Deux administrateurs peuvent être connectés simultanément avec les droits d'écriture sur un pare-feu Stormshield.
Faux

Les caractéristiques du pare-feu SN310
8 interfaces, 2.4 Gbps (IPS), 300 000 connexions simultanées, 600Mbps (VPN IPsec AES), Slot pour carte SD

Quel est le mot de passe et le compte administrateur par défaut du SNS ?
Login : admin, password : admin

Une translation dynamique (SNAT) peut être configurée au sein d'une règle de filtrage.
Faux

Par défaut, la valeur du Keepalive pour les tunnels VPN IPsec Site à Site est de :
0

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

Dois-je obligatoirement créer des règles de filtrage pour les flux émis par le pare-feu lui-même (NTP, mise à jour HTTPS, etc.) ?
Non

Je souhaite permettre à des utilisateurs de s'authentifier en LDAP, s'il n'est pas connu de mon LDAP je souhaite l'authentifier via SSO Agent. Est-ce possible ?
Non

Quelle directive de routage est la plus prioritaire ?
Route de retour

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

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

La fonctionnalité de VPN IPsec par interfaces virtuelles VTI est compatible avec les pares-feux :
Aucun autre à part Stormshield

Combien de politique de filtrage locale peuvent être actives à la fois ?
1

Sélectionnez la configuration cryptographique offrant la meilleure sécurité
Chiffrement AES-256, authentification SHA-2-256, groupe Diffie-Hellman 21 (ECC 521bits)

Mon entreprise possède un serveur SMTP et un server 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

Par défaut, la durée de vie d'un tunnel VPN SSL est de :
14400 secondes

Quelle est l'adresse IP par défaut du SNS ?
10.0.0.254/8

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

Lorsqu'un tunnel IPsec est défini entre deux passerelles Stormshield, avec une authentification par clé pré-partagées, les deux correspondants doivent impérativement utiliser la même clé pré-partagée. (Page 422)
Vrai

Le service NTP (Network Time Protocol)
A besoin de connaitre le fuseau horaire du firewall pour configurer correctement l'heure locale

En configuration usine, il est possible (si le matériel le supporte) de se connecter au firewall grâce :
Une connexion HTTPS
A un câble série
Un écran utilisant une connexion HDMI ou VGA

Il est conseillé de créer des comptes administrateur nominatifs et de désactiver le compte par défaut "admin" ?
Faux

Si je configure le réseau 172.16.37.0/24 comme réseau pour le VPN SSL, quelle IP aura le deuxième client ?
172.16.37.10

Le mécanisme de translation permet de
Cacher les adresses internes vis-à-vis de l'extérieur

Est-il possible de tracer une règle de NAT ?
Oui

Le droit d'accès VPN SSL est global à tous les utilisateurs (page 488)
Vrai
Faux

L'option automatique de l'objet réseau machine permet de faire périodiquement une résolution ARP de l'adresse IP (page 131)
Faux
Vrai

Un firewall en configuration usine (1 rep)
Bloque l'ensemble des flux
Bloque l'ensemble des flux sauf les pings et les ports d'administration
Laisse passer uniquement les pings
Laisse passer l'ensemble des flux

Les modems de la configuration réseau peuvent être de type (multi) (page 149)
PPPoE
PPTP
L2TP
HTTP
PPPoA

Quelles sont les particularités du mode « Transparent » ? (page 149)
Certaines interfaces sont dans un bridge et d'autres ont leur propre plan d'adressage
Toutes les interfaces sont contenues dans un bridge (pont)
Chaque interface dispose de son propre plan d'adressage
Toutes les interfaces ont la même adresse IP

Lorsque la base LDAP est interne au firewall, l'authentification des utilisateurs s'effectue obligatoirement par mot de passe (1 rep) (page 378)
Vrai, mais uniquement pour les utilisateurs qui ne possèdent pas de droits d'administration sur le firewall
Aucune des réponses proposées
Vrai, mais uniquement depuis les interfaces protégées
Faux
Vrai

