Stormshield

Montage d’un pare-feu

Table des matières

[Introduction : 2](#_Toc199490000)

[Pré-installation physique : 2](#_Toc199490001)

[Pré-installation virtuelle : 3](#_Toc199490002)

[Mise en place de la licence : 3](#_Toc199490003)

[Système : 9](#_Toc199490004)

[Politique de sécurité : 12](#_Toc199490005)

[Filtrage : 12](#_Toc199490006)

[NAT : 16](#_Toc199490007)

[SSL : 16](#_Toc199490008)

[URL : 17](#_Toc199490009)

[SMTP : 17](#_Toc199490010)

[Qualité de service : 17](#_Toc199490011)

[Règles implicites : 18](#_Toc199490012)

[Réseau : 19](#_Toc199490013)

[Routage : 19](#_Toc199490014)

[DHCP : 19](#_Toc199490015)

[Interfaces virtuelles : 21](#_Toc199490016)

[Routage dynamique : 21](#_Toc199490017)

[Multicast : 21](#_Toc199490018)

[DNS dynamique : 21](#_Toc199490019)

[Proxy cache DNS : 21](#_Toc199490020)

[Objet : 21](#_Toc199490021)

[Réseau : 21](#_Toc199490022)

[URL : 22](#_Toc199490023)

[Services web : 22](#_Toc199490024)

[Certificats pki : 22](#_Toc199490025)

[Protection applicative : 23](#_Toc199490026)

[VPN : 23](#_Toc199490027)

[IPsec : 23](#_Toc199490028)

[SSL Portail : 25](#_Toc199490029)

[SSL : 27](#_Toc199490030)

[Notifications : 27](#_Toc199490031)

[Installation physique : 28](#_Toc199490032)

[Installation chez le client : 28](#_Toc199490033)

[Utilisateurs : 28](#_Toc199490034)

[Droits d’accès : 28](#_Toc199490035)

[Authentification : 28](#_Toc199490036)

[Enrôlement : 28](#_Toc199490037)

[Configuration des annuaires : 28](#_Toc199490038)

[Conclusion : 28](#_Toc199490039)

[Sources : 28](#_Toc199490040)

# Introduction :

J’ai remplacé le pare-feu Stormshield chez un petit client qui possède une infrastructure assez simple : quelques postes de travail, une box Internet et un serveur principal utilisé pour la gestion de son activité. L’ancien pare-feu était devenu trop vieux et ne recevait plus de mises à jour, ce qui représentait un vrai risque de sécurité. Il était donc important de le changer pour un modèle plus récent. J’ai repris l’ensemble des règles de l’ancien pare-feu pour que le réseau continue à fonctionner normalement, sans gêner les utilisateurs. J’ai aussi ajouté des règles spécifiques pour permettre aux techniciens de se connecter facilement à distance en cas de problème. Cette configuration reste légère, car le client n’a pas de services complexes, mais elle garantit une bonne sécurité et un accès rapide pour l’assistance technique.

# Pré-installation physique :

Une image contenant câble, fils électriques, Appareils électroniques, Ingénierie électronique

Le contenu généré par l’IA peut être incorrect.

J’ai commencé par installer l’alimentation (power 1), on peut avoir deux câbles d’alimentation pour la redondance mais comme Stormshield en fournissait qu’un, j’en ai branché qu’un seul. Il ne sera pas stocké dans la salle de préparation lors de sa mise en service.

J’ai ensuite branché les câbles pour connecter mon pare-feu à internet (port 1, fil blanc) et à mon PC (port 2, fil bleu). Cet ordre est très important car les ports ont été configurés pour marcher comme ça :Une image contenant texte, livre, encre, intérieur

Le contenu généré par l’IA peut être incorrect.

Une image contenant Appareils électroniques, Appareil électronique, texte, câble

Le contenu généré par l’IA peut être incorrect.

On voit les voyants lumineux : ici, les ports 1 et 2 sont actifs (LED verte), ce qui signifie qu'ils sont connectés. Le voyant "STATUS" est vert, donc l'équipement est en ligne et fonctionne normalement. Je vérifie ici que mes branchages ont été faits comme il faut.

# Pré-installation virtuelle :

## Mise en place de la licence :

Une image contenant texte, ordinateur, logiciel, capture d’écran

Le contenu généré par l’IA peut être incorrect.

Ensuite je me connecte sur l’interface web pour le configurer. L’adresse IP par défaut est 10.0.0.254/admin et le mot de passe et l’identifiant sont admin par défaut.

Une image contenant texte, ordinateur, logiciel, Système d’exploitation

Le contenu généré par l’IA peut être incorrect.

Je suis maintenant connecté à l’interface web d’administration du Stormshield. On y voit le tableau de bord du pare-feu, avec :

* Les ports physiques en haut (seuls les ports 1 et 2 sont utilisés)
* La version installée (4.3.17) et le modèle du boîtier (SN S Series 220)
* Plusieurs alertes critiques à droite : le mot de passe admin est encore celui par défaut (à changer rapidement), certaines bases IP ne sont pas accessibles, et plusieurs interfaces sont hors service (igb0 à igb3).

Je m’en occuperai après la mise à jour. Pour ça il faut connecter le pare-feu à internet.

Une image contenant texte, capture d’écran, logiciel, Page web

Le contenu généré par l’IA peut être incorrect.

Je commence par de mettre en droit d’écriture pour modifier ou rajouter des choses. Par défaut il est sur lecture seule.

Une image contenant texte, capture d’écran, logiciel, Page web

Le contenu généré par l’IA peut être incorrect.

