Mise en place stormshield

Table des matières

Introduction

Stormshield est un firewall très connu le mùodele que j'ai est le SN200 dans cette documentation je vais découvrir l'installation de ce denier

Login par défaut : Admin

Password par défaut : Sur l'étiquette derrière

Pour tout reset pour partir sur une base propre « DEFAULCONFIG » dans le terminal

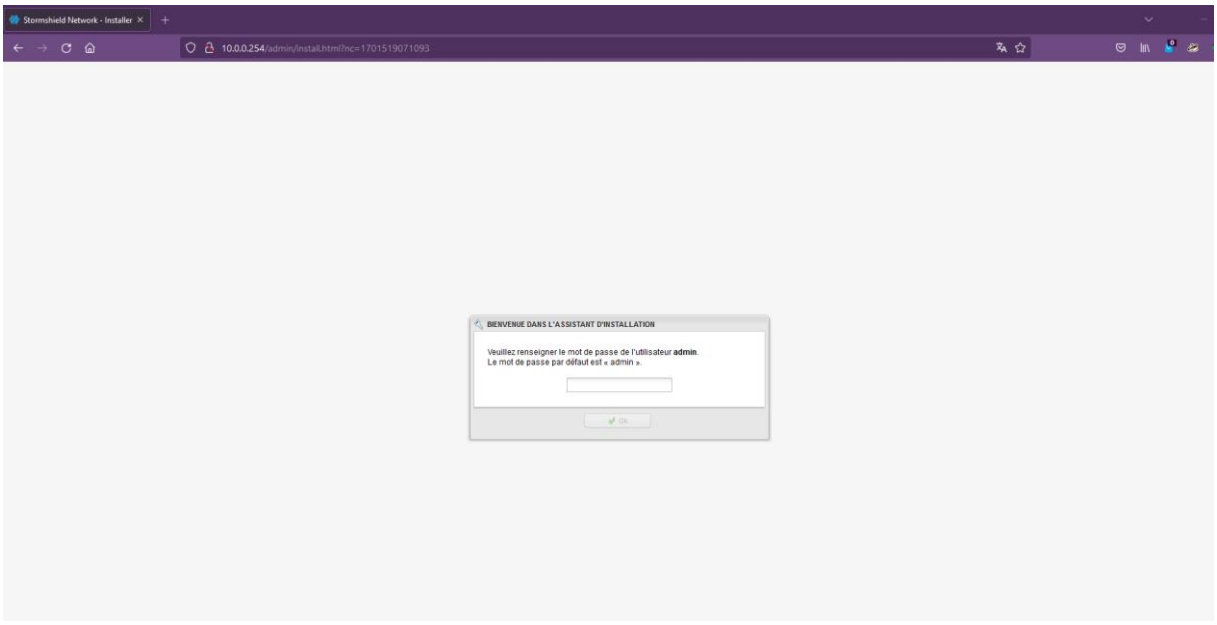
Une fois que j'ai réinitialisé l'ip est 10.0.0.254 /8 et le clavier est en qwerty

Important pour désactiver le filtrage en cli et pouvoir travailler « enfilter off »

Solution pour se connecter il fallait créer le fichier de rules et changer la date pour la mettre en 2005 et ne pas avoir la licence qui est expirée

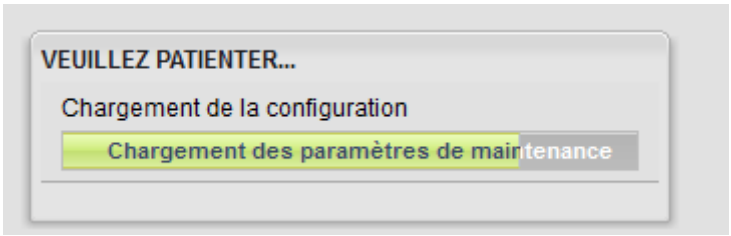
Ensuite remettre enfilter off, ouvrir un wireshark et se connecter et aussi mettre un masque en /24 pas /8

