

# STORMSHIELD

Montage d'un pare-feu

## Table des matières

Introduction : .....	2
Pré-installation physique : .....	2
Pré-installation virtuelle : .....	3
Mise en place de la licence : .....	3
Système : .....	9
Politique de sécurité : .....	12
Filtrage : .....	12
NAT : .....	16
SSL : .....	16
URL : .....	17
SMTP : .....	17
Qualité de service : .....	17
Règles implicites : .....	18
Réseau : .....	19
Routage : .....	19
DHCP : .....	19
Interfaces virtuelles : .....	21
Routage dynamique : .....	21
Multicast : .....	21
DNS dynamique : .....	21
Proxy cache DNS : .....	21
Objet : .....	21
Réseau : .....	21
URL : .....	22
Services web : .....	23
Certificats pki : .....	23
Protection applicative : .....	23
VPN : .....	23
IPsec : .....	24
SSL Portail : .....	26
SSL : .....	28
Notifications : .....	28
Installation physique : .....	29
Installation chez le client : .....	29
Utilisateurs : .....	29
Droits d'accès : .....	30

Authentification : .....	32
Enrôlement : .....	<b>Erreur ! Signet non défini.</b>
Configuration des annuaires : .....	<b>Erreur ! Signet non défini.</b>
Conclusion : .....	32
Sources : .....	32

## Introduction :

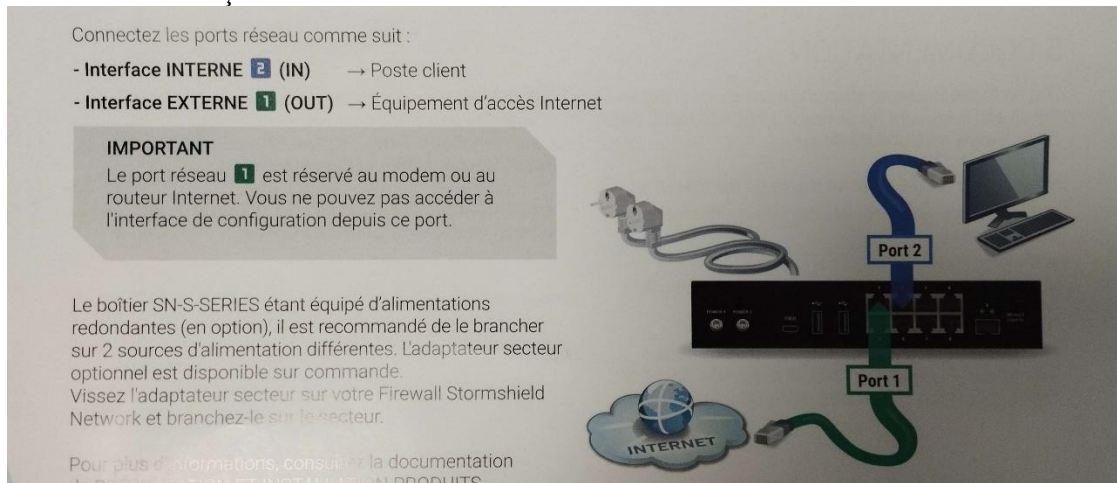
J'ai remplacé le pare-feu Stormshield chez un petit client qui possède une infrastructure assez simple : quelques postes de travail, une box Internet et un serveur principal utilisé pour la gestion de son activité. L'ancien pare-feu était devenu trop vieux et ne recevait plus de mises à jour, ce qui 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 :



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.

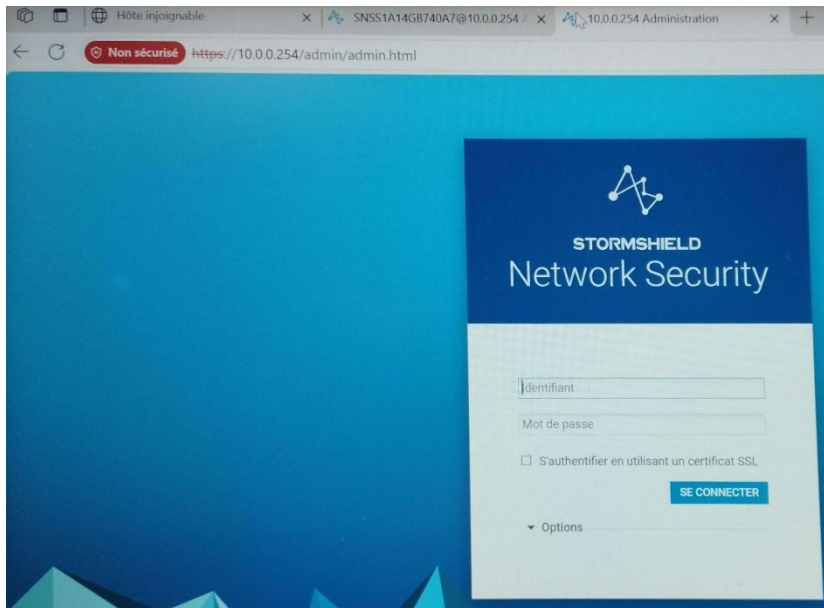
J'ai ensuite branché les câbles pour connecter mon pare-feu à internet (port 1, fil blanc) et à mon PC (port 2, fil bleu). Cet ordre est très important car les ports ont été configurés pour marcher comme ça :



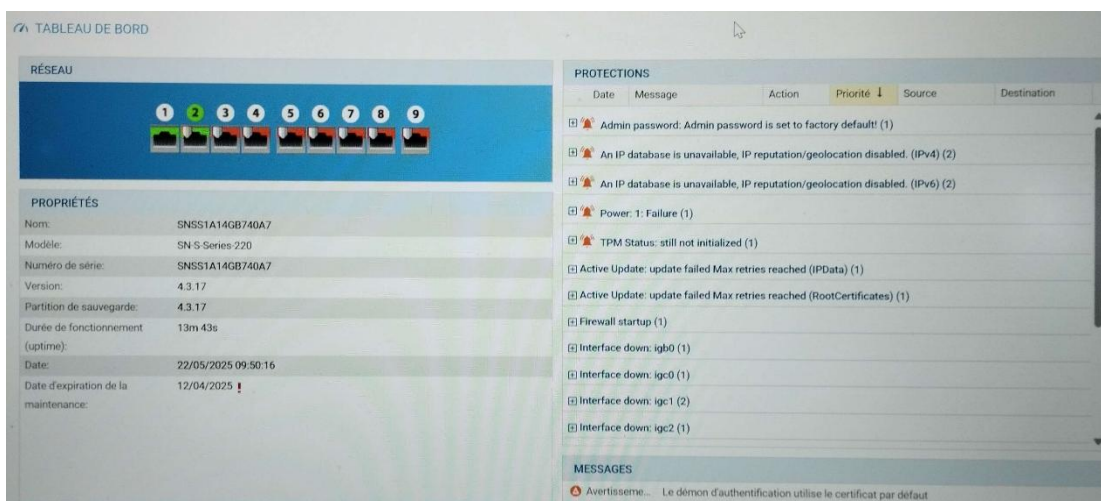
On voit les voyants lumineux : ici, les ports 1 et 2 sont actifs (LED verte), ce qui signifie qu'ils sont connectés. Le voyant "STATUS" est vert, donc l'équipement est en ligne et fonctionne normalement. Je vérifie ici que mes branchages ont été faits comme il faut.