Ensuite dans configuration, réseau et interface, je vais configurer le port n°8, celui pour sortir sur internet habituellement utilisé par l’entreprise pour ne pas gêner lors de la configuration des ports pour le client. Je lui assigne une IP statique puis je lui donne une adresse IP dans le réseau de préparation.

Une image contenant texte, logiciel, capture d’écran, nombre

Le contenu généré par l’IA peut être incorrect.

Je la mets en externe pour qu’elle puisse avoir accès à internet.

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Le contenu généré par l’IA peut être incorrect.

Je passe ensuite le bridge en /24 pour qu’elle soit dans le même réseau que mon interface. Cela permet d'associer plusieurs interfaces réseau tout en les traitant comme un seul segment, ce qui pourra appliquer des règles de sécurité tout en laissant passer le trafic entre les équipements connectés.

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Le contenu généré par l’IA peut être incorrect.

Je rajoute l’accès internet à mon interface que j’ai configuré pour que je puisse me connecter dessus.

Une image contenant texte, Police, capture d’écran, nombre

Le contenu généré par l’IA peut être incorrect.

Je crée ici un objet de type machine dans l’interface de gestion Stormshield, que je nomme GW\_PREPA. Je lui attribue l’adresse IP statique de la passerelle de la prépa. Mon pare-feu peut donc sortir sur internet :

Une image contenant texte, capture d’écran, Police, nombre

Le contenu généré par l’IA peut être incorrect.

Je teste en faisant un ping en ligne de commande dans mon pare-feu vers google pour vérifier qu’il accède à internet.

Je dois activer la licence sur le site de Stormshield pour que le pare-feu fasse les mises à jour automatiquement.

Une image contenant texte, logiciel, Page web, Site web

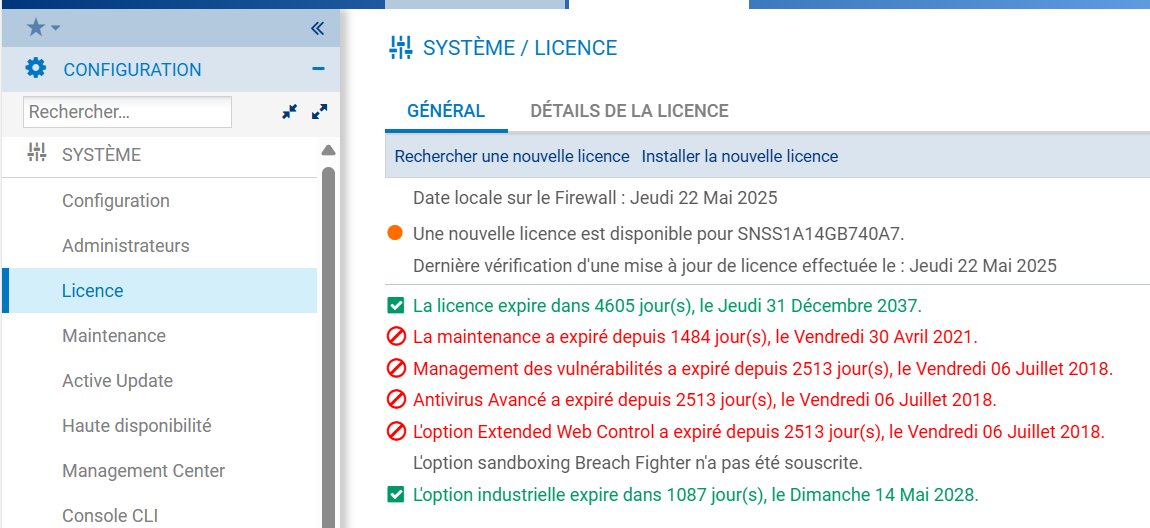
Le contenu généré par l’IA peut être incorrect.

Dans la section Produit, Enregistrement d’un produit, j’ai enregistré une appliance SNS afin d’activer officiellement la licence Stormshield associée à notre équipement. En déclarant notre Appliance, on associe son numéro de série au compte entreprise, ce qui garantit que le matériel est reconnu comme authentique et bénéficie de tous les droits liés à la licence acquise.

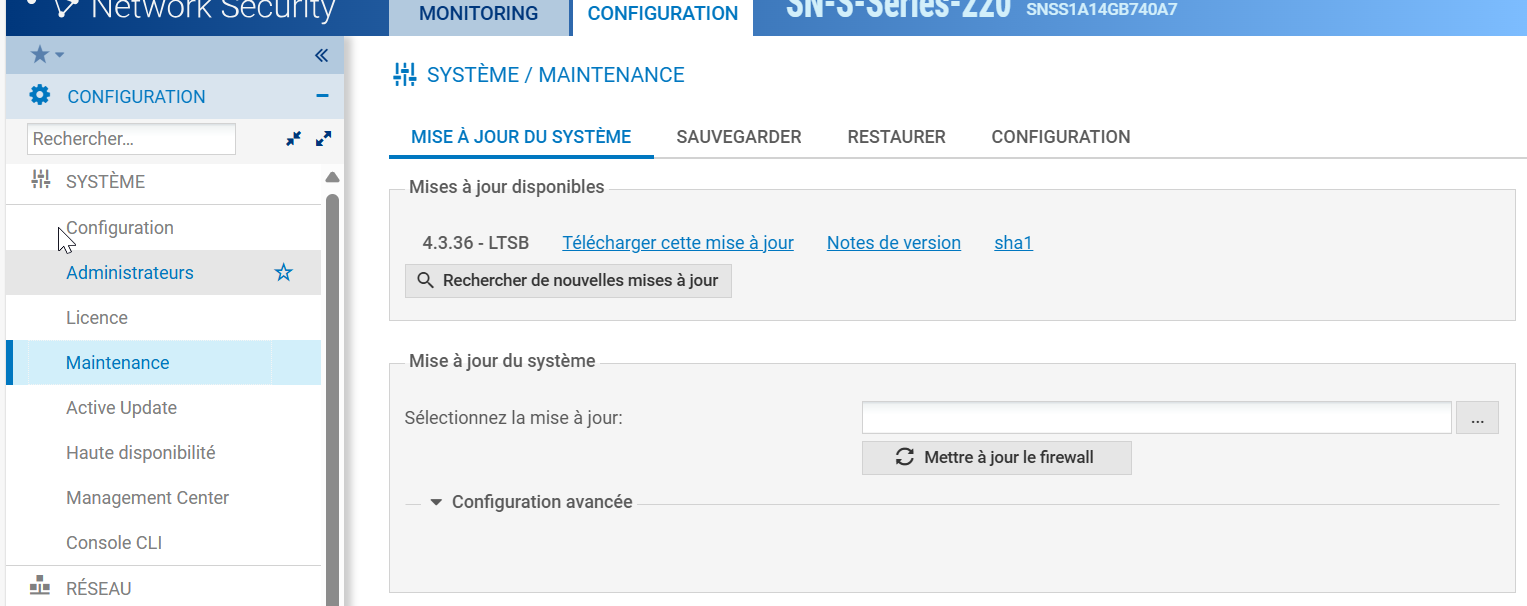
Une image contenant texte, capture d’écran, Page web, logiciel

