Quel proposition est fausse à propos des sources correspondant aux règles de pare-feu.*

Un utilisateur/groupe et périphérique source **doit** nécessairement être sélectionné dans une règle de pare-feu (il ne doit pas, il peut, pareil pour user)

### Question 71

*Quel proposition décrit le mieux le timeout authentication ?*

Le temps pendant lequel l'authentification d'utilisateur peut-être inactif sans envoyer de trafic avant de devoir se réauthentifier encore

### Question 72

*Quel action sera prise par default par le FortiGate lorsqu'il reçoit du trafic qui ne correspond avec aucune règle de pare-feu ?*

Le trafic est bloqué et aucun log n'est généré

### Question 73

*Dans quel ordre sont exécuté les règles de firewall d'un FortiGate Unit ?*

De haut en bas, selon leur numéros de séquences

### Question 74

*Quelle proposition est correcte selon le number ID policy des règles de pare-feu ?*

Ils sont nécessaires pour modifier les règles de pare-feu depuis le CLI.

### Question 75

*Quelle proposition est correcte selon le timeout d'authentification des règles de pare-feu ?*

C'est un timeout d'inactivité. Le FortiGate considère les utilisateurs à être inactif s'ils ne voient aucun paquet venir depuis l'adresse IP source de l'utilisateur.

### Question 76

*Dans quel circonstance allez-vous activer LEARN comme action d'une règle de pare-feu ?*

Lorsqu'on veut que le FortiGate surveille un profil spécifique sécurité dans les règles de FW, et fournit des recommandations pour ce profil.

### Question 77

*Quel objet de configuration peut être sélectionné dans le champ Source d'une règle de pare-feu ?*

Adresse FQDN – User ou user group.

### Question 78

*Une route statique est configurée comme une entité FortiGate depuis le CLI en utilisant les commandes suivantes. Quel condition est requise pour que cette route par default soit affichée dans la table de routage du Fortigate ?*

*Config routeur static*

*Edit 1*

*Set device « wan1 »*

*Set distance 20*

*Set gateway 192.168.100.1*

*Next*

*end*

Le statut du lien de l'interface « wan1 » doit être affiché en « down ».

L'adresse de l'interface « wan 1 » et la pppd doit être dans le même sous-réseau.

### Question 79

*Quels objets firewall peut être inclus dans le champs de Destination Address des règles de pare-feu ?*

Virtual IP address – IP address – IP address group

### Question 80

*L'ordre des règles de FW est important. Ces règles peuvent être réordonné depuis l'interface GUI ou CLI. Quel commande CLI est utilisé pour effectuer cette fonction ?*

Move.

### Question 81

*Examiner la configuration CLI suivante. Quel proposition est vraie à propos des effets de la ligne de configuration au-dessus (première ligne)*

La session peut être inactif pendant plus de 1800 secondes.

### Question 82

*Lequel des objets suivants n'est pas un paquet caractéristiques correspondant à un objet de service de FW ?*

Numéro de séquence TCP

### Question 83

*Quel sont les sous-types valides pour les règles type de FW ?*

Identité de périphériques – Adresse – Identité d'utilisateur

### Question 84

*Quels informations peuvent être incluses dans le champ d'adresse de destination des règles de FW ?*

Adresse IP Virtual – Adresse IP actuel ou Adresse IP groupe – FQDN

### Question 85

*Le serveur WEB a une adresse IP de 192.168.2.2 et un masque /24. Lorsqu'on définit l'adresse de pare-feu à utiliser pour cette règle, quel adresse suivant est correcte ?*

192.168.2.2 /32

### Question 86

*En mode NAT/Route, quand il n'y a aucune correspondance dans les règles de pare-feu pour le trafic, quel proposition décrit l'action prise par le FW ?*

Le trafic est bloqué.