## Pré-installation virtuelle :

## Mise en place de la licence :



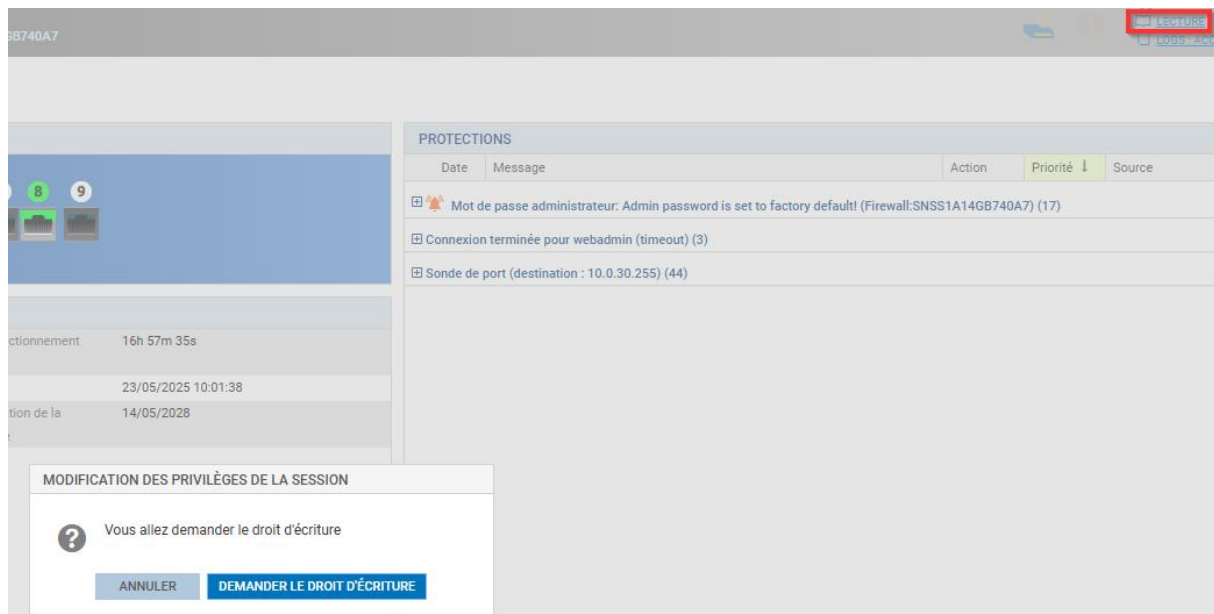
Ensuite je me connecte sur l'interface web pour le configurer. L'adresse IP par défaut est 10.0.0.254/admin et le mot de passe et l'identifiant sont admin par défaut.



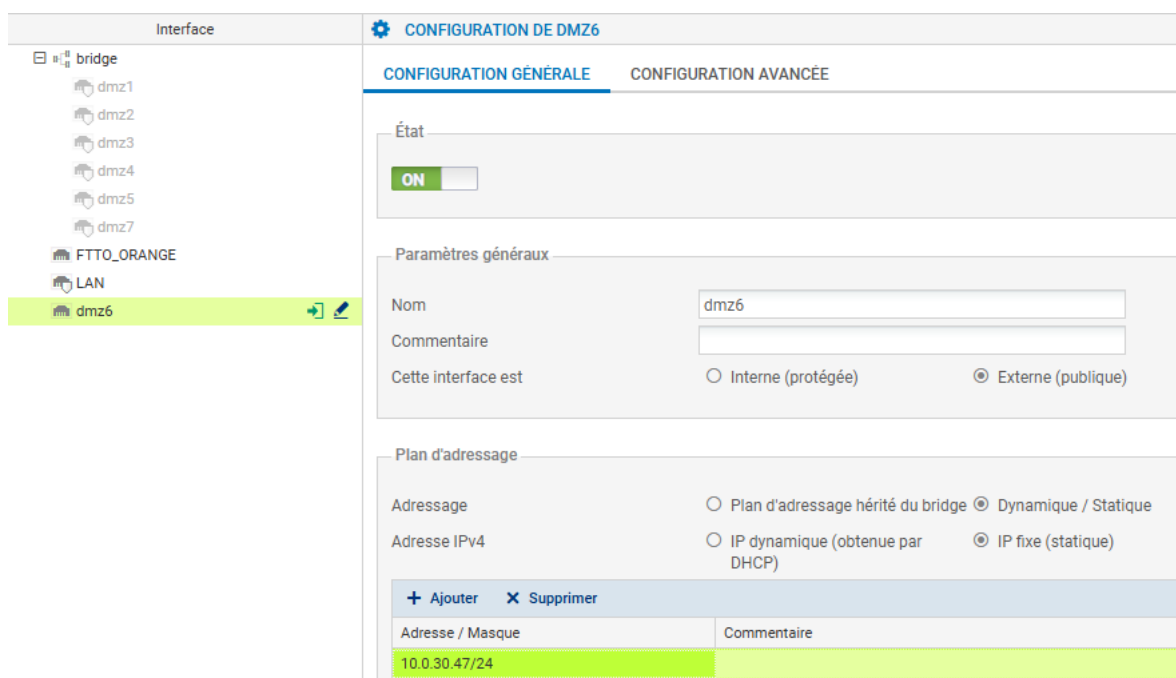
Je suis maintenant connecté à l'interface web d'administration du Stormshield. On y voit le tableau de bord du pare-feu, avec :

- 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).

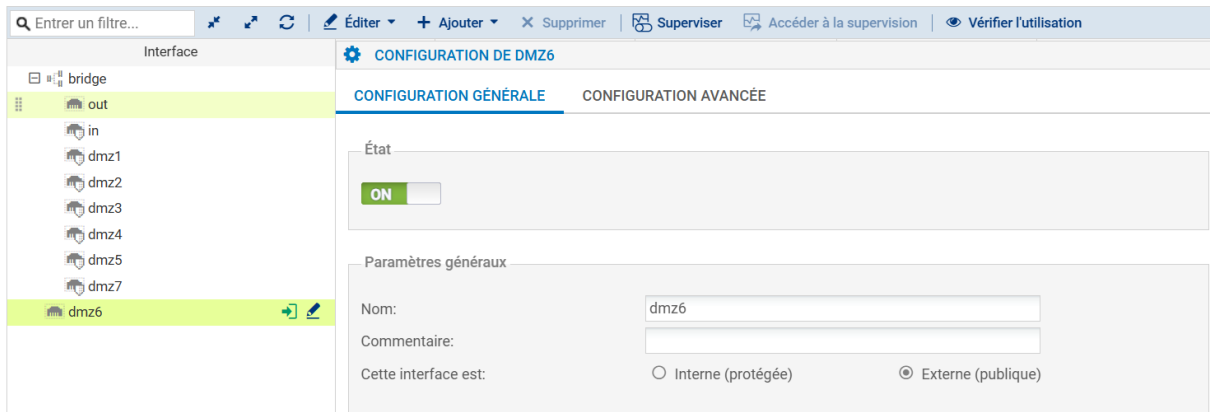
Je m'en occuperai après la mise à jour. Pour ça il faut connecter le pare-feu à internet.