Le contenu généré par l’IA peut être incorrect.

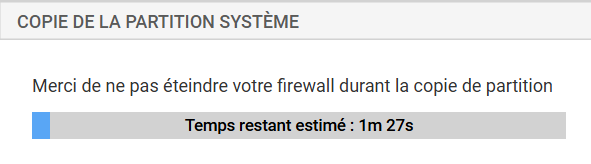
Je tape le mot de passe et l’identifiant qu’il y a sur le boitier physique pour l’activer.



Ici j’installe la licence qui va permettre de tenir à jour notre pare-feu. Il la cherche sur internet puis je l’installe.



Je peux maintenant faire ma mise à jour, je la cherche sur mon ordinateur. On l’a récupéré sur le site de Stormshield et on a pris une version de janvier 2025, assez récente mais pas trop pour éviter les bugs.



Il va d’abord sauvegarder automatiquement puis enregistrer la licence au cas où ça se passe mal, on pourra reconfigurer notre Stormshield.

## Système :

Une image contenant texte, capture d’écran, logiciel, Page web

Le contenu généré par l’IA peut être incorrect.

Ici je change la langue et le clavier en Français pour faciliter la configuration. Je change aussi la date et l’heure pour qu’il se synchronise avec un serveur NTP et je lui indique le fuseau horaire à utiliser. Je garde les paramètres par défaut car ils me conviennent et sont sécurisé.

Une image contenant texte, logiciel, Icône d’ordinateur, Page web

Le contenu généré par l’IA peut être incorrect.

Ensuite je change le port sur lequel on peut accéder via internet. Je serai obligé de le taper dans ma barre de recherche. C’est pour plus de sécurité.

Une image contenant texte, Police, capture d’écran

Le contenu généré par l’IA peut être incorrect.

Je change d’adresse IP en rajoutant le bon port.

Une image contenant texte, capture d’écran, logiciel, Page web

Le contenu généré par l’IA peut être incorrect.

Je change aussi le mot de passe admin pour que ça ne soit plus celui par défaut et que tout ce qui ont le port, l’adresse IP et qui sont dans le réseau attribuer.

Une image contenant texte, Police, ligne, capture d’écran

Le contenu généré par l’IA peut être incorrect.

Dans cette configuration DNS, j’indique les serveurs que le pare-feu doit utiliser pour résoudre les noms de domaine. J’ajoute d’abord les serveurs publics de Google (dns1.google.com et dns2.google.com) pour que mon pare-feu ait internet, le dns du client n’étant pas atteignable de trop loin. J’ajoute aussi le serveur interne.

Une image contenant texte, capture d’écran, Police, logiciel

Le contenu généré par l’IA peut être incorrect.

Je configure ici les serveurs NTP (Network Time Protocol) que le pare-feu utilisera pour se synchroniser à l’heure. J’ajoute deux serveurs recommandés par l’éditeur (ntp1.stormshieldcs.eu et ntp2.stormshieldcs.eu) pour garantir une synchronisation fiable et sécurisée. En complément, j’ajoute un serveur NTP universitaire français (ntp.univ-lyon.fr) pour bénéficier d’une source tierce indépendante. Cette redondance permet d'assurer la cohérence temporelle des logs et le bon fonctionnement des protocoles sensibles à l’heure.

Une image contenant texte, capture d’écran, Police, logiciel

Le contenu généré par l’IA peut être incorrect.

Ici, je définis les machines autorisées à accéder à l’interface d’administration du pare-feu. Je limite cet accès à Network\_dmz6, au poste de télémaintenance telem.megao.com et au domaine vpn.megao.com pour le dépannage et la configuration du firewall, ce qui permet de sécuriser l’administration à quelques postes de confiance. Ce choix réduit considérablement les risques d'accès non autorisé à l'interface d'administration.

## Politique de sécurité :

### Filtrage :

Une image contenant texte, capture d’écran, Police, nombre

Le contenu généré par l’IA peut être incorrect.

Pour mon filtrage NAT, je mets en place le filtre à 5, au milieu de l’échelle, le premier qui bloque tout et le dernier qui laisse tout passer). Ça donne n bon équilibre entre les deux.

Une image contenant texte, capture d’écran, logiciel, Police

Le contenu généré par l’IA peut être incorrect.

