386. La commande "sys ha reset-uptime" ?

Lequel des énoncés suivants décrit correctement l'utilisation de la fonction "diagnostiquer

A. Pour forcer un basculement HA lorsque le paramètre de contournement HA est désactivé

B. Pour forcer un basculement HA lorsque le paramètre HA override 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)

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

5. Le maître synchronise la configuration du cluster avec le stree

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

O. 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.

195. 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 ci-dessous :

config web-proxy explicit set pac-file-server-status enable set pac-file-server-port 8080 set pac-file-name 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. httos://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 A. Plus d'un proxy est supporté.

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

.. 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 proxiée ?

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 ForitGate 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 V

B. DOM 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 AII 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 tep ; --flow from_client ; --pattern "X-MMS-IM-Format" ; --pattern "fortinet",

- no_case ;)

B. F-SBID (--protocole top ; -flow from_client ; --pattern "fortinet" ; --no_case ;)

C. F-SBID(--protocole top ; -flow from_client ; --pattern "X-MMS-IM-Format", : --pattern "fortinet", - within

20 ; --no_case ;)

D. F-SBID(--protocole top ; -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. Configuré 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;-

contex 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.

3. 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.

p. 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.)

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. di 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] filterg= [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 _pktdetail 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 meg="allouer une nouvelle session=00000340

id=20085 trace id=1 func=vf_ip_route_input_common line=2583 mag="trouver une route : flag=04000000 gw-10.200.1.254

portin

id=20085 trace_id=1 func=fk_forward_handler line=586 mag="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 FERMEE.

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.