### Question 87

*Les règles de blocages de fichier sont appliquées avant ...*

Le scan de virus

### Question 88

*Les entités Fortigate sont préconfiguré avec 4 profils de protections de défaut. Ces profils de protections sont utilisés pour contrôler le type d'inspection de contenu à être performé. Quel action doit être prise par l'un de ses profils pour devenir actif*

Le profil protection doit être assignés à une règle de pare-feu.

### Question 89

*Un FortiGate 60 est configuré pour un SOHO. L'interface DMZ est connecté à un réseau qui contient un serveur web et mail. L'interface Internal est connecté à un réseau contenant 10 utilisateurs de travaux et l'interface Wan 1 est connecté à notre ISP.*

*On veut configurer les règles de pare-feu pour que les utilisateurs puissent envoyer et recevoir des emails depuis et vers le serveur mail sur le réseau DMZ.*

*On veut aussi que le serveur mail soit capable de transmettre des email depuis un serveur mail host par notre ISP utilisant le protocole POP3.*

*Quelles règles doivent être créés pour cette communication ?*

Internal > DMZ

DMZ < Internal



### Question 90

*Quel valeur de session TTL va prendre precedence ?*

Les sessions TTL dicté par la list d'application de contrôle associés avec les règles de FW.

### Question 91

*Quelle proposition décrit correctement le mode d'opération transparent ?*

Elle permet l'inspection du trafic interne et le pare-feu sans changer le schéma IP du réseau.

Les paquets Ethernet sont transmis selon l'adresse MAC de destination, **et non l'adresse IP.**

Le FortiGate agit en tant que pont transparent et transmet du trafic à la couche Layer-2.

### Question 92

*Quel objet de configuration peut être sélectionné dans le champ Source d'une règle de pare-feu ?*

Adresse FQDN – User ou user group – IP Pool

### Question 93

*Quel proposition est fausse à propos des paramètres pour un pool IP de type block allocation ?*

Les blocks par utilisateur définissent leur nombre de connections blocks pour chaque utilisateur

### Question 94

*Qu'est-ce qui est vrai à propos des tables de session FortiGate ?*

Il montre le statut des connections TCP

### Question 95

*Quelle proposition est vraie à propos des pool IP One-to-One ?*

Il autorise la configuration des requêtes ARP

Il n'utilise pas le PAT

### Question 96

*Comment le FortiGate choisit la règle SNAT central qui est appliqué à une session TCP ?*

Il sélectionne la règle SNAT spécifié dans le configuration de l'interface de sortie.

### Question 97

*Parmi les choix suivants, lequel permet à un hôte externe de joindre à un hôte interne ?*

Le port forwarding

### Question 98

*Quelles implémentations NAT permet de limiter le nombre de connexions par adresse IP ?*

IP pool type : Port Block Allocation

### Question 99

*L'interface WAN(port 1) a l'adresse IP 10.200.1.1/24. L'interface LAN(port 2) a l'adresse IP 10.0.1.254/24. La règle de FW du haut a le NAT d'activé utilisant des adresses d'interfaces de sorties. Quel adresse IP va être utilisé pour la source NAT du trafic internet entrant depuis une station de travail avec l'adresse IP 10.0.1.10/24 ?*

10.200.1.10

### Question 100

*Quelles propositions sont vraies à propos des règles de FW NAT utilisant l'adresse IP de l'interface de sortie avec le port fixe désactivé ?*

C'est un many-to-one NAT

Ip source est traduite depuis l'IP de l'interface de sortie

### Question 101

*NAT et Vip pas vu en cours ?*

### Question 102

*Examine la config du router*

*Quel proposition décrit correctement la configuration du routage static ?*

Le FortiGate envoie tout le trafic à 172.20.168.0/24 à travers le port 1

### Question 103

*S'il n'y a aucun changement dans la table de routage et dans le cas où le trafic TCP, quelle proposition est correcte à propos des tables de routage effectué par un FortiGate en Nat/route mode, lorsqu'il cherche une passerelle par défaut ?*

Une boucle est faite quand le premier paquet venant depuis le client (SYN) arrive, et quand le second est effectué lorsque le premier paquet venant depuis le serveur (SYN/ACK) arrive.