Ici on peut créer une règle simple, pour autoriser ou bloquer un flux basique selon des critères source/destination/port, un séparateur, pour organiser visuellement les groupes de règles, une règle d’authentification, qui impose une identification utilisateur avant de naviguer, une règle d’inspection SSL, pour décrypter et inspecter le trafic HTTPS (utile pour repérer du contenu malveillant) et une règle de proxy HTTP explicite, si je souhaite forcer le passage du trafic Web par un proxy configuré.

Une image contenant texte, Police, logiciel, nombre

Le contenu généré par l’IA peut être incorrect.

Je mets ma règle en état de fonctionnement,

Une image contenant texte, nombre, Police, logiciel

Le contenu généré par l’IA peut être incorrect.

Je choisi ce qu’elle va faire, laisser passer, bloquer, déchiffrer ou réinitialiser les connexions TCP/UDP.

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Le contenu généré par l’IA peut être incorrect.

Ici je définis la source de la règle. Je sélectionne un objet déjà défini dans la base d’objets. Cela permet de construire une règle ciblée, par exemple pour n’autoriser qu’un certain réseau ou une seule machine. Ensuite, je choisis l’interface d’entrée, c’est-à-dire le point d’entrée du trafic à contrôler.

Une image contenant texte, logiciel, Police, nombre

Le contenu généré par l’IA peut être incorrect.

Ensuite je choisis la destination, là ou la source peut (ou peut pas) accéder. On peut choisir un hôte, une interface, un objet ou tout.Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

Je sélectionne plusieurs services web de confiance, dans la destination. Ce qui permet d’appliquer des règles plus avancées en se basant sur la catégorie des services plutôt que sur des IP statiques, qui changent souvent. C’est idéal pour autoriser l’accès uniquement aux services Office 365 sans ouvrir tout le trafic web.

Une image contenant texte, Police, capture d’écran, nombre

Le contenu généré par l’IA peut être incorrect.

Ici, je définis les ports et protocoles. Cette configuration permet de limiter la règle à des flux bien spécifiques, ce qui améliore la sécurité en évitant d’ouvrir inutilement d'autres ports.

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Le contenu généré par l’IA peut être incorrect.

On peut aussi configurer un filtrage basé sur les protocoles. On peut filtrer pour autoriser seulement un port avec un protocole ou seulement un port.

Une image contenant texte, capture d’écran, nombre, logiciel

Le contenu généré par l’IA peut être incorrect.

Je définis un niveau d’inspection IPS, ce qui active l’analyse des paquets à la recherche d’attaques connues. Je laisse l’inspection applicative désactivée (antivirus, sandboxing, filtrage URL...), car dans ce cas elle n’est pas nécessaire. Cela permet d’économiser des ressources tout en maintenant un bon niveau de sécurité. Dans le réseau, il n’est pas toujours utile d’analyser les paquets, dans cette entreprise il est souvent désactivé pour économiser des ressources.

Une image contenant texte, logiciel, nombre, Page web

Le contenu généré par l’IA peut être incorrect.

Je commence par autoriser les flux SSH et ICMP provenant des domaines megao.com pour permettre la télémaintenance. Je choisis de cocher l’option "passer" pour laisser passer le trafic sans blocage. Ensuite, j’autorise les pings internes (ICMP) depuis le réseau local pour permettre le diagnostic réseau. Je permets aussi l'accès aux services Microsoft (Exchange, SharePoint, etc.) depuis le réseau local, ce qui est utile pour une connectivité bureautique fluide. Enfin, je bloque explicitement le trafic sortant depuis le LAN vers les services web jugés suspects ou malveillants pour limiter les risques de malware.

Une image contenant texte, nombre, Police, ligne

Le contenu généré par l’IA peut être incorrect.

Je commence par autoriser le trafic VPN SSL pour les utilisateurs à distance. Ensuite, je mets en place un filtrage spécifique du web avec une règle de contournement (Bypass filtrage web) vers certains sites, approuvés. Pour la navigation web classique des postes bureautiques, je permets HTTPS et HTTP, en activant l'inspection SSL et le filtrage d'URL. J’ajoute aussi une règle pour permettre l’accès à la console cloud de Kaspersky pour les mises à jour. Enfin, je termine par une règle de blocage total (Block ALL) qui interdit tout trafic non explicitement autorisé plus haut.

### NAT :

Une image contenant texte, Police, capture d’écran, ligne

Le contenu généré par l’IA peut être incorrect.

Ici, je configure une règle NAT. Je fais une translation d'adresse pour permettre aux machines du réseau local (Network\_LAN) d’accéder à Internet via l’interface FTTO. Je définis que le trafic sortant utilisera l’IP publique assignée à l’interface Firewall\_FTTO\_ORANGE, avec un port source aléatoire (ephemeral\_fw) pour que le port se ferme lorsque la connexion est finie. Cette règle est essentielle pour que les appareils puissent aller sur internet avec une adresse IP publique.

### SSL :

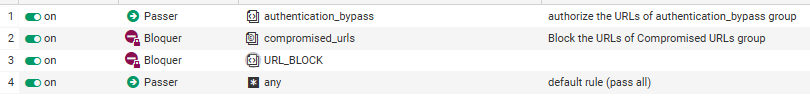
Une image contenant texte, capture d’écran, logiciel, Police

Le contenu généré par l’IA peut être incorrect.

