35. Lors de l'application d'une règle de NAT, il est possible de modifier simultanément l'adresse IP source et l'adresse IP destination

Vrai

Faux

36. L'accès au portail captif s'effectue via l'URL

https://<adresse_IP_firewall>/proxy

https://<adresse_IP_firewall>/auth

https://<adresse_IP_firewall>/portal

https://<adresse_IP_firewall>/ldap

Je souhaite que l'accès à Internet depuis mon réseau interne soit soumis à une authentification préalable. Pour cela, j'ajoute dans la politique de filtrage une règle d'authentification qui redirige tous les utilisateurs non-authentifiés vers le portail pour l'ensemble des sites d'Internet. Malgré cela, je souhaite que l'accès au site www.stormshield.eu reste accessible sans authentification. Comment puis-je faire cela ?

En créant une catégorie d'URL personnalisée contenant www.stormshield.eu et en l'ajoutant à la liste des exclusions de la règle d'authentification peut etre elle aussi si ya plsr reponse

En ajoutant une règle de filtrage, située au dessus de la règle d'authentification, et qui autorise l'accès à Internet depuis le réseau interne et sans authentification

Il n'est pas possible de créer cette exception

En ajoutant une règle de filtrage, située au dessus de la règle d'authentification, et qui autorise l'accès à l'objet FQDN www.stormshield.eu depuis le réseau interne et sans authentification

39. Par défaut, seul le super administrateur "admin" peut accéder aux logs complets en cliquant sur "Accès restreint aux logs"

Faux

Vrai

40. Les traces du firewall peuvent être stockées en local sur

Les firewalls qui disposent d'un disque dur

Les modèles les SN160, SN210 et SN310 avec une carte SD insérée

Tous les modèles de firewalls

Les firewalls virtuels

41. Le Règlement Général sur la Protection des Données (RGPD) a une incidence sur la gestion des logs

Faux

Vrai

42. Dans le cas où le firewall déclenche une alarme majeure, vous devez

Redémarrer le firewall

Ne rien faire
Analyser les serveurs
Analyser les traces

43. Un administrateur différent de "admin" peut accéder aux logs complets via un code d'accès
Qu'il peut générer lui-même
Qu'un autre administrateur ayant des droits doit générer
Temporaire
Non limité dans le temps

44. Dans quel(s) module(s) du firewall la plage VPN SSL attribuée aux clients mobiles peut-elle être utilisée ?
Le filtrage
Le VPN Ipsec
Le NAT

45. Si je réserve le réseau 10.8.0.0/24 aux clients se connectant par le biais du VPN SSL, les adresses IP obtenues à la connexion du premier client sont
10.8.0.3 pour adresse réseau, .4 pour l'IP de l'interface du tunnel côté serveur, .5 pour l'IP du client, et .6 pour l'adresse de diffusion
10.8.0.1 pour adresse réseau, .2 pour l'IP de l'interface du tunnel côté serveur, .3 pour l'IP du client, et .4 pour l'adresse de diffusion
10.8.0.2 pour adresse réseau, .3 pour l'IP de l'interface du tunnel côté serveur, .4 pour l'IP du client, et .5 pour l'adresse de diffusion
10.8.0.4 pour adresse réseau, .5 pour l'IP de l'interface du tunnel côté serveur, .6 pour l'IP du client, et .7 pour l'adresse de diffusion

46. Par défaut, la durée de vie d'un tunnel VPN SSL est de
14000 secondes
14400 secondes
3600 secondes
36000 secondes

48. L'adresse IP utilisée dans le tunnel VPN SSL est configurée manuellement par l'utilisateur dans le client VPN SSL
Faux
Vrai

50. Le nom d'un objet que je crée manuellement peut
Commencer par un chiffre
Être un nom de domaine
Contenir un nombre illimité de caractères

Commencer par Firewall_
Commencer par Network_

51. Les objets commençant par Network_ peuvent être modifiés dans la base d'objets par l'utilisateur
Vrai
Faux

52. Lors de la création d'un objet FQDN, l'adresse IP par défaut peut être obtenue par une résolution DNS
Faux
Vrai

53. Le filtrage par SNI (nom de certificat) permet de bloquer l'accès à des sites web. Il est utilisable sur les protocoles
HTTPS
HTTP
HTTP et HTTPS