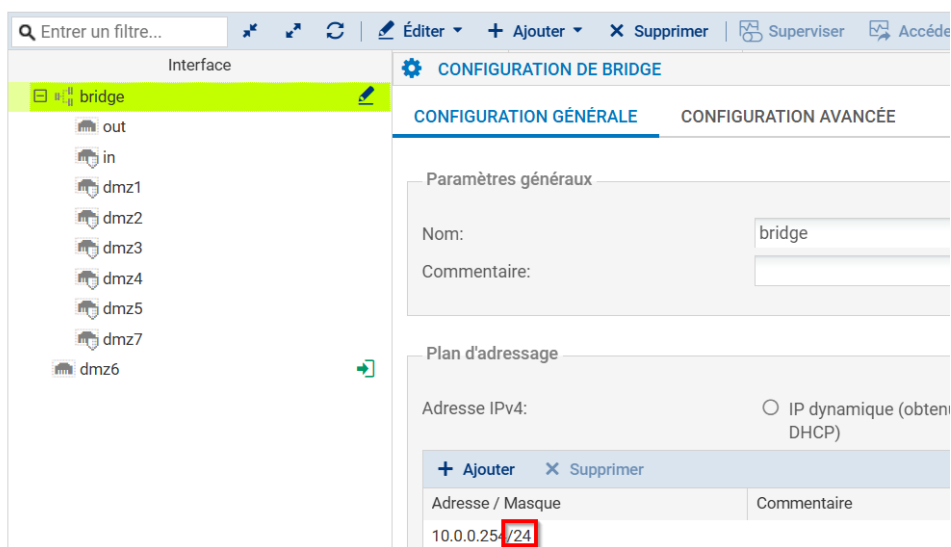
Je commence par de mettre en droit d'écriture pour modifier ou rajouter des choses. Par défaut il est sur lecture seule.



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.



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

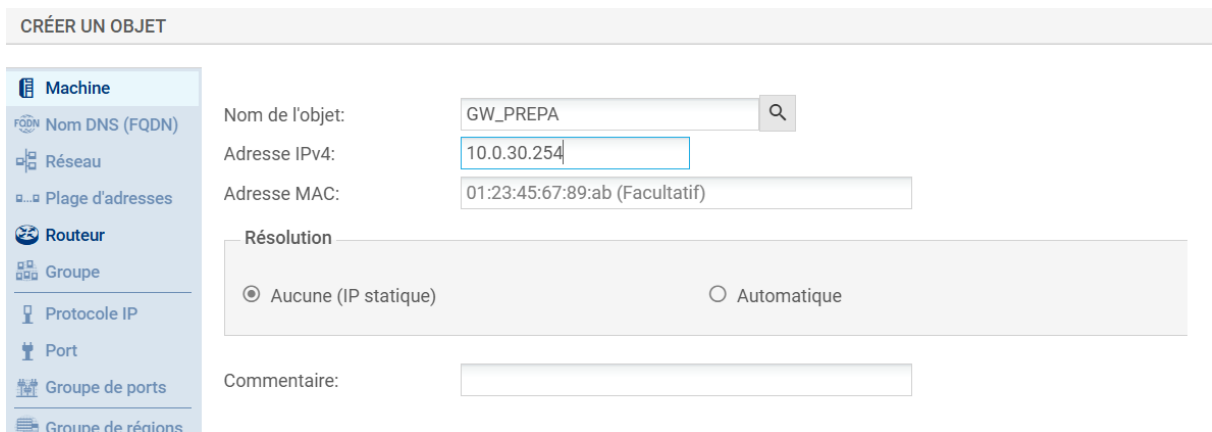


Je passe ensuite le bridge en /24 pour qu'elle soit dans le même réseau que mon interface. Cela permet d'associer plusieurs interfaces réseau tout en les traitant comme un seul segment, ce qui permettra d'appliquer des règles de sécurité tout en laissant passer le trafic entre les équipements connectés.

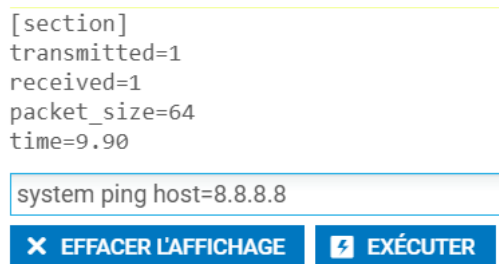




Je rajoute l'accès internet à mon interface que j'ai configuré pour que je puisse me connecter dessus.



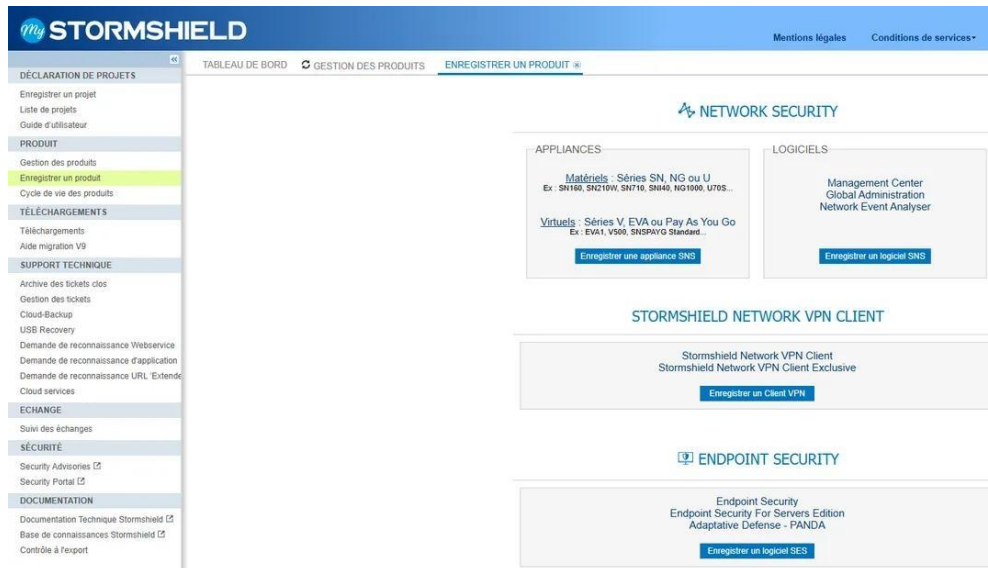
Je crée ici un objet de type machine dans l'interface de gestion Stormshield, que je nomme GW\_PREPA. Je lui attribue l'adresse IP statique de la passerelle de la prépa. Mon pare-feu peut donc sortir sur internet :