### Question 104

*Quel objet de configuration peut être sélectionné dans le champ Source d'une règle de pare-feu ?*

Adresse FQDN

## VDOM

### Question 139

*Lequel des paramètres suivants peut être configuré par VDOM ?*

Mode d'opération (NAT/Route ou transparent)

Routes statiques

Règles de firewall

### Question 140

*L'administrateur d'un FortiGate avec le profil super\_admin configure un domaine virtuel (VDM) pour un nouveau client. Après avoir créé le VDM, l'administrateur ne peut pas réaffecter l'interface dmz au nouveau VDM car l'option est grisée dans l'interface graphique du VDM de gestion. Quelle serait la cause possible de ce problème ?*

L'interface dmz est référencée dans la configuration d'un autre VDM.

### Question 141

*Un FortiGate est configuré avec 3 VDMs. Quel proposition est correct à propos des multiples VDM ?*

Le FortiGate supporte n'importe quel combinaison de VDM dans les modes NAT/Route ou transparent.

### Question 142

*Un appareil FortiGate a 2 VDMs en mode NAT/Route. Quelle solution peut être implémenté par un administrateur réseau pour router le trafic entre les 2 VDMs*

Créer manuellement et configurer un lien inter-VDM entre le vôtre.  
Interconnecter et configurer une interface physique externe sur un VDM à une autre interface physique dans le deuxième VDM.

### Question 143

*Un appareil FortiGate a 2 VDMs en mode NAT/Route. Le VDM de gestion est « root » et est configuré en mode transparent, « vdom 1 » est configuré en tant que NAT/Route. Quel trafic sera généré seulement par « root » et non « vdom1 »*

Piège SNMP

FortiGuard

NTP

#### Question 144

*Quelle proposition est correcte à propos des VDOMs FortiGate ?*

Les VDOMs partagent un FortiGate en 2 ou plus pare-feu indépendant.  
Le VDOM de gestion contient SNMP, logging, email d'alerte et les maj FortiGuard.

#### Question 145

*Quelle proposition est correcte à propos des multiples VDOMs configurés dans un appareil FortiGate ?*

Les appareils FortiGate, de FGT/FWF 60D et au-dessus supportent tous les VDOM

#### Question 146

*Un FortiGate possède plusieurs VDOM en mode NAT/route avec plusieurs interfaces VLAN dans chaque VDOM. Laquelle des affirmations suivantes est correcte concernant les adresses IP attribuées à chaque interface VLAN ?*

Différents VLAN peuvent utiliser la même adresse IP tant qu'ils se trouvent dans des VDOM différents.

#### Question 147

*Un appareil FortiGate est configuré avec 4 VDOMs : « root » et « vdom1 » sont en mode NAT/Route, « vdom 2 » et « vdom 3 » sont en mode transparent. Le VDOM de gestion est « root ». Quelles propositions suivantes sont vraies ?*

Un lien inter-VDOM peut être créé entre « root » et « vdom 1 »

Un lien inter-VDOM peut être créé entre « vdom 1 » et « vdom 2 »

#### Question 148

*Quelles propositions suivantes sont vraies à propos des domaines de diffusion layer 2 dans les VDOMs en mode transparent ?*

Le VDOM entier est considéré comme un seul domaine de diffusion même lorsqu'il utilise plusieurs VLAN.

### Question 149

*Quelles propositions suivantes sont vraies à propos des interfaces FortiGate et STP ?*

Toutes les interfaces FortiGate en mode transparent participe au STP.  
Toutes les interfaces FortiGate en mode transparent peuvent bloquer ou laisser passer les trames BPDU.