Je décide d’abord de laisser passer sans déchiffrement certains serveurs SSL spécifiques (proxyssl\_bypass) pour éviter les conflits de certificat. Ensuite, une règle désactivée visait à bloquer les URL. La règle suivante bloque sans déchiffrement toutes les connexions vers les catégories du groupe SSL\_BLOCK (défini plus tôt : warez, proxy, etc.), ce qui garantit la sécurité tout en évitant le déchiffrement inutile. Enfin, je termine par une règle par défaut qui laisse tout passer sans déchiffrement, pour éviter que les clients aient ce symbole et paniquent et appellent la hotline (ça arrive souvent) :



### URL :



Ici, je définis une politique de filtrage d'URL. La première règle autorise le trafic vers les sites inclus dans le groupe authentication\_bypass, ce qui est utile pour permettre l'accès à des portails d'authentification avant toute vérification de contenu. Ensuite, je bloque l'accès aux URL listées comme compromises (compromised\_urls) pour empêcher toute interaction avec des sites malveillants. Je bloque également les sites classés dans le groupe URL\_BLOCK, qui regroupe des catégories sensibles (comme le warez ou la pornographie). Enfin, je termine par une règle par défaut qui autorise tout le reste (any) afin de ne pas bloquer le trafic légitime non spécifiquement encadré par les règles précédentes.

### SMTP :

Une image contenant texte, capture d’écran, Police, nombre

Le contenu généré par l’IA peut être incorrect.

Ici, je configure le filtrage SMTP. J’autorise tous les mails envoyés vers les domaines wanadoo.fr et orange.fr, sans distinction d’expéditeur (indiqué par *@*). Ce type de règle est utile dans le cadre d’une entreprise ayant des échanges fréquents avec ces fournisseurs. L’objectif ici est de s’assurer que les courriels légitimes ne soient pas bloqués.

### Qualité de service :

Une image contenant texte, capture d’écran, logiciel, Police

Le contenu généré par l’IA peut être incorrect.

Je mets en place une règle de qualité de service (QoS) avec une file d’attente CBQ (Class-Based Queuing). Je crée une file nommée CBQ\_1 sans priorité particulière, avec une bande passante maximale fixée à 1 Mbit/s. Je n’attribue pas de bande passante garantie pour laisser de la flexibilité à d'autres files, mais je limite la bande passante globale utilisée par certaines applications ou utilisateurs, c’est utile pour éviter la saturation du lien.

### Règles implicites :

Une image contenant texte, capture d’écran, nombre, Police

Le contenu généré par l’IA peut être incorrect.

Ici, je configure les règles implicites du pare-feu. Je choisis d’activer l’accès au serveur d’administration via le port 1300 depuis les interfaces protégées, ce qui permet aux administrateurs réseau de gérer le pare-feu en interne de façon sécurisée. La plupart des autres règles sont également activées : accès DNS, VPN, WebAdmin, DHCP, etc. Cela garantit un bon fonctionnement de base de l’infrastructure sans créer manuellement toutes ces règles. Je laisse cochée l’option en bas pour inclure les règles de sortie implicites, ce qui est indispensable pour le bon fonctionnement des services hébergés. Elles se font automatiquement.

## Réseau :

Une image contenant texte, logiciel, Page web, Icône d’ordinateur

Le contenu généré par l’IA peut être incorrect.

Je configure ici l’interface LAN du pare-feu. Je l’active, je la nomme « LAN » et je la définis comme interface interne protégée, ce qui est logique pour un réseau local. Je choisis une adresse IP statique en 192.168.x.x/24 afin de garantir une passerelle stable pour les machines du réseau. Ce choix évite les conflits d’adressage et permet une meilleure maîtrise de la topologie réseau.

### Routage :

Une image contenant texte, Police, nombre, capture d’écran

Le contenu généré par l’IA peut être incorrect.

Ici, j’active la passerelle GW\_ORANGE sur l’interface FTTO\_ORANGE.

Je change aussi la passerelle par défaut pour que le client accède à internet.

### DHCP :

Une image contenant texte, capture d’écran, Police, nombre

Le contenu généré par l’IA peut être incorrect.

J’active le service en mode "serveur DHCP" pour qu’il attribue automatiquement les adresses IP aux clients. Je laisse la passerelle vide ici car je ne veux pas que ça soit la même pour tous, mais je définis dns1.google.com et dns2.google.com comme serveurs DNS par défaut.

Une image contenant texte, capture d’écran, Police, nombre

Le contenu généré par l’IA peut être incorrect.

Ici, je détaille la configuration des plages DHCP et des réservations. Je définis plusieurs plages avec des passerelles et des DNS adaptés aux différents segments réseau (LAN, bridge-LAN, WIFI invité). Chaque plage a ses propres paramètres DNS et suffixes de domaine pour séparer logiquement les réseaux. En dessous, je réserve manuellement des IP pour certains équipements comme des enregistreurs de température, en liant à chaque fois leur passerelle et leurs DNS. Cela permet de garantir une IP fixe à ces équipements tout en maintenant une gestion centralisée.

### Interfaces virtuelles :

Je ne les ai pas utilisées car le routage inter-VLAN est déjà assuré par un équipement dédié (comme un routeur ou un switch de niveau 3), et la création d’interfaces virtuelles (SVI) n’était pas nécessaire dans ce contexte. Leur usage se justifie surtout sur des switches de niveau 3 ou dans des environnements complexes avec segmentation logique avancée.

### Routage dynamique :

Le routage dynamique (OSPF, EIGRP, RIP) n’a pas été mis en place, car le réseau comporte peu de sous-réseaux et la topologie est fixe. Un routage statique est donc suffisant, plus facile à configurer, plus lisible, et plus adapté à une structure où les routes ne changent pas fréquemment.

### Multicast :

Je n’ai pas activé le multicast, car aucune application du réseau ne nécessite la diffusion de paquets vers plusieurs hôtes simultanément (comme la vidéo en streaming interne ou les mises à jour de masse). Le trafic unicast classique suffit amplement pour ce type d’infrastructure.