54. L'analyse antivirale peut s'appliquer à des flux
ICMP
SSH
SMTP
HTTPS, si déchiffrement préalable
HTTP

55. Breach Fighter peut analyser les fichiers transitant via le(s) protocole(s)
FTP
GRE
HTTPS
ICMP

56. Breach Fighter fonctionne uniquement avec l'option "Antivirus avancé"

Faux

Vrai

57. Un flux HTTPS dépend de l'action "Passer sans déchiffrer". Le certificat présenté au le navigateur est celui du proxy SSL
Faux
Vrai

58. Lorsque le filtrage URL se base sur le fournisseur "Extended Web Control", toutes les requêtes HTTP sont transmises à un des serveurs du cloud pour obtenir la catégorisation du site visité

Vrai, dans tous les cas
Faux, dans tous les cas
Vrai, si l'URL visitée n'est pas présente dans le cache local du proxy

60. En fonction de quel(s) critère(s) le firewall est capable de filtrer les flux ?
De l'adresse IP source
Du protocole
Du numéro de session
Du port
De l'adresse IP destination

61. Dans une connexion FTP, le mode de traces avancé dans une règle de filtrage est-il nécessaire pour journaliser le trafic FTP ?
Non
Oui

63. Dans une règle de filtrage, il est possible de renseigner plusieurs objets FQDN comme objets de destination
Faux
Vrai

64. La sélection d'une région dans le menu Géolocalisation / Réputation, permet de choisir
Un continent
Un pays
Un groupe de pays créé par l'administrateur

65. Les paquets ICMP de type "echo reply" peuvent être tracés dans les logs de filtrage avec le niveau de trace standard sur une règle de filtrage
Vrai
Faux

66. Parmi les paramètres suivants, quels sont ceux qui peuvent être utilisées dans une règle de filtrage ?
Adresse réseau source
Adresse IP destination
Port destination (TCP ou UDP)
Interface réseau d'entrée
Message ICMP

62. Pour tracer toutes les requêtes PING, je dois
Vérifier la présence des traces correspondantes dans le journal "Filtrage"
Utiliser le niveau de traces "avancé"
Aucune des réponses proposées

Utiliser le niveau de traces "standard"
Vérifier la présence des traces correspondantes dans le journal "Trafic réseau"

67. Les réponses d'une connexion établie au travers du firewall doivent être autorisées explicitement dans les règles de filtrage
Faux
Vrai

68. La modification de l'action peut s'appliquer à plusieurs règles de filtrage à la fois
Vrai
Faux

69. Quelles inspections de sécurité peuvent être activées dans la politique de filtrage
Filtrage URL
Analyse antispam
Filtrage SMTP
Antiphishing
Analyse antivirale

70. Quelle est l'action appliquée par défaut si aucune règle de filtrage ne correspond au paquet reçu par le firewall ?
Conserver une trace
Eteindre le firewall
Passer
Bloquer

4. L'adresse IP utilisée dans le tunnel VPN SSL est configurée manuellement par l'utilisateur dans le client VPN SSL

FauxVrai

5. Le service VPN SSL peut fonctionner sur le port

TCP/443

TCP/389

UDP/1194

TCP/4343

6. L'objet Network_internals contient (2 bonnes réponses)

Les réseaux déclarés dans une route statique et joignables depuis une interface protégée

Les réseaux de toutes les interfaces du firewall

Les réseaux privés définis par l'IETF dans la RFC 1918

Le réseau de l'interface "in"

Les réseaux de toutes les interfaces protégées

Les réseaux des interfaces "dmz"

8. Donnez un équivalent à l'objet "Internet"

Network_in

Network_out

Différent de Firewall_internals

Any

Différent de Network_internals

9. Dans la liste suivante, sélectionnez les éléments pouvant être représentés par un objet

Un réseau

Un routeur

Un utilisateur ou un groupe d'utilisateurs

Un groupe de mots clés à utiliser dans le filtrage URL

Une adresse IP

10. L'utilisation de l'option Extended Web Control pour le filtrage URL permet d'éviter le stockage local de la base URL Stormshield

Faux

Vrai

12. L'activation du proxy SSL s'effectue par la création d'une règle de filtrage

Faux

Vrai

13. Breach Fighter fonctionne uniquement avec l'option "Antivirus avancé"

Faux

Vrai

16. Lorsque la quantité d'espace disque allouée à une catégorie de log est atteinte, quelle(s) action(s) est(sont) possible(s) ?