### Question 150

*Un FortiGate est configuré avec de multiples VDOM. Un compte administrateur sur l'appareil a été assigné dans un range de valeur du VDOM root. Quels paramètres suivant l'administrateur sera capable de configurer ?*

Adresse de firewall – DHCP serveur

### Question 151

*Quelles propositions suivantes sont vraies à propos des sorties ?*

La configuration globales est synchronisé entre le primaire et secondaire FortiGate.

Le VDOM root n'est pas synchronisé entre le primaire et secondaire FortiGate.

### Question 152

*Un appareil FortiGate est configuré avec 3 VDOM comme illustré ici ?  
Quelles propositions sont correctes si l'admin réseau veut que le trafic route entre tous les VDOMs ?*

L'administrateur peut configurer des liens inter-VDOM pour éviter d'utiliser des interfaces externes et des routeurs.

Comme toutes les interfaces d'appareil FortiGate, les règles de pare-feu doivent être mis en place pour que le trafic soit autorisé à passer entre n'importe quel interface, incluant les lien inter-VDOM.

Comme chaque VDOM a une table de routage indépendant, les règles de routages doivent être configuré (p.e. routage statique, OSPF) dans chaque VDOM pour router le trafic entre les VDOM.

### Question 153

*Quelles propositions suivantes sont vraies à propos des VDOMs ?*

Différentes sous-interfaces VLAN de la même interface physique peut être assigné à différents VDOM.

Chaque VDOM a sa propre table de routage.

### Question 154

*Quelle proposition est correcte à propos des VDOMs ?*

Les VDOMs partage un FortiGate en 2 ou plusieurs unité virtuelle qui fonctionne comme plusieurs, unité indépendante.

Le VDOM de gestion contient SNMP, logging, email d'alerte et les maj FDN-based.

Les VDOMs partagent les versions firmware, comme les antivirus ou les DB IPS.

### Question 155

*L'administrateur d'un FortiGate avec le profil super\_admin configure un domaine virtuel (VDOM) pour un nouveau client. Après avoir créé le VDOM, l'administrateur ne peut pas réaffecter l'interface dmz au nouveau VDOM car l'option est grisée dans l'interface graphique du VDOM de gestion. Quelle serait la cause possible de ce problème ?*

L'interface dmz est référencée dans la configuration d'un autre VDOM.

### Question 156

*Quelle est l'erreur obtenu par l'administrateur dans l'interface ?*

Les paramètres globaux ne peuvent être configuré depuis le context VDOM root.

### Question 157

FIN DES VDOM, SUITE NON COHERENTE

*De quels périphériques la Fortinet Security Fabric doit-elle être composé ?*

Au min. un FortiAnalyser et 2 FortiGates.

### Question 158

*Parmi les choix suivants, lequel n'est pas un avantage lié à l'utilisation d'une translation d'adresse NAT ?*

Assure la cohérence des schémas d'adressage du réseau interne.

Permet d'économiser les adresses publiques.

Améliore la sécurité en empêchant de connaître les adresses utilisées en interne.

Simplification des communications utilisant des tunnels (tel que IPsec).

### Question 159

*Quel type de journal contient les informations relatives aux mises à jour FortiGuard ?*

System

### Question 160

*S'il n'y a pas de changement dans la table de routage et dans le cas du trafic TCP, lequel des éléments suivants décrit correctement les recherches dans la table de routage effectuées par un fFortiGate en mode NAT/Route, lors de la recherche d'une route ?*

Une recherche est faite quand le premier paquet venant depuis le client (SYN) arrive, et une seconde est effectuée lorsque le premier paquet provenant du serveur (SYN/ACK) arrive.

### Question 161

*Quelle affirmation est correcte en ce qui concerne les numéros d'identification (Policy ID) des règles de pare-feu ?*

Ils sont nécessaires pour modifier une règle de pare-feu à partir de la CLI

### Question 162

*Pour le trafic qui ne correspond à aucune règle de pare-feu configurée, quelle est l'action par défaut prise par le FortiGate ?*

Le trafic est bloqué et aucun journal (log) n'est généré.