DNS dynamique :

Le DNS dynamique, qui permet aux machines d’enregistrer automatiquement leurs adresses IP dans le DNS, n’est pas utile ici car j’ai préféré une configuration statique ou semi-automatisée, plus fiable et plus contrôlable. Cela évite aussi les enregistrements fantômes ou mal configurés dans le serveur DNS.

### Proxy cache DNS :

Je n’ai pas mis en place de proxy cache DNS, car le nombre de requêtes DNS dans le réseau est limité et les performances restent bonnes sans mise en cache avancée. Ce genre de mécanisme est pertinent dans des réseaux avec beaucoup de trafic DNS externe, ce qui n’est pas le cas ici.

## Objet :

### Réseau :

Une image contenant texte, nombre, Police, logiciel

Le contenu généré par l’IA peut être incorrect.

Je crée ici un nouvel objet de type machine dans l’interface Stormshield. Je remplis les champs nom de l’objet, adresse IPv4 et adresse MAC (facultative). Pour la résolution, je choisis Automatique, ce qui signifie que le pare-feu utilisera le DNS ou ARP pour résoudre l’adresse, plutôt que de s’appuyer uniquement sur l’IP fixe.

L’objet Machine représente un appareil précis (PC, serveur…). On lui donne un nom, une adresse IP, et parfois une adresse MAC. On peut choisir si cette IP est fixe ou récupérée automatiquement (par DNS).

L’objet Nom DNS (FQDN) sert quand on connaît le nom d’un appareil (comme un site ou un serveur) mais pas son IP fixe. Stormshield ira chercher l’IP en fonction du nom.

L’objet Réseau désigne tout un sous-réseau, par exemple 192.168.1.0/24. Ça permet de viser plusieurs appareils d’un seul coup.

L’objet Plage d’adresses permet de cibler plusieurs IP d’affilée, comme de 192.168.1.10 à 192.168.1.20, sans être obligé de passer par un masque.

L’objet Routeur représente une passerelle ou un routeur dans le réseau, utilisé pour orienter le trafic.

L’objet Groupe regroupe plusieurs objets (machines, réseaux…). C’est pratique pour appliquer une règle à tout un ensemble sans les gérer un par un.

Ces objets simplifient la gestion du pare-feu : on les crée une fois, et on les réutilise dans les règles de filtrage, NAT, ou VPN.

### URL :

Une image contenant texte, logiciel, Icône d’ordinateur, Page web

Le contenu généré par l’IA peut être incorrect.

Je créer un groupe nommé SSL\_BLOCK dans lequel je regroupe des catégories sensibles comme warez, proxy, pornography, illegal, et ads. Ce qui permet d’appliquer ce blocage dans les règles de filtrage SSL sans créer 5 règles.

Il y a de toutes nouvelles catégories. La manière du haut sera maintenu encore quelques temps et disparaitra pour laisser la place à celle-là :

Une image contenant texte, capture d’écran, logiciel, nombre

Le contenu généré par l’IA peut être incorrect.

Elle permet de mieux filtrer les catégories, j’ai bloqué tout ce qui contenait du sexe, de l’illégal proxy… J’en ai bloqué 43 en tout, c’est trop long a expliqer.

### Services web :

Je n’ai pas activé de serveur web (IIS ou autre) car le but du projet n’était pas d’héberger des applications ou des sites accessibles par HTTP/HTTPS. Le serveur est principalement utilisé pour l’Active Directory, le DNS, ou d’autres services de base. Ajouter un service web aurait occupé des ressources pour un usage inutile, et aurait ouvert des ports supplémentaires, ce qui augmente la surface d’attaque potentielle sans raison.

### Certificats pki :

Concernant la PKI, je n’ai pas installé de serveur de certificats car aucun service dans l’infrastructure ne nécessite l’émission, la gestion ou la vérification de certificats internes (comme ceux utilisés pour l’authentification, le chiffrement ou le VPN). La mise en place d’une autorité de certification (CA) demande une configuration avancée, une gestion des politiques de certificats, et une surveillance régulière, ce qui n’est pas justifié ici dans un réseau local simple, sans utilisateurs nomades ou services sensibles nécessitant des communications chiffrées avec des certificats internes.

## Protection applicative :

Je n’ai pas touché à la protection applicative dans Stormshield car les paramètres par défaut sont déjà activés et correctement configurés pour offrir un niveau de sécurité adapté à une utilisation standard. J’ai monté des Stormshield de base, je n’ai donc pas eu à les changer.

## VPN :

IPsec sert entre un réseau et un utilisateur et SSL entre un client et un serveur car IPSec sert à établir une liaison sécurisée globale entre un utilisateur et un réseau, tandis que SSL protège une communication spécifique entre un client et un serveur.

### IPsec :

Une image contenant texte, capture d’écran, logiciel, nombre

Le contenu généré par l’IA peut être incorrect.

Je crée ici un profil de chiffrement IKE nommé P1\_MEGAO\_2025 pour le VPN IPsec. J'utilise le groupe Diffie-Hellman DH14 (2048 bits) pour garantir un bon niveau de sécurité dans l'échange de clés. Je définis une durée de vie de 21600 secondes (6h), ce qui limite les risques en forçant un renouvellement périodique. En termes d’algorithme, j’utilise aes\_gcm\_16 avec une force de chiffrement de 256 bits, recommandé pour sa performance et sa robustesse.

Une image contenant texte, capture d’écran, Système d’exploitation, logiciel

Le contenu généré par l’IA peut être incorrect.