Le portail d'authentification ne peut être personnalisé qu'en ligne de commandes (page 391)
Faux
Vrai

Un utilisateur est redirigé vers une autre méthode d'authentification lorsqu'il ne parvient pas à s'authentifier sur le portail captif (1 rep) (page 382)
Vrai, mais cela dépend de la politique d'authentification
Faux, l'utilisateur ne peut s'authentifier qu'avec une seule méthode
Vrai, dans tous les cas

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 ? (page 349)
Oui
Non

L'objet Network_internals contient (2 bonnes réponses)
Les réseaux privés définis par l'IETF dans la RFC 1918
Les réseaux des interfaces « dmz »
Les réseaux déclarés dans une route statique et joignables depuis une interface protégée
Les réseaux de toutes les interfaces du firewall
Le réseau de l'interface « in » tuteur
Les réseaux de toutes les interfaces protégées tuteur

Les règles implicites générées lors de l'activation d'une politique IPsec permettent (multi) (page 435)
D'autoriser le trafic au sein du tunnel
La négociation ISAKMP et la réception des paquets ESP d'un tunnel site à site
La négociation d'un tunnel nomade
La réception de paquets 4500/UDP

Lorsque la quantité d'espace disque allouée à une catégorie de log est atteinte, quelle(s) action(s) est(sont) possible(s) ? (multi) (page 82)
Envoyer un ping
Effectuer une rotation automatique des fichiers de logs
Arrêter l'écriture des logs
Arrêter le firewall

Sélectionnez les critères d'application d'une règle de NAT parmi la liste suivante (multi)
Une adresse réseau
La passerelle de sortie
Le numéro de protocole
L'interface d'entrée
Un groupe d'utilisateurs
Une plage de ports destination

La clé ISAKMP négociée lors de la phase 1 d'un VPN IPsec permet (1 rep) (Page 423)
De chiffrer les échanges effectués lors de la négociation de la phase 2
De déchiffrer le trafic ESP reçu
De chiffrer le trafic à envoyer par le protocole ESP

Est-il possible de tracer une règle de NAT ? (vu avec la VM)
Oui
Non

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 ? (1 rep)
Translation statique par port
Aucune translation
Translation dynamique
Translation statique

Sur les firewalls Stormshield, la négociation des paramètres IPsec est assurée par le protocole (1 rep) (page 420)
L2TP
IKE
ESP
VPN
AH
PPTP

En IKEv1, l'identité pouvant représenter un correspondant IPsec pendant la négociation de phase 1 d'un tunnel anonyme est (page 422)
Un nom de domaine pleinement qualifié (FQDN)
Le numéro de série du produit

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 (Page 61)
Oui
Non

Combien de phases sont nécessaires à l'établissement d'un tunnel VPN IPsec ? (1 rep)
2 (page 423)
5
Aucune
10
3
1

Lors de la création d'un VPN IPsec, si je paramètre une authentification par PSK, cela signifie (1 rep)
Par certificat
Par clé pré-partagée (page 420)
Par authentification RADIUS
Par authentification LDAP

Si je veux établir des communications chiffrées entre mon LAN et le LAN d'un prestataire, ainsi qu'entre ma DMZ et le LAN du prestataire, combien de correspondants IPsec différents dois-je définir ? (1 rep)
2
4
5
1
3
Aucun

La partition active peut être sauvegardée (1 rep) (page 66 et 72)
Seulement sur les modèles de firewall virtuel
Seulement sur les modèles de firewall physique
Sur tous les modèles de firewalls

Quel que soit le client nomade utilisé (VPN SSL Stormshiel ou OpenVPN), il récupère automatiquement les paramètres de configuration depuis le portail captif (page 484)
Faux
Vrai

La fréquence de téléchargement des mises à jour effectuées par Active Update se paramètre depuis l'interface d'administration des firewalls (check sur la VM)
Faux
Vrai