### Question 163

*Parmi les niveaux de gravité présentés qui indiquent que l'importance d'un événement journalisé, quel est le niveau de gravité le moins sévère ?*

Emergency

### Question 164

Quelle affirmation est vraie concernant l'entrée de journal présentée ci-dessous ?

```
date=2018-05-20 time=09:30:18 logid=0100042008 type=event subtype=system  
level=information vd="root" user="admin" ui=http(192.168.1.11) action=login  
status=success reason=none profile="super_admin" msg="Administrator admin  
logged in successfully from http(192.168.1.11)"
```

Dans l'interface graphique, l'entrée journal se trouvait sous « Log&Report > Event Log > System »

La connexion était non crypté

L'ip de l'ordination de l'admin était de 192.168.1.11

### Question 165

*Quelle proposition n'est pas un type de journal utilisé sur un Fortigate ?*

Event Log

Security Log

Traffic Log

Syslog

### Question 166

*Quel protocole ne peut pas être utilisé avec le moniteur d'état de liaison (Link Health Monitor) ?*

Twamp – http – UDP\_echo – Stamp – TCP\_echo – Ping

### Question 167

*Quel est l'objectif de la phase 1 de IKE ?*

Créer un tunnel sécurisé temporaire pour protéger l'ensemble des échanges IKE phase 2.

### Question 168

*Quel élément est utilisé pour vérifier un certificat numérique envoyé par un serveur ?*

Clé publique de l'autorité de certification

### Question 169

*Quel affirmation est vraie concernant IKE ?*

Le mode agressif ralenti la négociation d'échange des clés en imposant des tailles de clés plus grandes.

Chaque IKE Phase 2 peut avoir plusieurs IKE Phase 1

IKE permet de négocier différentes clés de chiffrement. Différents trafics peuvent donc être chiffrés avec des clés différentes au sein du même tunnel IPsec de site à site

IKE phase 1 procède à l'authentification des utilisateurs via des PreSharedKey, des clés RSA ou des certificats.

### Question 170

*Quelle affirmation est fausse concernant le routage basé sur des règles (Policy-based routing)*

Les règles ne sont pas lues selon l'ordre séquentiel mais selon la meilleure correspondance.

### Question 171

*Quelle affirmation est fausse concernant la correspondance des sources dans une règle de pare-feu ?*

Un périphérique source **doit** nécessairement être sélectionné dans une règle de pare-feu (il ne doit pas, il peut, pareil pour user)

### Question 172

*Parmi les choix suivants, lequel est un mode de fonctionnement pris en charge par un périphérique FortiGate ?*

Nat/route

### Question 172

*Quelle méthode peut être utilisée pour délivrer le code du jeton à un utilisateur lors de l'utilisation d'une authentification à deux facteurs ?*

Utiliser un email - Message d'un téléphone SMS – FortiToken

### Question 173

*Un FortiGate possède 2 VDOM en mode NAT/Route. Parmi les propositions suivantes, laquelle peut être mise en œuvre par un administrateur pour router le trafic entre les 2 VDOMs*

Créer et configurer manuellement un lien inter-VDOM entre les deux VDOM.  
Interconnecter et configurer une interface physique externe sur un VDOM à une autre interface physique dans le deuxième VDOM.

### Question 174

*Laquelle des affirmations suivantes est correcte concernant les VDOM multiples configurés dans un FortiGate ?*

Les modèles FortiGate FGT60D et supérieurs prennent en charge les VDOM.

### Question 175

*Laquelle des affirmations suivantes est fausse concernant les paramètres d'une allocation de blocs de ports lors de la configuration de la NAT ?*

Les blocks par utilisateur définissent leur nombre de blocks utilisable pour chaque utilisateur.