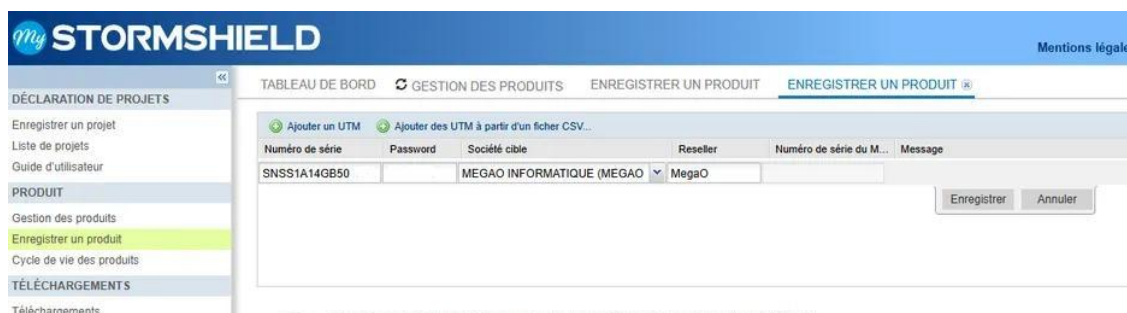
Je teste en faisant un ping en ligne de commande dans mon pare-feu vers google pour vérifier qu'il accède à internet.

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

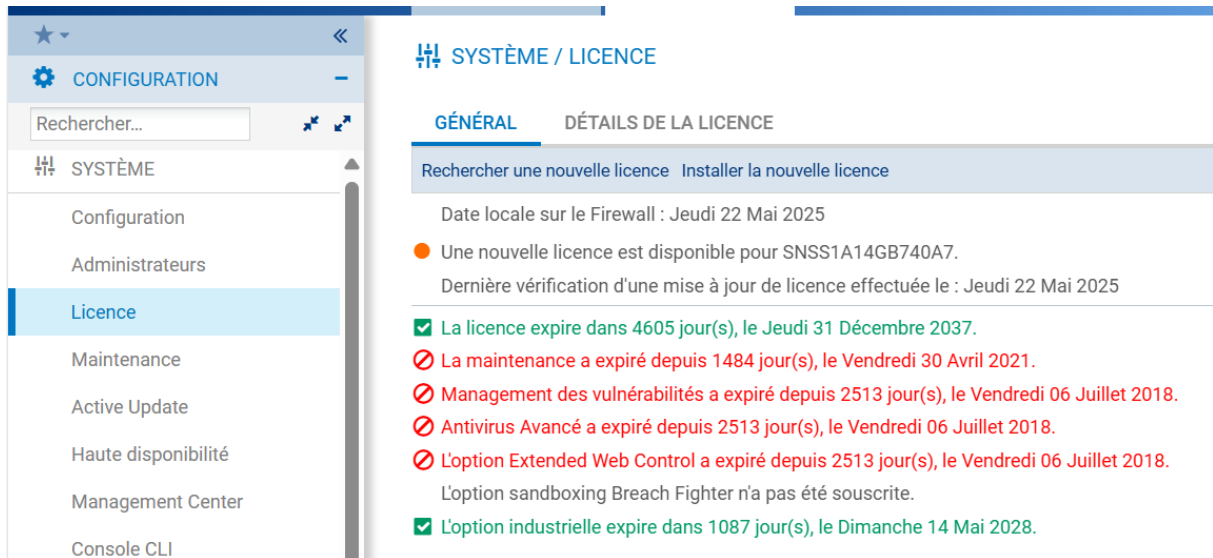




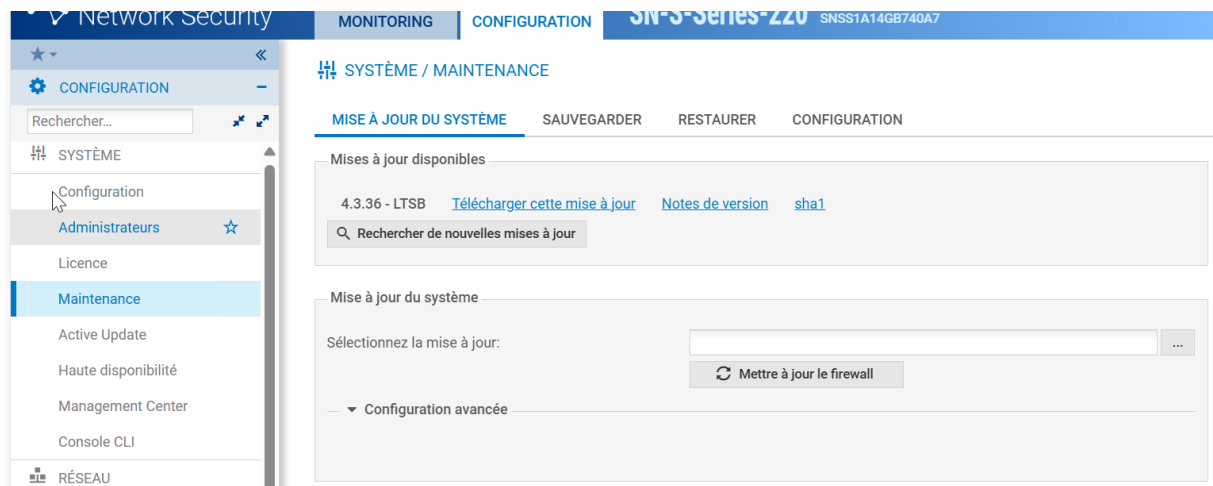
Dans la section Produit, Enregistrement d'un produit, j'ai enregistré une appliance SNS afin d'activer officiellement la licence Stormshield associée à notre équipement. En déclarant notre Appliance, on associe son numéro de série au compte entreprise, ce qui garantit que le matériel est reconnu comme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



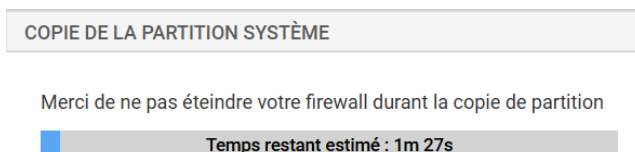
Je tape le mot de passe et l'identifiant qu'il y a sur le boîtier physique pour l'activer.



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 :

**SYSTÈME / CONFIGURATION**

**CONFIGURATION GÉNÉRALE** ADMINISTRATION DU FIREWALL PARAMÈTRES RÉSEAUX

**Configuration générale**

Nom du firewall: SNSS1A14GB740A7

Langue du Firewall (traces): Français

Clavier (console): Français

**Paramètres cryptographiques**

☒ Activer la récupération régulière des listes de révocation de certificats (CRL)

☐ Activer le mode de conformité « Diffusion Restreinte (DR) » version 2021

**Politique de mots de passe**

Longueur minimale des mots de passe: 8

Types de caractères obligatoires: Aucun

Entropie minimale: 20

**Paramètres de date et d'heure - 22/05/2025 15:03:42**

☐ Saisie manuelle

☐ Synchroniser avec votre machine - 22/05/2025 17:03:20

☒ Maintenir le firewall à l'heure (NTP)

Fuseau horaire: Europe/Paris

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.

**CRÉER UN OBJET**

**Machine**

Nom de l'objet: PORT

☒ Port

Port: 8080

☐ Plage de ports

Depuis:

Jusqu'à: 0

Protocole: TCP

Commentaire:

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.