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

Chaque utilisateur se connectant via un tunnel VPN SSL est automatiquement authentifié au niveau du firewall (page 486)
Faux
Vrai

La limite du nombre de tunnels VPN SSL dépend (multi) (page 481)
Du modèle du firewall et de l'adresse réseau assignée aux clients

D'aucune des réponses citées
De la version de firmware
Du nombre de VPN IPsec actifs

Pour l'adresses IP 194.12.27.33 et le masque 255.255.255.240, l'adresse réseau et l'adresse de diffusion sont respectivement (1 rep)
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

Sélectionner parmi les propositions les caractéristiques qui s'appliquent à une configuration usine (multi) (page 49)
Configuration réseau en mode transparent (mode bridge)
Filtrage autorisant tout type de trafic
Serveur DHCP actif
Adresse IP des interfaces en 10.0.0.254/16

Dans la configuration par défaut, quel est l'ordre d'évaluation des types de routage (1= plus prioritaire, 4= moins prioritaire) (1 rep) (page 184)
1) Routage par politique (PBR) / 2) Routage statique / 3) Routage dynamique / 4) Passerelle par défaut
1) Routage statique / 2) Routage dynamique / 3) Routage par politique (PBR) / 4) Passerelle par défaut
1) Routage statique / 2) Routage par politique (PBR) / 3) Routage dynamique / 4) Passerelle par défaut
1) Passerelle par défaut / 2) Routage dynamique / 3) Routage par politique (PBR) / 4) Routage statique

Le module de prévention d'intrusion (IPS) des firewalls Stormshield Network est (page 18)
Propriétaire
Libre (open source)

L'algorithme de répartition de charge utilisé dans les objets routeurs permet de répartir les paquets en fonction de (multi) (page 175)
Port source seulement
Le quadruplet adresses IP source, adresse IP destination, port source et port destination (connexion)
Port destination seulement
L'adresse IP source seule
L'adresse IP destination seule

Un firewall SNS est capable (multi)
D'authentifier les utilisateurs
D'agir comme un routeur
De filtrer le trafic selon un port
De filtrer selon un protocole

Une interface peut disposer de deux adresses IP faisant partie du même réseau (page 154)
Vrai
Faux

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) correcte(s) pour les poids des passerelles (multi)
GW1 : 3, GW2 : 2, GW3 : 1

GW1 : 4, GW2 : 2, GW3 : 2
GW1 : 8, GW2 : 1, GW3 : 1
GW1 : 2, GW2 : 1, GW3 : 1

En utilisant un objet routeur dans le routage par défaut, est-il possible de bloquer (ne pas router) les paquets si aucune passerelle n'est disponible ? (page 184)
Non
Oui

Dans un objet routeur, la passerelle de secours peut être activée quand (multi)(page 180)
Le nombre de passerelles disponibles est inférieur à un certain seuil
Une passerelle principale n'est plus disponible
Toutes les passerelles principales ne sont plus disponibles
Le nombre de passerelles disponibles est supérieur à un certain seuil

Dans la politique de filtrage URL, il est possible de sélectionner une page de blocage spécifique par catégorie d'URL (page 310)
Faux
Vrai

Le nombre maximum d'interfaces (1 rep)(page 20)
Peut être modifié depuis l'IHM et ne nécessite pas de redémarrage du firewall
Dépend du modèle de firewall
Peut être modifié depuis l'IHM mais nécessite un redémarrage du firewall
Se modifie uniquement en ligne de commandes et nécessite un redémarrage du firewall
Ne peut pas être modifié

Dans le module « objets WEB », il est possible d'éditer les catégories d'URL de la base embarquée afin de lire leur contenu (page 315)
Vrai
Faux

Lors d'un routage sans NAT, quels champs de la trame sont modifiés à chaque passage par un routeur ? (multi)
Adresse IP source
Port de destination
Adresses ethernet (MAC) source
Adresse ethernet (MAC) de destination
Port source
Adresse IP de destination

