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

O Le FortiGate établi un tunnel SSL avec le poste client et un autre tunnel SSL avec le serveur web.

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

O Le Fortigate doit disposer d'un certificat permettant d'émettre des certificats.

O 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 ?

O Dans n'importe quel serveur Windows

O II n'y a pas dagent collecteur, le FortiGate interroge les contrôleurs de domaine AD.

C) Dans le contrôleur de domaine AD maître

O Dans l'un des contrôleurs de domaine AD

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

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

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

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

O 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
```

O La destination syslog

O L'horodotage du message syslog

O La gravité Syslog

O La capacité Syslog

O Le numéro de séquence du message syslog

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

O Monitor scan flow-based

O Proxy-based

O Full scan flow-based

O Quick scan flow-based

Quelle affirmation concernant IPS est fausse ?

O La configuration la plus performante pour bloquer les attaques consiste à utiliser l'IPS derrière une interface en mode One•arm sniffer.

O L'IPS peut bloquer une tentative d'intrusion alors qu'un IDS ne peut pas.

O L'IPS peut détecter des attaques de type "zero•daf.

O Le moteur IPS est utilisé par lilPS mais aussi par dautres fonctions de sécurité du Fortigate.

Quelle affirmation est fausse concernant l'authentification NTLM ?

O Elle doit être prise en charge (supportée) par les contrôleurs de domaine.

O Elle permet l'authentification lorsque la communication avec l'agent DC ne fonctionne plus.

O Elle doit être prise en charge par le navigateur de l'utilisateur.

O 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) ?

O Augmenter la vitesse des ports du commutateur.

O Désactiver la fonction Dynamic Trunking Protocol (DTP).

O Utiliser une liste de contrôle daccès (ACL) pour filtrer le trafic de diffusion.

O Filtrer les VLAN sur les liens trunk.

O Configurer la sécurité des ports (port-security).

O Augmenter ta 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 IO 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 blcxlués.

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

O 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" ?

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

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

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

O 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 ?

O 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.

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

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

O 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 ?

O Dans un profil de contrôle d'application.

O Dans une interface.

O Dans une règle DOS.

O 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 ?

O Utiliser le -web-only

O Désactiver le split tunneling

O Configurer des signets web (Bookmarks)

O 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 ?

O NAT/ Route

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

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

O Mode transparent

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

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

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

O Utiliser SSH pour tous les accès à distance.

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

O 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?

O Polling mode

O Terminal Server agent mode

O Domain Controler agent mode

O eDirectory agent mode

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

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

O 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.

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

O 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 ?

O Les rapports en temps réel et l'analyse à long terme des événements de sécurité sont activés.

O Les analystes réseau sont en mesure daccéder aux fichiers journaux des périphériques réseau et de surveiller le comportement du réseau.

O 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.

O 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 ?

O La compression

O L'ajout de code mort

O Le chiffrement

O 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 ?

O LLDP

O BPDU Guard

O Protector

O EEE BPDU

O Watchdog

O STP Checker

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

O Snooping

O Spoofing

O Flooding

O Starvation

O Sweep scan

O 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 » ?

O Configurer l'application cliente pour qu'elle transfère le trafic IP vers l'applet Java préalablement installée.

O Configurer les applications qu'elles utilisent des ports TCP dynamiques.

O Installer le client VPN SSL FortiClient.

O 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 ?

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

O La clé publique du certificat du serveur web doit être installée dans le navigateur.

O Le navigateur doit avoir la clé privée du certificat de la CA qui a signé le certificat du navigateur web.

O Le certificat du serveur web doit être installé dans le navigateur.

Quelle affirmation sur les profils de filtrage DNS est vraie ?

O Ils permettent de filtrer plus précisément que le filtrage HTTP.

O Ils peuvent aussi inspecter le trafic HTTPS.

O Ils peuvent bloquer les requêtes DNS vers des serveurs de commande et de contrôle de botnets connus.

O Ils peuvent inspecter le trafic HTTP.

O 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 ?

O Le Fortigate devra de la clé privée qui a signé les certificats numériques des clients.

O Les utilisateurs devront fournir un nom dutilisateur et un mot de passe valides.

O Le FortiGate devra envoyer un token (un jeton) aux utilisateurs afin de valider leur certificat.

O Les utilisateurs doivent appartenir à un dutilisateurs de pare-feu (Firewall user group).

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

O La recherche de virus est activée par défaut.

O L'activation du scan de virus dans un profit de sécurité permet la protection contre les virus pour tout le trafic passant par le FortiGate.

O Le scan de virus doit être activé dans un profil de sécurité, qui doit être appliqué à une règle de pare-feu.

O 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) ?

O Attaques par injection SQL

O Attaques via des scripts de site à site (XSS)

O Trafic vers les serveurs de botnets

O Fuites de données relatives aux cartes de crédit de la société

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

O L'attaquant envoie de nombreuses demandes de connexions TCP mais ne les finalisent pas.

O 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.

O L'attaquant envoie un paquet malformé spécialement conçu la synchronisation des sessions de la cible.

O L'attaquant envoie un paquet s*ifiquement conçu pour se synchroniser avec le FortiGate.

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

O Trap

O Syslog message

O SNMP POST

O SNMP GET

O Capture