SNSS1A14GB740A7@10.0.30.47:8080

Non sécurisé https://10.0.30.47:8080/admin/admin.html#configuration/firewall

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


ADMINISTRATEURS **! COMPTE ADMIN** GESTION DES TICKETS

---

Authentification

**!** Le mot de passe par défaut du compte admin n'a pas été changé

Ancien mot de passe

Nouveau mot de passe  

Confirmer le mot de passe

---

Exports

Clé privée de l'administrateur

Clé publique du firewall

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.

Résolution DNS

LISTE DES SERVEURS DNS UTILISÉS PAR LE FIREWALL

+ Ajouter ✕ Supprimer

Serveur DNS (machine)
dns1.google.com
dns2.google.com
srv-ad-v <input type="text"/>

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.

+ Ajouter ✕ Supprimer

Serveur NTP (machine ou groupe - plage d'adresses) (15 max.)

ntp1.stormshieldcs.eu	Appliquer Annuler
ntp2.stormshieldcs.eu	
ntp.univ-lyon.fr	

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.

ACCÈS AUX PAGES D'ADMINISTRATION DU FIREWALL

+ Ajouter ✕ Supprimer

Poste d'administration autorisé (machine ou groupe - réseau - plage d'adresses)

Network_dmz6
telem.megao.com
vpn.megao.com

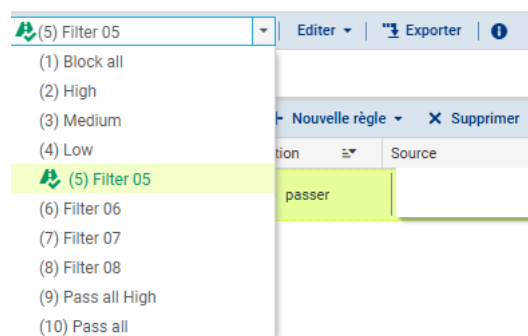
Ici, je définis les machines autorisées à accéder à l'interface d'administration du pare-feu. Je limite cet accès à Network\_dmz6, au poste de télémaintenance telem.megao.com et au domaine

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.

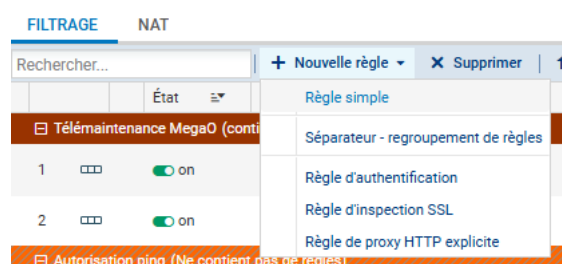
## Politique de sécurité :

### Filtrage :

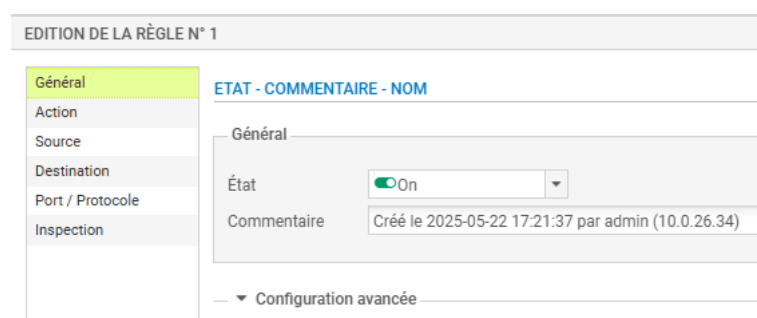
✚ POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT



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.



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.



Je mets ma règle en état de fonctionnement,

EDITION DE LA RÈGLE N° 1

Général  
**Action**  
Source  
Destination  
Port / Protocole  
Inspection

**ACTION**

GÉNÉRAL    QUALITÉ DE SERVICE    CONFIGURATION AVANCÉE

Général

Action: passer

Niveau de trace: passer

Programmation horaire: bloquer

déchiffrer

reinit. TCP/UDP

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

EDITION DE LA RÈGLE N° 1

Général  
**Source**  
Destination  
Port / Protocole  
Inspection

**SOURCE**

GÉNÉRAL    GÉOLOCALISATION / RÉPUTATION    CONFIGURATION AVANCÉE

Général

Utilisateur: Rechercher...

Machines sources: + Ajouter X Supprimer

Interface d'entrée: Choisissez une interface

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.

EDITION DE LA RÈGLE N° 1

Général  
Action  
Source  
**Destination**  
Port / Protocole  
Inspection

**DESTINATION**

GÉNÉRAL    GÉOLOCALISATION / RÉPUTATION    CONFIGURATION AVANCÉE

Général

Machines destinations: + Ajouter X Supprimer

Firewall\_all

Ensuite je choisis la destination, là où la source peut (ou peut pas) accéder. On peut choisir un hôte, une interface, un objet ou tout.

Services Web et réputations IP

Sélectionnez un service Web ou une catégorie de réputation IP

Exchange Online X Office 365 communes X

Sharepoint Online X Skype Entreprise Online X

Microsoft X

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.

EDITION DE LA RÈGLE N° 1

Général	<b>PORT ET PROTOCOLE</b> <hr/> <div>Port</div> <div>Port destination</div> <div> + Ajouter    ✕ Supprimer    [Menu] </div> <div> ssh  Admin_srv </div>
Action	
Source	
Destination	
Port / Protocole	
Inspection	

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.

EDITION DE LA RÈGLE N° 2

Général	<b>PORT ET PROTOCOLE</b> <hr/> <div>Port</div> <div>Port destination</div> <div> + Ajouter    ✕ Supprimer    [Menu] </div> <div>Any</div>
Action	
Source	
Destination	
Port / Protocole	
Inspection	

Protocole	
Type de protocole	Protocole IP
Protocole applicatif	Aucune analyse applicative
Protocole IP	icmp
Message ICMP	Tous types et codes

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.



EDITION DE LA RÈGLE N° 1

Général  
Action  
Source  
Destination  
Port / Protocole  
Inspection

### INSPECTION DE SÉCURITÉ

Général

Niveau d'inspection: **IPS**  
Profil d'inspection: Selon le sens du trafic

Inspection applicative

Antivirus: Off  
Sandboxing: Off  
Antispam: Off  
Filtrage URL: Off  
Filtrage SMTP: Off  
Filtrage FTP: Off  
Filtrage SSL: Off

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.

FILTAGE		NAT					
Rechercher...	État	Action	Source	Destination	Port dest.	Protocole	Inspection de sécurité
Télémaintenance Mega0 (contient 2 règles, de 1 à 2)							
1	on	passer	telem.megao.com vpn.megao.com	Firewall_all	ssh Admin_srv		IPS
2	on	passer	telem.megao.com vpn.megao.com	Firewall_all	Any	icmp	FW
Autorisation ping (contient 1 règles, de 3 à 3)							
3	on	passer	Network_LAN	Firewall_all	Any	icmp	FW
Autorisation vers IP Microsoft (contient 1 règles, de 4 à 4)							
4	on	passer	Network_LAN	Internet Services Web et réputations IP Exchange Online Office 365 communes Sharepoint Online Skype Entreprise Online Microsoft	Any		FW
Filtrage anti-malwares (contient 2 règles, de 5 à 6)							
5	on	bloquer	Internet interface: FT Services Web et réputations IP bad	Firewall_all	Any		IPS
6	on	bloquer	Network_LAN	Internet Services Web et réputations IP bad	Any		IPS
Autorisation trafic via VPN SSL (contient 1 règles, de 7 à 7)							

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.