Arrêter le firewall

Envoyer un ping

Effectuer une rotation automatique des fichiers de logs

Arrêter l'écriture des logs

48. Le chiffrement des paquets IP au sein d'un tunnel Ipsec est assuré par le protocole

ESP

43. La directive "Via Tunnel VPN IPsec" des règles de filtrage permet de forcer l'émission du trafic correspondant dans le tunnel VPN IPsec.

O Faux

O Vrai

35. Quelles bases LDAP peuvent être configurées sur un firewall Stormshield Network?

Base LDAP externe (ex: OpenLDAP)

Base LDAP interne

Base Microsoft Active Directory

37. Le portail d'authentification peut être accessible (ID)

Depuis toutes les interfaces

Depuis l'interface "in" seulement

Depuis l'interface "out" seulement

39. Quel que soit le client nomade utilisé (VPN SSL Stormshield ou OpenVPN), il récupère automatiquent les paramètres de configuration depuis le portail captif.

O Faux

O Vrai

40. La fonctionnalité VPN SSL permet uniquement à des postes Windows d'accéder aux ressources d'un réseau protégé

O Faux

© Vrai

44. Pour des tunnels négociés en IKEv1, les extrémités de trafic doivent être rigoureusement identiques sur les deux sites participant au tunnel IPsec pour que les tunnels puissent fonctionner

O Vrai

O Faux

45. Combien de phases sont nécessaires à l'établissement d'un tunnel VPN IPsec?

10

1

2

5

3

AUCUNE

46. Lors de la création d'un VPN IPsec, si je paramètre une authentification par PSK, cela signifie

O Par certificat

© Par authentification RADIUS

O Par authentification LDAP

O Par clé pré-partagée

47. Les règles implicites générées lors de l'activation d'une politique IPsec permettent

C D'autoriser le trafic au sein du tunnel

O La réception de paquets 4500/UDP

O La négociation d'un tunnel nomade

O La négociation ISAKMP et la réception des paquets ESP d'un tunnel site à site

Pages 435 regarder si ya plus d'options

50. Quels types de VPN puis-je établir entre deux firewalls Stormshield Network?

VPN IPsec

OpenVPN

VPN PPTP

VPN SSL

51. Il est possible de créer une liste de ports destination dans une seule et même règle de filtrage

O Faux

© Vrai

18. Il est possible d'arrêter l'écriture des événements pour une catégorie de trace

Faux

Vrai

19. La mise en œuvre du Règlement Général sur la Protection des Données (RGPD) restreint l'accès aux logs

Depuis l'interface d'administration du firewall

Pour tous les administrateurs

Pour tous les administrateurs sauf le super administrateur admin

20. Il est possible de visualiser les journaux (logs) ou une portion des journaux via

L'interface d'administration du firewall

Wireshark

21. Le module de prévention d'intrusion (IPS) des firewalls Stormshield Network est

Libre (open source)

Propriétaire

22. Un firewall SNS est capable

D'authentifier les utilisateurs

De filtrer le trafic selon un port

De filtrer selon un protocole

D'agir comme un routeur

23. L'administrateur peut configurer le firewall via

Un navigateur web

SSH

Telnet

console série

24. La restauration d'une configuration

Ne peut pas s'effectuer depuis une sauvegarde automatique

Ne peut s'effectuer que si le fichier de configuration est protégé par un mot de passe

Peut s'effectuer partiellement depuis une sauvegarde automatique

S'effectue grâce à l'import d'un fichier au format ".na"

25. La partition active peut être sauvegardée

Sur tous les modèles de firewalls

Seulement sur les modèles de firewall virtuel

Seulement sur les modèles de firewall physique

26. La mise à jour système est possible

Seulement lorsque la partition principale est active

Peu importe la partition active

Seulement lorsque la partition de secours est active

Est-il possible de créer en un clic une politique de filtrage URL avec l'ensemble des groupes URL

personnalisés que vous avez créés au préalable ?

Oui

Non

63. Mon accès Internet est assuré par une connexion modem ADSL. J'ai paramétré cet accès dans mon firewall. Il me suffit alors d'activer la politique de filtrage n°10, telle qu'elle est définie dans la configuration d'usine, pour que mes machines internes puissent accéder à Internet ?