### Question 176

*Quelle technologie est la plus susceptible d'être utilisée dans un VPN de type site à site ?*

IPsec

### Question 177

*Laquelle des affirmations suivantes est fausse concernant les domaines virtuels FortiGate (VDOM) ?*

Des règles de pare-feu ne sont pas nécessaires pour autoriser le trafic entrant par les liens inter-vgdom

### Question 178

*Laquelle des affirmations suivantes est fausse concernant les domaines virtuels FortiGate (VDOM) ?*

Le même compte administrateur doit être utilisé pour la gestion des différents VDOM d'un FortiGate.

### Question 179

*D'après les informations fournies, quelle affirmation est fausse si la protection contre l'usurpation d'adresse IP (Reverse Path Forwarding Check, RPF) est configurée en **mode loose** ?*

**Mode loose** : Paquet accepté tant qu'il y a une route active vers IP source via interface entrante.

**Mode stricte** : Route active vers IP source vers interface entrante et si route = meilleur chemin possible

Le paquet IP dont l'IP source est 150.142.15.73 et l'IP destination est 10.0.3.17 arrivant sur l'interface Wan2 est bloqué par la fonction RPF.

### Question 180

*Quelle fonction permet d'obtenir l'empreinte numérique d'un fichier*

SHA

### Question 181

*Un administrateur veut créer un tunnel VPN IPsec entre 2 appareils FortiGate. Quelle proposition n'est pas une étape de configuration qui doit être effectuée sur les 2 périphériques ?*

Configurer le mode de fonctionnement en mode VPN IPsec.

Configurer les groupes d'utilisateurs appropriés pour permettre aux utilisateurs d'accéder au tunnel.

Définir les paramètres de la phase 1

Définir les paramètres de la phase 2

Créer des règles de pare-feu pour autoriser et contrôler le trafic entre les adresses IP source et destination

### Question 182

*Lors de l'établissement d'un tunnel, quel mode IPsec inclut les informations d'identification des pairs dans le premier paquet envoyé avant tout chiffrement ?*

Main mode

### Question 183

*En sécurité informatique, quel terme désigne le fait de pouvoir consulter tous les faits et gestes des utilisateurs qui se sont authentifiés et qui ont été autorisés à accéder à un équipement ?*

La traçabilité

### Question 184

*Dans quel ordre sont exécutées les règles de firewall d'un FortiGate Unit ?*

De haut en bas, selon leur numéros de séquences (Sequence number)

### Question 185

*Parmi les propositions suivantes, laquelle est une méthode de configuration de la NAT sur un FortiGate ?*

Firewall Policy NAT mode – Central NAT mode

### Question 186

Chrono : 55.70 s / 4788 s

Une route statique est configurée comme présenté ci-dessous. Laquelle des conditions proposées est requise pour que cette route statique soit affichée dans la table de routage ?

**New Static Route**

	Subnet	Named Address
Destination ⓘ	172.16.1.0/255.255.255.0	
Gateway	192.168.100.1	
Administrative Distance ⓘ	20	
Comments	<div>0/255</div>	
<input checked="" type="checkbox"/> <b>Advanced Options</b>		
Priority ⓘ	0	

L'adresse IP de l'interface de sortie et l'adresse IP de tronçon suivant (Gateway) doivent se trouver sur le même sous-réseau.

### Question 187

*Parmi les champs suivants contenus dans les en-têtes IP/TCP/UDP, lequel peut être utilisé pour prendre une décision de routage lors de l'utilisation du routage basé sur des politiques (Policy-based routing) ?*

Ports TCP/UDP source

### Question 188

*Quelle proposition est un mode IKE utilisé lors de la négociation de la phase 2 d'IPsec ?*

Quick Mode

### Question 189

*Quelle affirmation est vraie concernant les numéros d'identification (Policy ID) des règles de pare-feu ?*

Ces ID sont nécessaires pour modifier une règle de pare-feu à partir de la CLI.