Autorisation trafic via VPN SSL (contient 1 règles, de 7 à 7)						
7		passer	GRP_LAN_VPN via Tunnel VPN SSL	Network_LAN	Any	IPV
Filtrage flux vers Internet (Ne contient pas de règles)						
Bypass filtrage web (contient 1 règles, de 8 à 8)						
8		passer	Network_LAN	SITES_BYPASS_FILTRAGE_WEB	Any	IPV
Filtrage LAN bureautique vers Internet (Ne contient pas de règles)						
Autorisation vers console Kaspersky MegaO (contient 1 règles, de 9 à 9)						
9		passer	Network_LAN	kav.cloud.megao.com	GRP_PORTS_I	IPV
Filtrage web global LAN bureautique vers Internet (contient 3 règles, de 10 à 12)						
10		déchiffrer	Network_LAN	Internet	https	IPV ↳ Filtrage SSL : SSLFilter_OC
11		passer	Network_LAN	Internet	http	IPV ↳ Filtrage URL : URLFilter_OI
12		passer	Network_LAN	Internet	GRP_PORTS_mail	IPV
Block ALL (contient 1 règles, de 13 à 13)						
13		bloquer	Any	Any	Any	IPV

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 :

### POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT

(5) Filter 05							
Filtrage NAT							
Rechercher...	État	Trafic original (avant translation)		Trafic après translation			
		Source	Destination	Port src.	Port dest.	Source	Destination
1		Network_LAN	Internet interface: FTTO_ORANGE	Any	Any	Firewall_FTTO_ORANGE	ephemeral_fw

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 :

### POLITIQUE DE SÉCURITÉ / FILTRAGE SSL

(0) SSLFilter_00				
Fournisseur de base URL : Base URL embarguée				
État	Action	URL - CN	Commentaire	
1	Passer sans déchiffrer	proxyssl_by...	don't decrypt some specific ssl servers	
2	Bloquer sans déchiffrer	compromise...	Block the URLs of Compromised URLs group	
3	Bloquer sans déchiffrer	SSL_BLOCK		
4	Passer sans déchiffrer	any	default rule (decrypt all)	

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 :

1	on	Passer	authentication_bypass	authorize the URLs of authentication_bypass group
2	on	Bloquer	compromised_urls	Block the URLs of Compromised URLs group
3	on	Bloquer	URL_BLOCK	
4	on	Passer	any	default rule (pass all)

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 :

### POLITIQUE DE SÉCURITÉ / FILTRAGE SMTP

(0) MailFilter_00							Editer	?
<a href="#">+ Ajouter</a> <a href="#">X Supprimer</a> <a href="#">↑ Monter</a> <a href="#">↓ Descendre</a> <a href="#">Couper</a> <a href="#">Copier</a> <a href="#">Coller</a>								
	Etat	Action	Expéditeur	Destinataire (to, cc, cci)	Commentaire			
1	on	Passer	*@*	*@wanadoo.fr				
2	on	Passer	*@*	*@orange.fr				

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 :

### POLITIQUE DE SÉCURITÉ / QUALITÉ DE SERVICE

#### FILES D'ATTENTE TRAFFIC SHAPER

**Fonctionnalité en accès anticipé, veuillez consulter les problèmes connus avant de l'activer**

#### FILES D'ATTENTE

<input type="text" value="Entrer un filtre..."/> <a href="#">+ Ajouter</a> <a href="#">X Supprimer</a> <a href="#">Éditer la sélection</a> <a href="#">Vérifier l'utilisation</a>							
Nom	Type	Priorité	Bp garantie	Bp max	Bp inv. garantie	Bp inv. max	Commentaire
Type: CBQ							
CBQ_1	CBQ		Aucun	1 Mbit/s	Aucun	1 Mbit/s	

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 :

### ✚ POLITIQUE DE SÉCURITÉ / RÈGLES IMPLICITES

#### RÈGLES DE FILTRAGE IMPLICITES

Activé	≡	Nom
<input type="checkbox"/> Désactivé		Autoriser l'accès au serveur PPTP
<input type="checkbox"/> Désactivé		Autoriser l'accès mutuel entre les membres d'un groupe de firewalls (cluster HA)
<input checked="" type="checkbox"/> Activé		Autoriser ISAKMP (UDP port 500) et le protocole ESP pour le VPN IPsec Site à site (gateway-gateway)
<input checked="" type="checkbox"/> Activé		Autoriser l'accès au service DNS (port 53) du Firewall pour les interfaces protégées
<input checked="" type="checkbox"/> Activé		Bloquer et réinitialiser les requêtes ident (port 113) pour les interfaces modems (dialup)
<input checked="" type="checkbox"/> Activé		Bloquer et réinitialiser les requêtes ident (port 113) pour les interfaces ethernet
<input checked="" type="checkbox"/> Activé		Autoriser l'accès au serveur d'administration (port 1300) du Firewall pour les interfaces protégées (Serverd)
<input checked="" type="checkbox"/> Activé		Autoriser l'accès au port ssh du Firewall pour les interfaces protégées
<input checked="" type="checkbox"/> Activé		Autoriser l'accès au portail d'authentification et au VPN SSL pour les interfaces associées aux profils d'authentification (Authd)
<input checked="" type="checkbox"/> Activé		Autoriser l'accès au serveur d'administration web du firewall (WebAdmin)
<input checked="" type="checkbox"/> Activé		Autoriser les requêtes "Bootp" avec une adresse IP spécifiée pour relayer les requêtes DHCP
<input checked="" type="checkbox"/> Activé		Autoriser les clients à joindre le service VPN SSL du firewall sur les ports TCP et UDP
<input checked="" type="checkbox"/> Activé		Autoriser les sollicitations de routeur (RS) en multicast ou à destination du firewall
<input checked="" type="checkbox"/> Activé		Autoriser les requêtes au serveur DHCPv6 et les sollicitations multicast DHCPv6
<input checked="" type="checkbox"/> Activé		Ne pas tracer les paquets IPFIX dans le trafic IPFIX
<input checked="" type="checkbox"/> Activé		Autoriser la réception de paquets IGMP et PIM pour le fonctionnement du routage multicast dynamique
<input checked="" type="checkbox"/> Activé		Autoriser l'envoi des requêtes d'analyse de certificats vers une autre interface Utile pour TLS 1.3

▲ Configuration avancée

☒ Inclure les règles implicites de sortie des services hébergés (indispensable)

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 :

The screenshot shows the 'CONFIGURATION DE IN' window for the 'LAN' interface. The interface is active (ON). The name is 'LAN'. The comment is empty. The interface type is 'Interne (protégée)'. The IP addressing plan is 'Dynamique / Statique'. The IP address is '192.168.x.x/24'. The table below shows the IP configuration:

Adresse / Masque	Commentaire
192.168.x.x/24	

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 :

ROUTES STATIQUES IPV4

ROUTES DE RETOUR IPV4

ROUTES DE RETOUR

Rechercher...