Les routes statiques (1 rep)
N'ont pas d'utilité sur les firewalls Stormshield Network
Permettent au firewall de connaitre le routeur derrière lequel se trouvent les réseaux distants
Permettent de faire du routage en fonction de l'adresse IP source

Il est possible d'arrêter l'écriture des évènements pour une catégorie de trace (Page 82)
Vrai
Faux

Les traces du firewall peuvent être stockées en local sur (multi) (page 33)
Les firewalls virtuels

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

La mise en œuvre du Règlement Général sur la Protection des Données (RGPD) restreint l'accès aux logs (multi)(page 86)
Pour tous les administrateurs sauf le super administrateur admin
Depuis l'interface d'administration du firewall
Pour tous les administrateurs
En interface web et dans le Real-Time Monitor
Seulement en Interface web

L'administration du firewall peut être effectuée sur un port différent de TCP/443 (page 57à
Faux
Vrai

La mise à jour système est possible (1 rep) (page 66 et 72)
Seulement lorsque la partition de secours est active
Peu importe la partition active
Seulement lorsque la partition principale est active

La sauvegarde automatique de configuration (auto-backup) (multi) (pages 68-69)
Peut être stockée sur mystormshield.eu
Peut être stockées sur un serveur personnalisé
S'effectue périodiquement, à une fréquence personnalisable
Se configure uniquement en ligne de commandes

L'administrateur peut configurer le firewall via (multi) (pages 46)
Telnet
Console série
Un navigateur web
SSH

Quelle plage d'adresses IP est utilisée par le serveur DHCP en configuration d'usine ? (1 rep) p49
10.1.0.10 à 10.1.0.100
10.0.0.100 à 10.0.0.110
192.168.0.10 à 192.168.0.20
10.0.0.10 à 10.0.0.100

Si elle n'est pas utilisée, une route statique peut être désactivée depuis l'IHM (Page 169)
Vrai
Faux

Je dois installer un firewall Stormshield Network au sein d'un réseau existant. La configuration actuelle est composée d'un routeur relié directement au LAN. Le routeur est la passerelle par défaut de l'ensemble des machines internes. Je souhaite sécuriser ce réseau en ne modifiant ni la configuration du routeur, ni la configuration des stations de travail. Quel mode est le plus approprié à ce type d'architecture ? (1 rep) (Page 169)
Mode Furtif (stealth)
Mode Hybride
Mode Transparent (bridge)
Mode Avancé (routé)

Il est possible de faire de la redirection de port pour le protocole ICMP
Faux
Vrai

172.30.0.1 est une adresse (1 rep)
Privée
Publique
Multicast

Le routage par politique permet de définir (multi)
Une route pour un type de trafic ciblé (SMTP, POP3, etc.) (page 174)
Une route de secours en cas de défaillance de la passerelle par défaut (page 184)
Une route en fonction de l'IP source et destination simultanément
Une deuxième route pour la répartition de charge (page 184)

Est-il possible de configurer plusieurs adresses IP sur une seule interface du firewall ? (1 rep) (Page 154)
Non, peu importe le modèle
Oui, dans tous les cas
Oui, mais seulement à partir du modèle SN510
Oui, mais seulement sur les interfaces ethernet 10 Gbps

Il est possible d'avoir plus de deux interfaces au sein d'un bridge (page 149)
Vrai
Faux

La fonction keepalive de VPN IPsec (multi) (Page 434)
Provoque la négociation d'un tunnel VPN IPsec, même quand il n'y a pas de trafic applicable aux extrémités de trafic
Permet au firewall d'initier la négociation d'un tunnel avec un correspondant nomade
Doit être désactivée dans un environnement de haute sécurité
Se configure en secondes

