STORMSHIELD

29. Le nombre maximum d'interfaces

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

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

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

O Ne peut pas être modifié

O Dépend du modèle de firewall

30. Les VLAN créés sur les firewalls SN respecent la norme

☐ ISO-3166

☐ RFC 894

☐ 802.1q

☐ Hyperlan

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

☐ Adresse ethernet (MAC) source

☐ Port source

☐ Adresse IP source

☐ Adresse ethernet (MAC) de destination

☐ Port de destination

☐ Adresse IP de destination

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

☐ Vrai V

☐ Faux

33. 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

34. Dans la configuration par défaut, quel est l'ordre d'évaluation des types de routage (1= plus prioritaire, 4= moins prioritaire)

☐ 1) Routage par politique (PBR) / 2) Routage statique / 3) Routage dynamique / 4) Passerelle par défaut V

☐ 1) Routage statique / 2) Routage par politique (PBR) / 3) Routage dynamique / 4) Passerelle par défaut

☐ 1) Routage statique / 2) Routage dynamique / 3)Routage par politique (PBR) / 4) Passerelle par défaut

☐ 1) Passerelle par défaut / 2) Routage dynamique / 3) Routage par politique (PBR) / 4) Routage statique

35. Les routes statiques

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

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

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

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

☐ Faux

☐ Vrai

37. Parmi les affirmations suivantes, cochez celles qui sont correctes

☐ Il est possible d'envoyer les logs par email

☐ Il est possible d'envoyer les logs vers quatre serveurs externes simultanément

☐ Sur les firewalls ne disposant pas de stockage local des journaux, l'historique maximum des graphes et rapports est limité à 30 jours

☐ Le trafic Syslog peut être chiffré

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

☐ Faux

☐ Vrai

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

☐ Pour tous les administrateurs

☐ Pour tous les administrateurs sauf le super administrateur admin V

☐ Depuis l'interface d'administration du firewall

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

☐ Effectuer une rotation automatique des fichiers de logs

☐ Arrêter l'écriture des logs

☐ Arrêter le firewall

☐ Envoyer un ping

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

☐ Faux

☐ Vrai V

42. Breach Fighter peut analyser les fichiers transitant via le(s) protocole(s)

☐ FTP

☐ ICMP

☐ HTTPS

☐ GRE

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

☐ Faux

☐ Vrai

44. 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 V

45. Dans le module "objets WEB", il est possible d'éditer les catégories d'URL de la base embarquée afin de lire leur contenu

☐ Faux

☐ Vrai V

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

☐ HTTPS

☐ HTTP et HTTPS

☐ HTTP

47. Sur les appliances PHYSIQUES SNS, il est possible de10

☐ Copier la partition active vers la partition passive

☐ Sauvegarder uniquement un slot de configuration depuis l'interface graphique

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

☐ Sauvegarder la configuration complète vers un fichier chiffré

48. Quels navigateurs sont officiellement supportés ?

☐ Microsoft Edge dernière version

☐ Opera dernière version

☐ Chrome dernière version

☐ Mozilla Firefox dernière version

49. La restauration d'une configuration

☐ Peut s'effectuer partiellement depuis une sauvegarde automatique

~~☐ 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~~

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

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

☐ Non

☐ Oui

51. L'administration du firewall peut être effectuée sur un port différent de TCP/443

☐ Faux

☐ Vrai

52. La sauvegarde automatique de configuration (auto-backup)

☐ Se configure uniquement en ligne de commandes

☐ Peut être stockée sur un serveur personnalisé

☐ S'effectue périodiquement, à une fréquence personnalisable

☐ Peut être stockée sur mystormshield.eu

53. Pour le compte "admin", le mot de passe de la configuration usine n'a jamais été modifié. L'interface d'administration affiche une erreur critique

☐ Non

☐ Oui

54. La partition active peut être sauvegardée

☐ Sur tous les modèles de firewalls

☐ Seulement sur les modèles de firewall physique

☐ Seulement sur les modèles de firewall virtuel

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

☐ Vrai

☐ Faux

56. 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 ?

☐ Faux

☐ Vrai

57. Combien de politiques de filtrage NAT locales peuvent être activées à la fois ?

☐ 1

☐ 10

☐ 3

☐ 5

58. 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

59. Parmi les paramètres suivants, quels sont ceux qui peuvent être utilisées dans une règle de filtrage ?

☐ Adresse IP destination

☐ Port destination (TCP ou UDP)

☐ Interface réseau d'entrée

☐ Adresse réseau source

☐ Message ICMP

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

☐ Faux

☐ Vrai

61. Il est possible d'activer le slot de filtrage numéro 5 et le slot de NAT numéro 1

☐ Vrai

☐ Faux

51. Comment sont analysées les règles de NAT ?

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

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

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

☐ En fonction de l'adresse IP source

52. 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 statique par port

☐ Translation statique

☐ Translation dynamique

53. 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 ?