+ Ajouter

✕ Supprimer

État	Passerelle	Interface
 on	GW_ORANGE	 FTTO_ORANGE

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 :

## RÉSEAU / DHCP

**Général**

☒ ON

☒ serveur DHCP  
☐ relai DHCP

**Paramètres par défaut**

Nom de domaine:   
 Passerelle:   
 DNS primaire: dns1.google.com  
 DNS secondaire: dns2.google.com

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.

Rechercher...	+ Ajouter	X Supprimer			
Plage d'adresses	Passerelle	DNS primaire	DNS secondaire	Nom de domaine	
dhcp_range	Firewall_LAN_	default	default	Domaine par défaut	
DHCP_	Firewall-bridge-LAN		dns1.google.com		.local
DHCP_INVITE	Firewall-WIFI-INVITE	dns1.google.com	dns2.google.com		Invite.local

## RÉSERVATION

Rechercher...	+ Ajouter	X Supprimer			
Réservation ↑	Passerelle	DNS primaire	DNS secondaire	Nom de domaine	
ENREGISTREUR_TEMPER...	default	default	default	Domaine par défaut	
ENREGISTREUR_TEMPER...	Firewall-bridge-LAN	default	default	Domaine par défaut	
ENREGISTREUR_TEMPER...	Firewall-bridge-LAN	dns2.google.com	dns1.google.com	Domaine par défaut	

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 :

CRÉER UN OBJET

Machine  
Nom DNS (FQDN)  
Réseau  
Plage d'adresses  
Routeur  
Groupe  
Protocole IP  
Port  
Groupe de ports

Nom de l'objet

Adresse IPv4

Adresse MAC  (Facultatif)

Résolution

☐ Aucune (IP statique)
☒ Automatique

Commentaire

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.

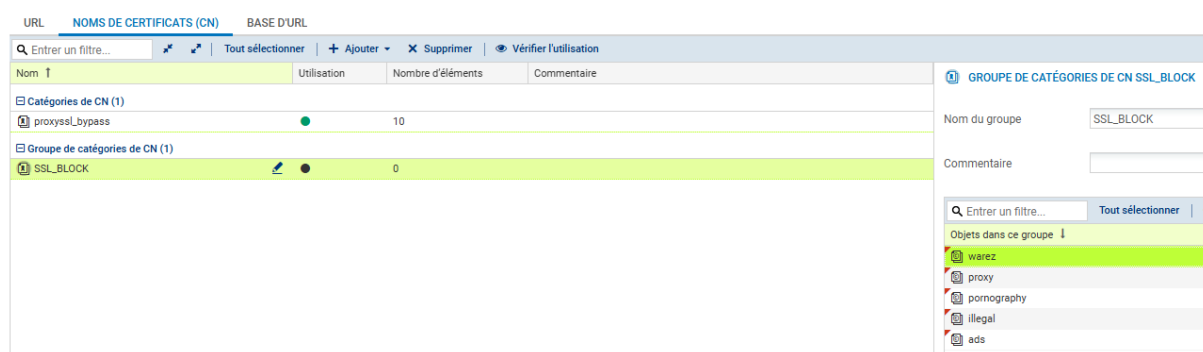
L'objet Plage d'adresses permet de cibler plusieurs IP d'affilée, comme de 192.168.1.10 à 192.168.1.20, sans être obligé de passer par un masque.

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.

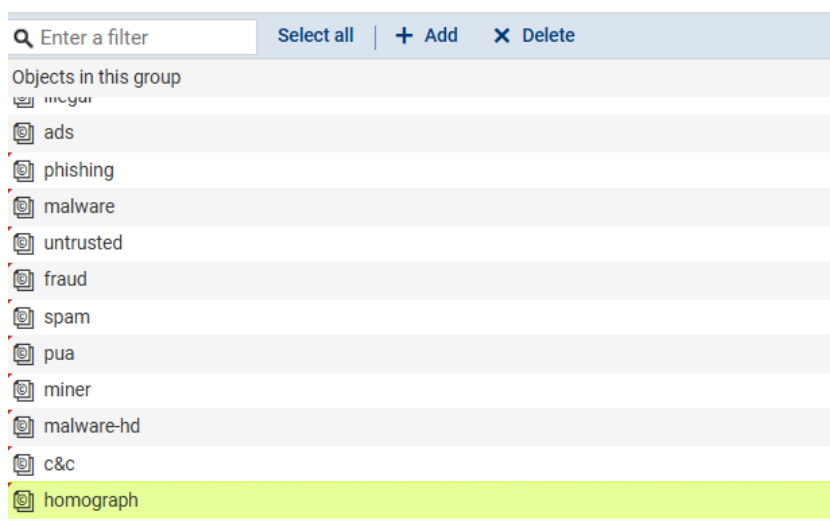
Ces objets simplifient la gestion du pare-feu : on les crée une fois, et on les réutilise dans les règles de filtrage, NAT, ou VPN.

## URL :



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 disparaîtra pour laisser la place à celle-là :



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 à expliquer.

### 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 :

VPN / VPN IPSEC

POLITIQUE DE CHIFFREMENT - TUNNELS    CORRESPONDANTS    IDENTIFICATION    **PROFILS DE CHIFFREMENT**

+ Ajouter    Actions

IKE (5)

- DR
- ☒ StrongEncryption
- GoodEncryption
- Mobile
- P1\_MEGAO\_2025**

IPsec (4)

- DR
- ☒ StrongEncryption
- GoodEncryption
- Mobile

**PROFIL IKE : P1\_MEGAO\_2025**

Général

Commentaire

Diffie-Hellman par défaut: DH14 MODP Group (2048-bits)

Durée de vie maximum (en secondes): 21600

PROPOSITIONS

+ Ajouter    X Supprimer    Monter    Descendre

	Chiffrement		Authentification		Groupe DH ⓘ
	Algorithme	Force	Algorithme	Force	
1	aes_gcm_16 (recom...	256	—	—	

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.

CRÉER UNE PASSERELLE DISTANTE

SÉLECTIONNER LA PASSERELLE - ASSISTANT DE CRÉATION DE CORRESPONDANT



Passerelle distante: vpn.cloud.megao.co

Nom: MegaO Infra Hébergée

Version IKE: IKEv1

X ANNULER    << PRÉCÉDENT    SUIVANT >>

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.

## CRÉER UNE PASSERELLE DISTANTE

## IDENTIFICATION DU CORRESPONDANT - ASSISTANT DE CRÉATION DE CORRESPONDANT

Type d'authentification	<input type="radio"/> Certificat <input checked="" type="radio"/> Clé pré-partagée (PSK)
Certificat	Sélectionner un certi <input type="button" value="x"/>
Autorité de confiance	Sélectionner une CA <input type="button" value="x"/>
Clé pré-partagée (PSK)	5 <input type="button" value="x"/>
Confirmer	5i <input type="button" value="x"/>
Saisir la clé en caractères ASCII	<input checked="" type="checkbox"/>

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.