La directive « Via Tunnel VPN IPsec » des règles de filtrage permet de forcer l'émission du trafic correspondant dans le tunnel VPN IPsec (page 436)
Vrai
Faux

IPsec est un standard (1 rep)
IBM
Cisco
Stormshield
Checkpoint
Internet (IETF)

Comment sont analysées les règles de NAT ? (1 rep) (Connaissances)
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
En donnant la priorité aux règles qui modifient l'adresse IP source
En donnant la priorité aux règles qui modifient l'adresse IP destination

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

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

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

Par défaut, seul le super administrateur "admin" peut accéder aux logs complets en cliquant sur "Accès restreint aux logs"(page 86)

Faux

Vrai

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

Redémarrer le firewall

Ne rien faire

Analyser les serveurs

Analyser les traces

Un administrateur différent de "admin" peut accéder aux logs complets via un code d'accès (page 87)

Qu'il peut générer lui-même

Qu'un autre administrateur ayant des droits doit générer -> Si multi

Temporaire

Non limité dans le temps

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

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

Si je réserve le réseau 10.8.0.0/23 aux clients se connectant par le biais du VPN SSL, le nombre maximum de clients VPN SSL connectés simultanément est de (page 583)
64
128
126
63
Aucune des réponses proposées

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

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_

Les objets commençant par Network_ peuvent être modifiés dans la base d'objets par l'utilisateur (pas ce qu'on avait mis mais vérifié sur la VM) (page 129)
Vrai
Faux

Lors de la création d'un objet FQDN, l'adresse IP par défaut peut être obtenue par une résolution DNS (connaissance) (page 131)
Faux
Vrai

Le filtrage par SNI (nom de certificat) permet de bloquer l'accès à des sites web. Il est utilisable sur les protocoles (page 321)
HTTPS
HTTP
HTTP et HTTPS

L'analyse antivirale peut s'appliquer à des flux (page 331)
ICMP
SSH
SMTP (page 331)
HTTPS, si déchiffrement préalable http
HTTP

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

Breach Fighter fonctionne uniquement avec l'option "Antivirus avancé" (page 328)
Faux
Vrai

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

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

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

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

Dans une connexion FTP, le mode de traces avancé dans une règle de filtrage est-il nécessaire pour journaliser le trafic FTP ? (page 1021 w/doc SS)
Non
Oui

Pour tracer toutes les requêtes PING, je dois (page 295)
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"

Dans une règle de filtrage, il est possible de renseigner plusieurs objets FQDN comme objets de destination
Faux (page 283)
Vrai

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

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

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
Adresse MAC destination

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

Quelles inspections de sécurité peuvent être activées dans la politique de filtrage
Filtrage URL
Analyse antispam
Filtrage SMTP (page 287)
Antiphishing
Analyse antivirale (page 266)

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

Le service VPN SSL peut fonctionner sur le port (multi)
TCP/443
TCP/389
UDP/1194
TCP/4343

Donnez un équivalent à l'objet "Internet"
Network_in
Network_out
Différent de Firewall_internals
Any
Différent de Network_internals

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

Il est possible de visualiser les journaux (logs) ou une portion des journaux via (page 83)
L'interface d'administration du firewall
Wireshark
Stormshield Real Time Monitor
Stormshield Visibility Cerner

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"

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 (page 67)

Lors de la connexion sur l'interface d'administration de mon firewall, le navigateur remonte un problème de sécurité (page 57):
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

Une politique d'authentification peut se baser sur
Le port destination
La machine source
La machine destination
L'utilisateur ou le groupe d'utilisateurs

Quelles bases LDAP peuvent être configurées sur un firewall Stormshield Network ? (ChatGPT)
Base LDAP externe (ex: OpenLDAP)
Base LDAP interne
Base Microsoft Active Directory

L'action "Bloquer" dans une règle de filtrage lève systématiquement une alarme
Faux
Vrai

Le nombre de règles de filtrage que peut gérer le firewall est (page 266)
Limité en fonction du modèle
Limité à 1024
Limité à 2048
Illimité