Vrai

Faux

11. L'activation d'une règle de filtrage peut se faire en fonction du jour et de l'heure

O Faux

O Vrai

14. J'installe un serveur Web dans une DMZ. Je souhaite rendre ce serveur accessible sur les ports HTTP et HTTPS depuis n'importé quelle machine d'internet. Quelle(s) règle(s) de filtrage dois-je ajouter ?

Les flux HTTP et HTTPS depuis T'adresse publique du serveur web vers Internet

Les flux HTTP et HTTPS depuis Internet vers l'adresse publique du serveur

Les flux HTTP et HTTPS depuis Internet vers l'adresse privée du serveur

Les flux HTTP et HTTPS depuis Network-out vers l'adresse privée du serveur

Sur les appliances PHYSIQUES SNS, il est possible de

Sauvegarder uniquement un slot de configuration depuis l'interface graphique

Sauvegarder les fichiers de logs vers un serveur en utilisant le protocole FTP

Copier la partition active vers la partition passive

Sauvegarder la configuration complète vers un fichier chiffré p.67

17. Les firewalls Stormshield Network sont capables de limiter la taille de chaque paquet ping (ICMP echo) arrivant sur un

serveur

O Faux

O Vrai

28. Lors de la connexion sur l'interface d'administration de mon firewall, le navigateur remonte un problème de sécurité :

Ce comportement n'est constaté que lors de la première connexion et en configuration usine

Il faut ajouter une exception de sécurité pour le certificat du firewall dans le navigateur pour pouvoir continuer

C'est normal et ce comportement ne peut être modifié

29. Un utilisateur est redirigé vers une autre méthode d'authentification lorsqu'il ne parvient pas à s'authentifier sur le portail captif

Vrai, dans tous les cas

Vrai, mais cela dépend de la politique d'authentification

Faux, l'utilisateur ne peut s'authentifier qu'avec une seule méthode

Une politique d'authentification peut se baser sur

Le port destination

La machine source

La machine destination

L'utilisateur ou le groupe d'utilisateurs

32. L'action "Bloquer" dans une règle de filtrage lève systématiquement une alarme

Faux

Vrai

33. Les paquets ICMP de type "echo reply" peuvent être tracés dans les logs de filtrage avec le niveau de trace standard sur une règle de filtrage

FAUX

34. Les réponses d'une connexion établie au travers du firewall doivent être autorisées explicitement dans les règles de filtrage

Vrai

Faux

35. Le nombre de règles de filtrage que peut gérer le firewall est

Limité en fonction du modèle

Limité à 1024

Limité à 2048

Illimité

36. Le niveau de traces d'une règle de filtrage est défini à standard, je tente d'établir une connexion sans succès, je peux visualiser les traces correspondantes dans le journal des connexions réseau

Oui

Non

37. Quelle est l'action appliquée par défaut si aucune règle de filtrage ne correspond au paquet reçu par le firewall ?

Passer

Bloquer

Conserver une trace

Eteindre le firewall

38. Les règles de filtrage implicites

Sont désactivables

Sont modifiables

N'ont pas d'utilité

Sont prioritaires sur les règles de filtrage explicites

39. Vous souhaitez configurer le filtrage afin de permettre l'accès à Internet depuis votre réseau interne. Vous voulez que vos utilisateurs puissent naviguer sur Internet, envoyer et recevoir des mails (vous disposez d'un serveur en interne par lequel l'ensemble des flux mails devra passer). Vous n'avez pas de serveur DNS interne. Quels flux devez-vous autoriser pour cela ?

Les flux SMTP depuis l'extérieur vers votre serveur mail

lLes flux SMTP depuis votre serveur mail vers l'extérieur

Les flux DNS depuis le réseau interne vers l'extérieur

Les flux POP3 depuis le réseau interne vers l'extérieur

Les flux HTTP et HTTPS depuis votre réseau interne vers l'extérieur

33. st-il possible de configurer plusieurs adresses IP sur une seule interface du firewall ?