## MEGAO INFRA HÉBERGÉE

Général	
Commentaire	<input type="text"/>
Passerelle distante	vpn.cloud.megao.com <input type="button" value="x"/>
Adresse locale	Any <input type="button" value="x"/>
Profil IKE	P1_MEGAO_2025 <input type="button" value="x"/>
Version IKE	IKEv1 <input type="button" value="x"/>
Identification	
Méthode d'authentification	Clé pré-partagée (PSK) <input type="button" value="x"/>
Local ID	1 <input type="button" value="x"/>
ID du correspondant	Saisir un identifiant (optionnel) <input type="button" value="x"/>
Clé pré-partagée (PSK)	..... <input type="button" value="x"/> <input type="button" value="Éditer"/>

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.

## ASSISTANT DE POLITIQUE VPN IPSEC



Ressources locales	Choix du correspondant	Réseaux distants
Network-bridge-LAN <input type="button" value="x"/>	VPN_via_Starlink <input type="button" value="x"/>	LAN_ <input type="button" value="x"/>

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.

POLITIQUE DE CHIFFREMENT - TUNNELS					
(01) IPsec 01					
SITE À SITE (GATEWAY-GATEWAY)					
1	État	Réseau local	Correspondant	Réseau distant	Profil de chiffrement
	on	Network-bridge-LAN	VPN_via_Starlink	LAN	P2_MEGAO_2025

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 :

GÉNÉRAL
SERVEURS WEB
SERVEURS APPLICATIFS
PROFILS UTILISATEURS

**Le module VPN SSL portail est obsolète. Il sera supprimé dans une version SNS à venir.**

Activer le VPN SSL

ON

☐ uniquement l'accès aux serveurs Web  
☐ uniquement l'accès aux serveurs applicatifs  
☒ l'accès aux serveurs Web et applicatifs

Configuration avancée

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.

ÉDITION DU SERVEUR WEB IMM-ESX

Configuration du serveur

Serveur de destination

IMM-ESX

Port

https

URL : chemin d'accès

URL utilisée par le VPN SSL

<http://IMM-ESX:443/>

Nom du lien sur le portail utilisateur

IMM-ESX

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.

## AJOUTER UN SERVEUR APPLICATIF

**Configuration du serveur**

Nom du serveur applicatif: SRVDRS

Serveur de destination: SRV-DRS

Port: microsoft-ts

**Paramètres du poste utilisateur**

Adresse IP d'écoute (locale):

Port:

**Configuration avancée**

☐ Activer la compatibilité Citrix

Commande exécutée au démarrage: mstsc /v:127

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.

**PROFILS UTILISATEURS**

Q Entrer un filtre... + Ajouter X Supprimer

Nom du profil utilisateur

RDS

**ÉDITION DU PROFIL RDS**

Configuration du profil

Commentaire

**SERVEURS WEB ACCESSIBLES**

État	Serveur Web
<input type="checkbox"/> Désactivé	IMM-ESX

**SERVEURS APPLICATIFS ACCESSIBLES**

État	Serveur applicatif
<input checked="" type="checkbox"/> Activé	SRVDRS

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 :

VPN / VPN SSL

**ON** Activer le VPN SSL

PARAMÈTRES GÉNÉRAUX

VÉRIFICATION DES POSTES CLIENTS (ZTNA) (DÉSACTIVÉ)

Paramètres réseaux	
Adresse IP publique (ou FQDN) de l'UTM utilisée	21
Réseaux ou machines accessibles	Network_LAN
Réseau assigné aux clients (UDP)	LAN_VPN_UDP
Réseau assigné aux clients (TCP)	LAN_VPN_TCP
Maximum de tunnels simultanés autorisés	100

Paramètres DNS envoyés au client	
Nom de domaine	local
Serveur DNS primaire	srv-ad- local
Serveur DNS secondaire	Configuré pour le firewall

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 servi du serveur PPTP 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 sécuriser 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 :



J'ai plus qu'à regarder où sont branchés les fils 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 :

ASSISTANT DE CRÉATION D'ANNUAIRE UTILISATEUR

SÉLECTIONNEZ LE TYPE DE RÉPERTOIRE - (ÉTAPE 1 SUR 3)



- ☒ Se connecter à un annuaire Microsoft Active Directory
- ☐ Se connecter à un annuaire LDAP externe
- ☐ Se connecter à un annuaire LDAP externe PosixAccount
- ☐ Se connecter à un annuaire LDAP interne

✖ ANNULER

« PRÉCÉDENT

SUIVANT »

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.

USERS / ACCESS PRIVILEGES

DEFAULT ACCESS		DETAILED ACCESS		PPTP SERVER			
Searching...		+ Add	✖ Delete	↑ Up ↓ Down			
Status	User - user group	SSL VPN Portal	IPSEC	SSL VPN	Sponsorship	Description	
1	G_acces_TSE_via_stormshield@.local	Block	Block	Allow	Block		

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.

## ASSISTANT DE CRÉATION D'ANNUAIRE UTILISATEUR

## AUTHENTIFICATION - (ÉTAPE 3 SUR 3)



Activer le profil d'authentification 0 (interne) sur l'interface sélectionnée

LAN

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.

## ASSISTANT DE CRÉATION D'ANNUAIRE UTILISATEUR

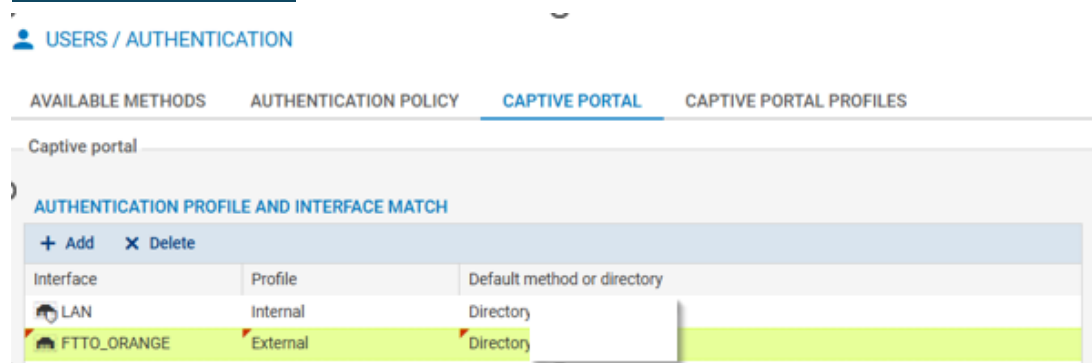
## ACCÉDER AU RÉPERTOIRE - (ÉTAPE 2 SUR 3)



Nom de domaine	local
Serveur	srv-ad: local
Port	ldap
Domaine racine (DN de base)	dc: dc=local
Connexion (DN utilisateur)	stormshield@ local
Mot de passe	.....
Hachage du mot de passe	SHA

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 :



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](#)

[Point-to-Point Tunneling Protocol — Wikipédia](#)