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 (page 279)
Oui
Non

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

Les règles de filtrage implicites
Sont désactivables (page 272)
Sont modifiables
N'ont pas d'utilité
Sont prioritaires sur les règles de filtrage explicites

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
Les 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

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 (page 241)
Faux
Vrai

Quel type de translation nécessite la modification de l'adresse source et du port source sur les paquets translatés ? (page 226)
Translation statique
Translation dynamique
Translation statique par port

Les extrémités de trafic d'un tunnel IPsec représentent les machines/réseaux qui pourront communiquer au travers du tunnel (page 427)
Vrai
Faux

Les règles implicites générées lors de l'activation d'une politique IPsec permettent (page 435)
La réception de paquets 4500/UDP
D'autoriser le trafic au sein du tunnel
La négociation ISAKMP et la réception des paquets ESP d'un tunnel site à site
La négociation d'un tunnel nomade

Quels types de VPN puis-je établir entre deux firewalls Stormshield Network ? (page 418)
VPN SSL
VPN PPTP
OpenVPN
VPN IPsec

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

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"

Pour quel(s) type(s) de routage est-il possible de configurer une répartition de charge vers plusieurs passerelles ? (j'avais lu dans le MAN, page à retrouver)
Le routage par politique
Le routage statique
Le routage par défaut
Le routage dynamique

Pour une meilleure sécurité, on placera les serveurs publics (mail, Web, FTP, etc.)(connaissances)
De préférence dans une DMZ
De préférence dans le réseau des utilisateurs
De préférence sur un switch connecté à l'interface externe

Le protocole de gestion des erreurs de transmission est
NNTP
IPX
ICMP
NTP

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

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

La définition d'une route statique nécessite la configuration d'une interface de sortie
Faux
Vrai

P: 169

L'adresse IP 135.1.1.0/23 est une adresse
De broadcast
De réseau
Privée
D'hôte

Parmi les affirmations suivantes, sélectionnez celles qui sont correctes (multi)
Par défaut, le routage par politique est plus prioritaire que le routage statique en version 3 et 4 du firmware
La passerelle par défaut est la route la plus prioritaire
La route de retour est la plus prioritaire (page 184)
Seul le routage par politique est plus prioritaire que le routage dynamique
La passerelle par défaut est la route la moins prioritaire

Les interfaces vlan sont toujours internes (protégées)
Faux
Vrai

Le portail d'authentification peut être accessible (Page 386)
Depuis l'interface "out" seulement
Depuis toutes les interfaces
Depuis l'interface "in" seulement

Il est possible de personnaliser la page de blocage utilisée dans le filtrage URL (page 319)
Faux
Vrai

Le filtrage URL permet de filtrer (multi) (page 308)
Les requêtes HTTP
Les requêtes HTTPS sans déchiffrement
Les e-mails
Les requêtes FTP

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
Vrai (page 423)
Faux

Il est possible d'arrêter l'écriture des événements pour une catégorie de trace
Vrai
Faux
P: 82

Est-il possible de modifier le pourcentage d'espace disque réservé qu'occupe une famille de traces ? (vu en TP) p82
Oui
Non

Parmi les affirmations suivantes, cochez celles qui sont correctes (multi) p114
Il est possible d'envoyer les logs vers quatre serveurs externes simultanément
Il est possible d'envoyer les logs par email
Le trafic Syslog peut être chiffré
Sur les firewalls ne disposant pas de stockage local des journaux, l'historique maximum des graphes et rapports est limité à 30 jours

Les objets routeurs (multi) p179
Permettent de configurer une répartition de charge sur plusieurs passerelles p175
Sont utililisés par les routes statiques p175
Ne peuvent avoir qu'une seule passerelle de secours
Permettent de tester la disponibilité des passerelles p167

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 ? (multi) p286
ESP
Aucune réponse
PIM
GRE
L2TP