☐ Non

☐ Oui

44. Parmi les affirmations suivantes, sélectionnez celles qui sont correctes

☐ Les règles de filtrage et de NAT globales sont accessibles depuis l'interface d'administration du firewall

☐ Les connexions autorisées par le filtrage implicite ne seront pas soumises à la politique de NAT active

☐ Les règles de filtrage sont traitées après les règles de NAT

☐ Le filtrage implicite ne contient aucune règle

☐ Les règles implicites peuvent être désactivées

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

☐ Faux

☐ Vrai

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

☐ Oui

☐ Non

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

☐ Faux

☐ Vrai

STORMSHIELD

48. Par défaut, quand l'action "passer" est sélectionnée, quel(s) protocole(s) est (sont) gérés de manière stateful par le module de prévention d'intrusion Stormshield Network ?

☐ PIM

☐ ESP

☐ L2TP

☐ aucun réponse

☐ GRE

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

☐ Vrai

☐ Faux

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

☐ Faux

☐ Vrai

41. Sélectionner parmi les propositions les caractéristiques qui s'appliquent à une configuration usine

- Adresse IP des interfaces en 10.0.0.254/16

- Serveur DHCP actif

- Configuration réseau en mode transparent (mode bridge)

- Filtrage autorisant tout type de trafic

40. La mise à jour système est possible

- Seulement lorsque la partition de secours est active

- Seulement lorsque la partition principale est active

- Peu importe la partition active

38. Quelle plage d'adresses IP est utilisée par le serveur DHCP en configuration d'usine ?

- 10.0.0.100 à 10.0.0.110

- 10.1.0.10 à 10.1.0.100

- 192.168.0.10 à 192.168.0.20

- 10.0.0.10 à 10.0.0.100

37. L'administrateur peut configurer le firewall via

- SSH

- Telnet

- console série

- Un navigateur web

35. La sauvegarde automatique de configuration (auto-backup)

- S'effectue périodiquement, à une fréquence personnalisable

- Se configure uniquement en ligne de commandes

- Peut être stockée sur un serveur personnalisé

- Peut être stockée sur mystormshield.eu

32. Un administrateur différent de "admin" peut accéder aux logs complets via un code d'accès

- Qu'un autre administrateur ayant des droits doit générer

- Non limité dans le temps

- Temporaire

- Qu'il peut générer lui-même

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

STORMSHIELD

- Base Microsoft Active Directory

- Base LDAP interne

- Base LDAP externe (ex: OpenLDAP)

61. Le portail d'authentification peut être accessible

- Depuis l'interface "out" seulement

- Depuis toutes les interfaces

- Depuis l'interface "in" seulement

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

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

- Vrai, mais cela dépend de la politique d'authentification

- Vrai, dans tous les cas

59. La limite du nombre de tunnels VPN SSL dépend

- Du modèle du firewall et de l'adresse réseau assignée aux clients

- De la version de firmware

- Du nombre de VPN IPsec actifs

- D'aucune des réponses citées

58. Par défaut, la durée de vie d'un tunnel VPN SSL est de

- 14400 secondes

- 3600 secondes

- 14000 secondes

- 36000 secondes

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

- Faux

- Vrai

56. Dans quel(s) module(s) du firewall la plage VPN SSL attribuée aux clients mobiles peut-elle être utilisée ?

~~- Le VPN IPsec~~

- Le NAT

- Le filtrage

55. Le droit d'accès VPN SSL est global à tous les utilisateurs

- Faux

- Vrai

54. Une interface peut disposer de deux adresses IP faisant partie du même réseau

- Faux

- Vrai

53. Dans un objet routeur, la passerelle de secours peut être activée quand

- Le nombre de passerelles disponibles est supérieur à un certain seuil

- Le nombre de passerelles disponibles est inférieur à un certain seuil

- Toutes les passerelles principales ne sont plus disponibles

- Une passerelle principale n'est plus disponible

63. En IKEv1, l'identité pouvant représenter un correspondant IPsec pendant la négociation de phase 1 d'un tunnel anonyme est

- Le numéro de série du produit
- Un nom de domaine pleinement qualifié (FQDN)

51. Si elle n'est pas utilisée, une route statique peut être désactivée depuis l'IHM

- Faux

- Vrai

50. Le nombre maximum d'interfaces

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

- Dépend du modèle de firewall

- Ne peut pas être modifié

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

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

49. Il est possible d'avoir plus de deux interfaces au sein d'un bridge

- Vrai

- Faux

48. L'adresse IP 135.1.1.0/23 est une adresse

- De réseau

- De broadcast

- D'hôte

- Privée

47. Le routage par politique est prioritaire sur la passerelle par défaut

- Vrai

- Faux

46. 172.30.0.1 est une adresse

- Publique

- Multicast

- Privée

45. Le firewall Stormshield Network peut jouer le rôle de serveur DHCP pour les machines du réseau local

- Vrai

- Faux

44. Les routes statiques

- 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

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

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

- Adresse ethernet (MAC) de destination

- Adresse IP de destination

- Port de destination

- Adresse IP source

- Adresse ethernet (MAC) source

- Port source

42. 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 194.12.27.63

- 194.12.27.0 et 194.12.27.15

- 194.12.27.0 et 194.12.27.127

- 194.12.27.32 et 194.12.27.47