Oui, mais seulement à partir du modèle SN510

Oui, dans tous les cas

Non, peu importe le modèle

Oui, mais seulement sur les interfaces ethernet 10 Gbps

43. Le compteur indiquant le nombre de fois où une règle de filtrage a été appliquée s'actualise en temps réel depuis la page d'administration web

Faux

Vrai

44. Un utilisateur authentifié peut être un critère d'application d'une règle de NAT

Vrai

Faux

45. Mon entreprise possède un serveur smtp et un serveur http. Ils sont situés dans une DMZ en adressage privé. Le firewall Stormshield Network permet de rendre joignable simultanément ces 2 services depuis Internet bien que mon fournisseur d'accès ne m'ait attribué qu'une seule IP publique

Vrai

Faux

46. Il est possible de faire de la redirection de port pour le protocole ICMP

Faux

Vrai

47. Vous devez configurer la translation d'adresses afin de permettre à une cinquantaine d'utilisateurs d'accéder à Internet. Quel type de translation utilisez-vous ?

Translation dynamique

Translation statique

Translation statique par port

48. Vous n'avez qu'une seule adresse IP publique disponible pour configurer votre firewall SNS. Vous avez une règle de translation permettant l'accès à Internet pour l'ensemble des machines internes. Vous devez maintenant permettre aux clients externes d'accéder à votre serveur web. Quelle translation utilisez-vous ?

Aucune translation

Translation statique

Translation dynamique

Translation statique par port

49. Quel type de translation nécessite la modification de l'adresse source et du port source sur les paquets translatés ?

Translation statique

Translation dynamique

Translation statique par port

9. Deux VLAN peuvent être rattachés à la même interface physique

O. Vrai

O Faux

50. Combien de phases sont nécessaires à l'établissement d'un tunnel VPN IPsec ?

Aucune 10 5 2 1 3

Question précédente

51. La fonction keepalive de VPN IPsec

Se configure en secondes

Doit être désactivée dans un environnement de haute sécurité*

Permet au firewall d'initier la négociation d'un tunnel avec un correspondant nomade

Provoque la négociation d'un tunnel VPN IPsec, même quand il n'y a pas de trafic applicable aux extrémités de trafic

52. Sur les firewalls Stormshield, la négociation des paramètres IPsec est assurée par le protocole

AHESPL2TPVPN

IKE

PPTP

53. IPsec est un standard

Internet (IETF)

Stormshield

IBM

CiscoCheckpoint

54. Les extrémités de trafic d'un tunnel IPsec représentent les machines/réseaux qui pourront communiquer au travers du tunnel

Vrai

Faux

57. Si une politique VPN IPsec est activée sur le firewall, chaque paquet arrivant au firewall sera soumis à cette politique

Vrai

Faux

58. J'ai à ma disposition un serveur DHCP connecté sur l'interface "dmz1". Puis-je utiliser ce serveur pour délivrer des adresses IP aux clients connectés sur l'interface "in" ?

Non, car les clients et le serveur ne sont pas sur le même réseau

Oui, en utilisant le routage par interface

Oui, en modifiant la configuration réseau pour créer un bridge entre les interfaces "in" et "dmz1"

46. **Un code d'accès pour un accès complet aux logs**

Peut être utilisé par plusieurs administrateurs

Est créé dans le menu Configuration > Notifications > Logs - Syslog

Ne peut être émis que par un administrateur ayant les droits correspondants

A une date de début et une date de fin

60. 172.30.0.1 est une adresse

Publique

Privée

Multicast

61. Nous souhaitons effectuer un routage par défaut avec une répartition de charge sur 3 passerelles. Une passerelle doit recevoir la moitié du trafic et les deux autres passerelles doivent se partager la moitié restante. Parmi les propositions suivantes, choisissez la (ou les) configuration(s) correctes) pour les poids des passerelles

GW1 : 4, GW2: 2, GW3: 2

GW1 : 3, GW2: 2, GW3: 1

GW1 : 2, GW2: 1, GW3: 1

GW1 : 8, GW2: 1, GW3: 1

62. Lors d'un routage sans NAT, quels champs de la trame sont modifiés à chaque passage par un routeur ?

Port source

Adresse IP de destination

Adresse ethernet (MAC) source

Port de destination

Adresse ethernet (MAC) de destination

Adresse IP source

63. Les routes statiques

N'ont pas d'utilité sur les firewalls Stormshield Network

Permettent de faire du routage en fonction de l'adresse IP source

Permettent au firewall de connaître le routeur derrière lequel se trouvent les réseaux distants

64. Quelles sont les particularités du mode "Transparent" ?

Chaque interface dispose de son propre plan d'adressage

Toutes les interfaces ont la même adresse IP

Certaines interfaces sont dans un bridge et d'autres ont leur propre plan d'adressage