Les règles de filtrage sont traitées
De la plus restrictive à la moins restrictive
En commençant par les règles passantes
En commençant par les règles bloquantes
Par ordre d'apparition dans la politique
De la moins restrictive à la plus restrictive

Il est possible d'activer le slot de filtrage numéro 5 et le slot de NAT numéro 1
Vrai
Faux

Il est possible de créer une liste de ports destination dans une seule et même règle de filtrage
Vrai
Faux
Page 265/492 sns-fr-manuel_d'utilisation_et_de_configuration-v3.11.27-LTSB - 18/10/2023

Parmi les affirmations suivantes, sélectionnez celles qui sont correctes (multi)
Les connexions autorisées par le filtrage implicite ne seront pas soumises à la politique de NAT active
Le filtrage implicite ne contient aucune règle
Les règles implicites peuvent être désactivées
Les règles de filtrage sont traitées après les règles de NAT
Les règles de filtrage et de NAT **globales** sont accessibles depuis l'interface d'administration du firewall
P: 273

L'opération de NAT qui modifie l'adresse IP et le port source
Est uniquement configurable dans la politique de NAT
Modifie le port destination dans tous les cas
Peut être définie dans une règle de filtrage et sera analysée en priorité sur les règles définies dans l'onglet NAT de la politique active
Doit impérativement être définie dans le filtrage

La fonctionnalité VPN SSL permet uniquement à des postes Windows d'accéder aux ressources d'un réseau protégé
Faux
Vrai
P: 482
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 ? (page 317)
Oui
Non

Le chiffrement des paquets IP au sein d'un tunnel IPsec est assuré par le protocole (page 421, 423)
GRE
AH
L2TP
PPTP
ESP

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

Quels navigateurs sont officiellement supportés ?
Chrome dernière version
Microsoft Edge dernière version
Opera dernière version
Mozilla Firefox dernière version

La création d'objets réseaux s'effectue seulement depuis le menu Configuration > Objets > Objets Réseaux (ChatGPT, à voir si c'est seulement par là)
Vrai
Faux
C'est fauux on peut le créer qd on fait une politique de filtrage directement là bas sans revenir au menu config objets réseaux
Le Règlement Général sur la Protection des Données (RGPD) a une incidence sur la gestion des logs
Faux
Vrai

Les VLAN créés sur les firewalls SN repectent la norme (1 rep)
802.1q
Hyperlan
ISO-3166
RFC 894
P:159
Sur un firewall physique, peut-on basculer de la partition principale vers la partition de secours sans redémarrage ?
Oui
Non
P: 72
L'utilisation de l'option Extended Web Control pour le filtrage URL permet d'éviter le stockage local de la base URL Stormshield

Vrai
Faux
P: 308 309

Pour connaitre la catégorie URL dans laquelle est présente un site, je peux

Utiliser le bouton « Classifier » des modules « Objets WEB » ou « Filtrage URL »
Il n'existe aucun moyen de faire cette recherche
Utiliser le bouton « Vérifier l'utilisation » du module « Objets réseau »
P: 315

Les firewalls Stormshield Network analysent les connexions provenant de l'extérieur seulement

Vrai
Faux

Le firewall peut récupérer automatiquement l'adresse IP de sa passerelle par défaut, dans le cas où l'interface est configurée en DHCP

Vrai
Faux
P: 167

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

Vrai
Faux
Page 288/492 sns-fr-manuel_d'utilisation_et_de_configuration-v3.11.27-LTSB - 18/10/2023

Un tunnel VPN IPsec peut être monté entre

Un firewall Stormshield et un client mobile IPSec
Deux Firewalls StromShield
Un Firewall Stormshield et un client VPN Stormshield
Un firewall Stormshield et un équipement compatible IPsec
Page 430/492 sns-fr-manuel_d'utilisation_et_de_configuration-v3.11.27-LTSB - 18/10/2023

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

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?

- 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