Je configure la passerelle distante pour établir un tunnel IPsec. J’entre l’adresse vpn.cloud.megao.co, je nomme la connexion “MegaO Infra Hébergée” et je choisis IKEv1 pour la compatibilité avec l'infrastructure distante.

Une image contenant texte, capture d’écran, Police, nombre

Le contenu généré par l’IA peut être incorrect.

Dans cette étape, je choisis la méthode d’authentification par clé pré-partagée (PSK). C’est plus simple à déployer qu’un certificat dans un environnement restreint. Je saisis la même clé dans les deux champs pour assurer la cohérence entre les extrémités du tunnel VPN. C’est une méthode rapide et efficace, même si elle demande une bonne gestion de la clé.

Une image contenant texte, capture d’écran, nombre, Police

Le contenu généré par l’IA peut être incorrect.

Je finalise ici la configuration de la passerelle VPN “MegaO Infra Hébergée”. Je précise l’adresse distante, le profil IKE que j’ai créé (P1\_MEGAO\_2025) et la version IKEv1. En méthode d’authentification, je confirme le choix de la PSK et j’entre un Local ID pour identifier cette extrémité du tunnel, essentiel pour l’échange des identifiants pendant la phase 1 du VPN.

Une image contenant capture d’écran, conception

Le contenu généré par l’IA peut être incorrect.

Cette capture montre l’étape de liaison des réseaux locaux et distants via l’assistant de politique VPN IPsec. Je sélectionne mes réseaux distants, ce qui permet de définir précisément quels sous-réseaux peuvent communiquer à travers le tunnel.

Une image contenant texte, Police, capture d’écran, nombre

Le contenu généré par l’IA peut être incorrect.

Enfin, je valide le tunnel VPN site-à-site. Il est activé et associe bien Network-bridge-LAN au réseau distant LAN via le correspondant VPN\_via\_Starlink. Le profil de chiffrement utilisé est P2\_MEGAO\_2025, assurant un niveau de sécurité élevé. Cette vue confirme que le tunnel est fonctionnel et prêt à acheminer du trafic sécurisé entre les deux sites.

### SSL Portail :

Une image contenant texte, Police, capture d’écran, Page web

Le contenu généré par l’IA peut être incorrect.

Je configure ici le module VPN SSL pour permettre un accès distant sécurisé client-serveur. Je l’active en sélectionnant l’option « accès aux serveurs Web et applicatifs », car je souhaite que l’utilisateur puisse à la fois consulter des interfaces web internes et se connecter à des applications. Cela permet une gestion souple selon les profils utilisateurs.

Une image contenant texte, capture d’écran, nombre, Police

Le contenu généré par l’IA peut être incorrect.

Dans cette configuration, je déclare un serveur Web nommé IMM-ESX, en précisant le protocole HTTPS. Le lien généré permettra aux utilisateurs connectés en VPN SSL d'accéder directement à l’interface d’administration de l'hyperviseur via le portail. Je renseigne un nom clair pour que l’utilisateur identifie facilement la ressource à utiliser dans l’interface.

Une image contenant texte, capture d’écran, nombre, Police

Le contenu généré par l’IA peut être incorrect.

Ici, je configure un serveur applicatif SRVDRS pour permettre une session RDP à distance. Je choisis microsoft-ts comme protocole, et je complète les paramètres du poste utilisateur avec l’adresse IP locale du serveur et la commande mstsc /v:..., ce qui déclenchera automatiquement une session Bureau à distance. Ce paramétrage permet une prise en main directe de la machine via le portail VPN SSL.

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

Dans cette dernière capture, je crée un profil utilisateur RDS. Je désactive l’accès à l’interface web IMM-ESX mais j’active l’accès à l’applicatif SRVDRS. L’objectif est ici de limiter les ressources visibles par l’utilisateur selon son rôle : dans ce cas, uniquement l’accès au serveur de bureau à distance. C’est une bonne pratique pour cloisonner les droits d’accès dans un contexte professionnel.

### SSL :

Une image contenant texte, capture d’écran, logiciel, nombre

Le contenu généré par l’IA peut être incorrect.

Je configure ici les paramètres généraux du VPN SSL. Je renseigne l’adresse IP publique (ou FQDN) utilisée par l’UTM, ce qui permettra aux clients de se connecter depuis l’extérieur. Je définis ensuite les réseaux internes accessibles (Network\_LAN) ainsi que les sous-réseaux dédiés aux clients VPN (LAN\_VPN\_UDP et LAN\_VPN\_TCP) selon leur protocole de connexion. Je limite à 100 le nombre de tunnels simultanés, ce qui est suffisant pour la majorité des PME. Enfin, j’envoie automatiquement aux clients le nom de domaine local et le DNS interne (srv-ad.local) pour qu’ils puissent résoudre les noms internes correctement une fois connectés au VPN.

Je ne me suis pas servie du serveur PPTP car car ce protocole est ancien et considéré comme non sécurisé.

PPTP (Point-to-Point Tunneling Protocol) utilise des mécanismes de chiffrement faibles et présente de nombreuses vulnérabilités connues, qui le rendent facilement exploitable par un attaquant.

## Notifications :

Je n’ai pas paramétré les notifications car je n’avais pas besoin d’un suivi en temps réel par mail ou via une alerte distante car ceux sont des petites entreprises. Megao propose aux grandes entreprises de sécurisé leur réseau via Tehtris

Je n’ai pas activé les notifications car, dans un contexte de petites entreprises, la supervision (suivi en temps réel par mail ou via une alerte distante) peut rester locale et manuelle, ce qui est suffisant. En revanche, les grandes structures ont besoin d’outils de cybersécurité avancés comme Tehtris (proposé par Megao), capable de gérer en temps réel des menaces complexes sur un grand périmètre, tout en automatisant la réponse et en facilitant la gestion globale de la sécurité.

