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

☐ 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

☐ 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

☐ 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

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

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

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 de

☐ 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