Toutes les interfaces sont contenues dans un bridge (pont)

65. Pour l'adresse IP 194.12.27.33 et le masque 255.255.255.240, l'adresse réseau et l'adresse de diffusion sont respectivement

194.12.27.32 et 194.12.27.47

194.12.27.32 et 194.12.27.63

194.12.27.0 et 194.12.27.127

194.12.27.0 et 194.12.27.15

66. Pour quel(s) type(s) de routage est-il possible de configurer une répartition de charge vers plusieurs passerelles ?

Le routage par politique

Le routage statique

Le routage par défaut

Le routage dynamique

67. Pour une meilleure sécurité, on placera les serveurs publics (mail, Web, FTP,etc...)

De préférence dans une DMZ

De préférence dans le réseau des utilisateurs

De préférence sur un switch connecté à l'interface externe

68. Le nombre maximum d'interfaces

Dépend du modèle de firewall

Se modifie uniquement en ligne de commandes et nécessite un redémarrage du firewall

Peut être modifié depuis l'IHM mais nécessite un redémarrage du firewall

Peut être modifié depuis l'IHM et ne nécessite pas de redémarrage du firewall

Ne peut pas être modifié

69. Le protocole de gestion des erreurs de transmission est

NNTPIPX

ICMP

NTP

70. L'algorithme de répartition de charge utilisé dans les objets routeurs permet de répartir les paquets en fonction de

L'adresse IP destination seule

L'adresse IP source seule

Le quadruplet adresses IP source, adresse IP destination, port source et port destination (connexion)

Port destination seulement

Port source seulement

1. Est-il possible de tracer une règle de NAT ?

Oui

Non

2**. Sélectionnez les critères d'application d'une règle de NAT parmi la liste suivante (multi)**

La passerelle de sortie

Une adresse réseau

L'interface d'entrée

Le numéro de protocole

Un groupe d'utilisateurs

Une plage de ports destination

3. **Comment sont analysées les règles de NAT ?**

En donnant la priorité aux règles qui modifient l'adresse IP source

En donnant la priorité aux règles qui modifient l'adresse IP destination

En fonction de l'adresse IP source

Par ordre d'apparition dans la politique, c'est à dire de la première règle à la dernière

4. **Si j'utilise une adresse IP secondaire (alias) d'une interface (nommé Firewall_out_1) dans les règles de NAT, est-il nécessaire d'activer la publication ARP ?**

Oui

Non

5. **La translation statique permet de (multi)**

Translater une adresse IP privée en une adresse IP publique

Translater une adresse IP en un port pré-défini

Translater une adresse IP privée en N adresses IP publiques

Translater N adresses IP privées en une adresse IP publique

57. **Sur un firewall physique, peut-on basculer de la partition principale vers la partition de secours sans redémarrage ?**

Non

Oui

63. **Un serveur DNS permet**

De récupérer des alarmes

D'associer le nom d'une machine à une adresse IP

De translater l'adresse IP privée d'un serveur avec une adresse IP publique

D'envoyer des e-mails

8**. La sauvegarde automatique de configuration (auto-backup) (multi)**

S'effectue périodiquement, à une fréquence personnalisable

Peut être stockée sur un serveur personnalisé

Peut être stockée sur mystormshield.eu

Se configure uniquement en ligne de commandes

9. **Le service NTP (Network Time Protocol)**

Détermine lui-même l'heure locale grâce à un signal GPS

A besoin de connaître le fuseau horaire du firewall pour configurer correctement l'heure locale

Est soumis à une option de licence

10. La fréquence de téléchargement des mises à jour effectuées par Active Update se paramètre depuis l'interface d'administration des firewalls

Vrai

Faux

Il est possible de désactiver les mises à jour automatiques « Active Update » par module (check sur la VM)

Vrai

Faux

En configuration usine, le port d'administration du firewall est

Telnet (23/TCP)

HTTP (80/TCP)

SSH (22/TCP)

Aucun des ports proposés

la réponse sera https TCP 443 si jamais

13**. Sélectionner parmi les propositions les caractéristiques qui s'appliquent à une configuration usine (multi)**

Adresse IP des interfaces en 10.0.0.254/16

Serveur DHCP actif

Filtrage autorisant tout type de trafic

Configuration réseau en mode transparent (mode bridge)