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 Adress 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-vdom, 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-vdom.
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-vdom 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 « maintainer » 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)
Prevention 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 correspondant 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 modifiés 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 phasé 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 executé 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 « maintainer » 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 décharger 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 – Uniterruptable 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 « maintainer » 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 « maintainer » 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 reçu, 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 FartiGate 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 FartiGate 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 authentification ?

Le temps pendant lequel l'authentification d'user 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 executé 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 règle 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 ppd 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'user

Question 84

Quels informations peuvent être inclues 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 cet 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 travails 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 crées 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 desactivé ?

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 (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 141

Un FortiGate est configuré avec 3 VDOMs. Quel proposition est correct à propos des multiples VDOM ?

Le FortiGate supporte n'importe quel combinaison de VDOM dans les modes NAT/Route ou transparent.

Question 142

Un appareil FortiGate a 2 VDOMs en mode NAT/Route. Quelle solution peut être implémenté par un administrateur réseau pour router le trafic entre les 2 VDOMs

Créer manuellement et configurer un lien inter-VDOM entre le vôtre.
Interconnecter et configurer une interface physique externe sur un VDOM à une autre interface physique dans le deuxième VDOM.

Question 143

Un appareil FortiGate a 2 VDOMs en mode NAT/Route. Le VDOM 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 partage 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 configuré dans un appareil FortiGate ?

Les appareils FortiGate, de FGT/FWF 60D et au-dessus supporte 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 créer entre « root » et « vdom 1 »
Un lien inter-VDOM peut être créer 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.

FIN DES VDOM, SUITE NON COHERENTE

Question 157

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 utilisé 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 effectué lorsque le premier paquet provenant dule 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 ?

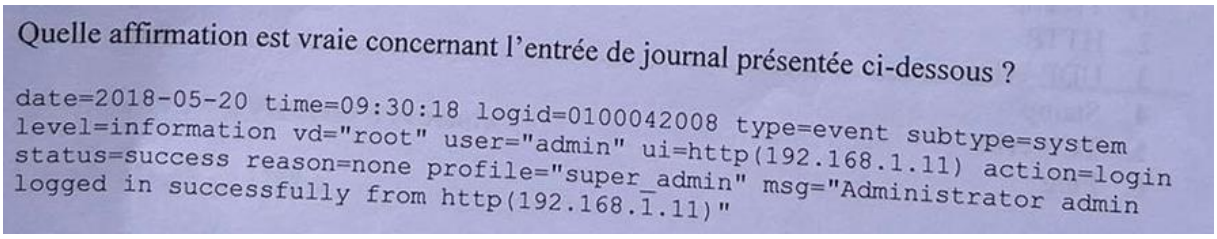
Le trafic est bloqué et aucun journal (log) n'est généré.

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



Dans l'interface graphique, l'entrée journal se trouvait sous « Log&Report > Event Log > System »

La connection 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 correspondant 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 affirmation 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 affirmation 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 le plus susceptible d'être utilisée dans un VPN de type site à site ?

IPsec

Question 177

Laquelle des affirmation 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-vdom

Question 178

Laquelle des affirmation 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 executé les règles de firewall d'un FortiGate Unit ?

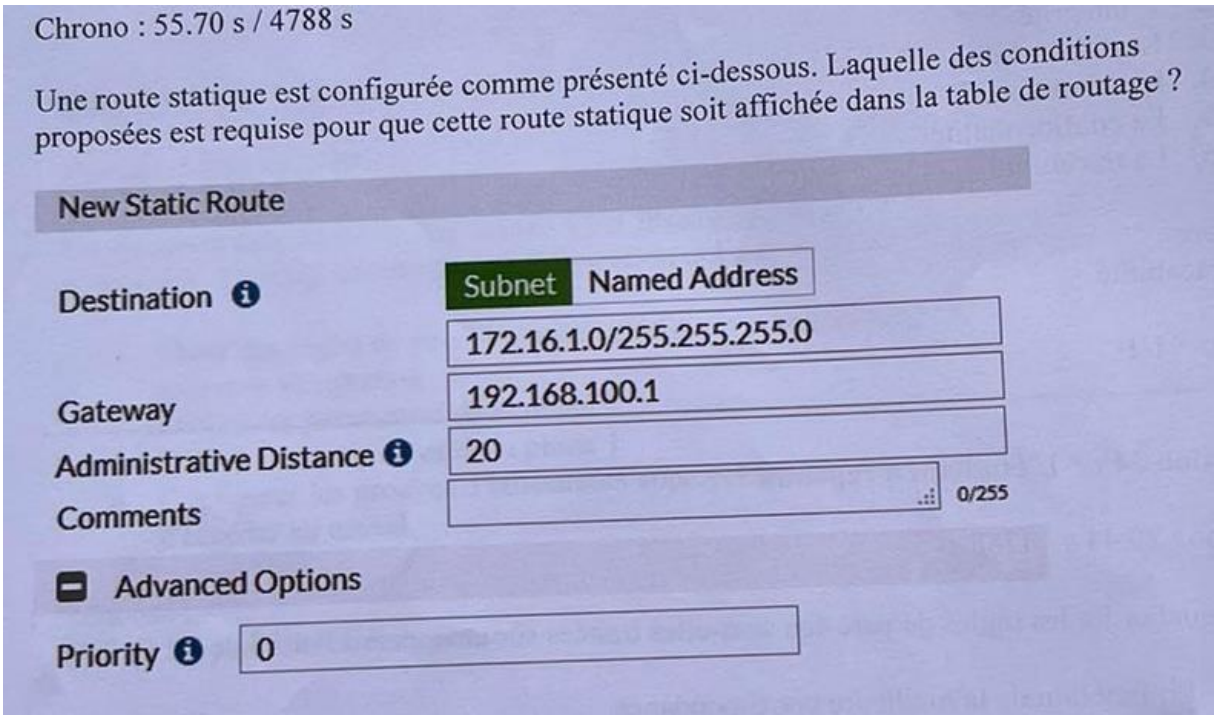
De haut en bas, selon leur numéros de séquences (Sequence number)

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



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-base routin) ?

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.