# Installation physique :

Une image contenant texte, Appareils électroniques, Appareil électronique, Ingénierie électronique

Le contenu généré par l’IA peut être incorrect.

J’ai plus qu’à regarder ou sont branchés les files sur l’ancien routeur et les rebranchés sur les bons ports que j’ai configurés.

# Installation chez le client :

## Utilisateurs :

Nous pouvons configurer les utilisateurs que chez le client car il faut pouvoir se connecter à leur AD pour coupler les utilisateurs. Une fois fait, on pourra les voir dedans.

### Droits d’accès :

Une image contenant texte, capture d’écran

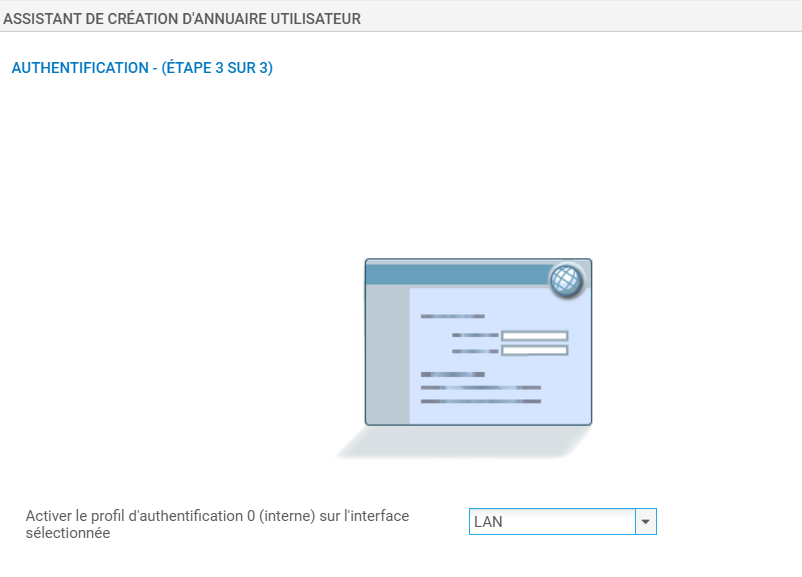
Le contenu généré par l’IA peut être incorrect.

Dans la première étape de l’assistant de création d’annuaire utilisateur, je sélectionne l’option "Se connecter à un annuaire Microsoft Active Directory". Ce choix est logique car mon infrastructure utilise un contrôleur de domaine Windows (AD), ce qui me permet d'intégrer directement Stormshield à l'annuaire existant sans devoir gérer manuellement les comptes utilisateurs ou leurs droits. Cela centralise l’authentification et simplifie la gestion des accès.

Une image contenant texte, Police, ligne, nombre

Le contenu généré par l’IA peut être incorrect.

Dans l’onglet "Detailed Access", je configure les privilèges d’accès d’un groupe d’utilisateurs G\_acces\_TSE\_via\_stormshield. Je décide ici de bloquer l’accès au portail SSL VPN et au tunnel IPsec pour réduire la surface d’exposition. Par contre, je laisse l’accès au SSL VPN (client lourd) activé, car c’est le seul moyen sécurisé et maîtrisé par lequel ce groupe est autorisé à accéder au réseau distant. Le parrainage est désactivé pour garder le contrôle total sur les connexions.



Dans l’étape 3 de l’assistant de création d’annuaire, j’active le profil d’authentification interne sur l’interface LAN. Je choisis le LAN car c’est sur cette interface que mes utilisateurs internes vont se connecter. Ce paramétrage est essentiel pour que les utilisateurs soient bien authentifiés depuis le bon segment réseau, en interne, sans risque de conflit avec des profils externes.

Une image contenant texte, capture d’écran, Téléphone mobile, conception

Le contenu généré par l’IA peut être incorrect.

Je configure l’accès LDAP au domaine xx.local. Je remplis toutes les informations nécessaires : nom de domaine, serveur Active Directory, port LDAP, DN de base, et les identifiants d’un compte ayant les droits de lecture LDAP. Je choisis le hachage SHA pour le mot de passe car il est compatible avec Stormshield. Cette configuration est nécessaire pour que le firewall interroge le bon annuaire pour les authentifications utilisateurs.

### Authentification :

Une image contenant texte, capture d’écran, Police, logiciel

Le contenu généré par l’IA peut être incorrect.

Je configure les profils d’authentification du portail captif en fonction des interfaces. Pour l’interface LAN, j’utilise un profil "Interne" lié à l’annuaire de l’AD, ce qui permet une authentification transparente pour les utilisateurs en interne. Pour l’interface FTTO\_ORANGE, qui correspond à un lien Internet ou à une zone d’accès invité, j’associe un profil "Externe" mais toujours basé sur le même annuaire AD. Cela permet aux utilisateurs à distance ou en mobilité de s’authentifier de façon sécurisée via le portail captif, tout en restant intégrés dans l’annuaire central.

# Conclusion :

Cette installation m’a permis de mettre en place un pare-feu Stormshield complet et fonctionnel, en tenant compte des besoins du client. J’ai configuré les règles de sécurité, les accès VPN, et l’intégration à l’Active Directory, tout en laissant de côté les fonctions inutiles dans ce contexte. Le pare-feu est désormais opérationnel, sécurisé et adapté à l’infrastructure en place.

# Sources :

Mégao

[Tehtris — Wikipédia](https://fr.wikipedia.org/wiki/Tehtris)

[Point-to-Point Tunneling Protocol — Wikipédia](https://fr.wikipedia.org/wiki/Point-to-Point_Tunneling_Protocol)