Résultat

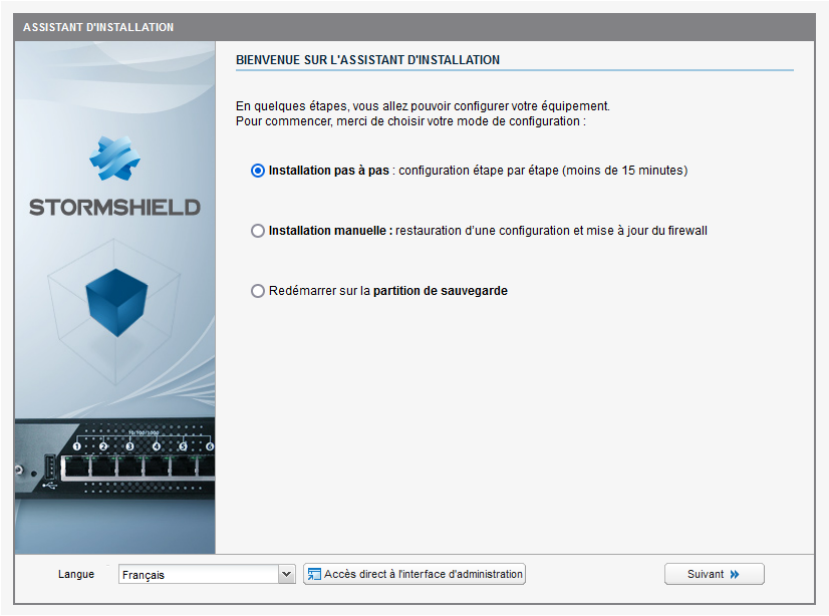


Renseigner le mdp qui est sur le boitier

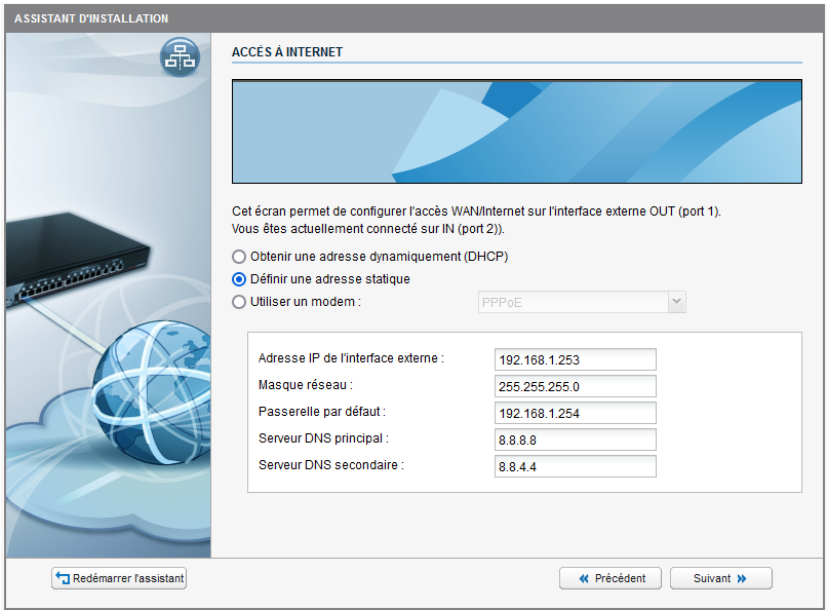
La configuration charge



Un assistant apparait je lance une install pas à pas

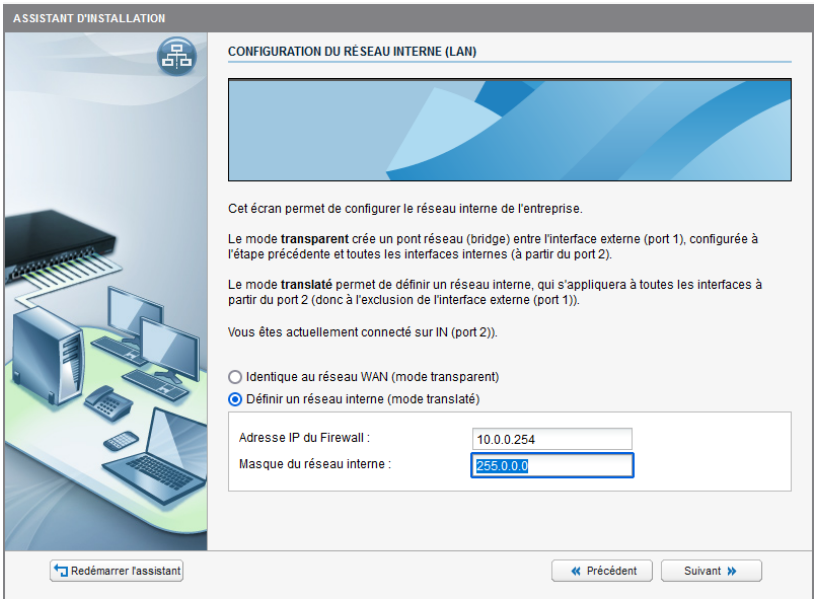


Configuration interface out



Le firewall renverra tout les requetes vers mon routeur qui est dans le réseau de mon domicile

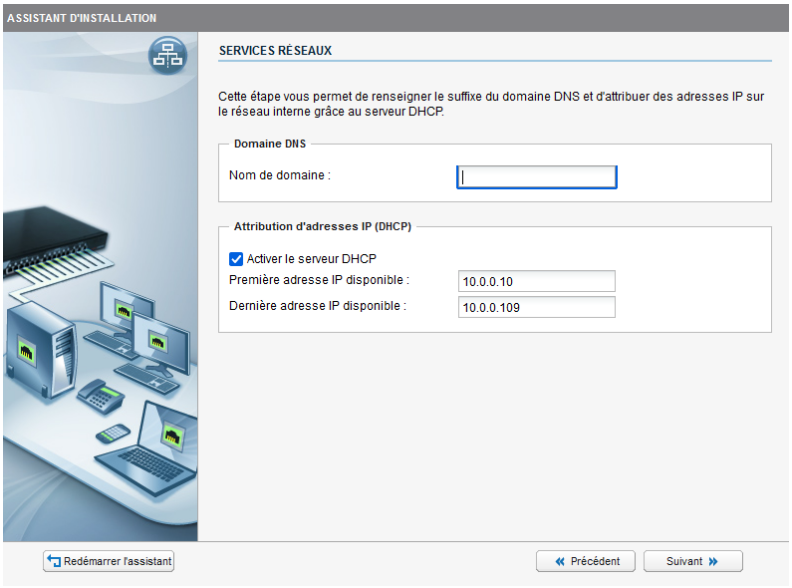
Configuration interface IN



Je choisis de configurer un réseau interne séparer de mon interface WAN pour bien tout segmenter

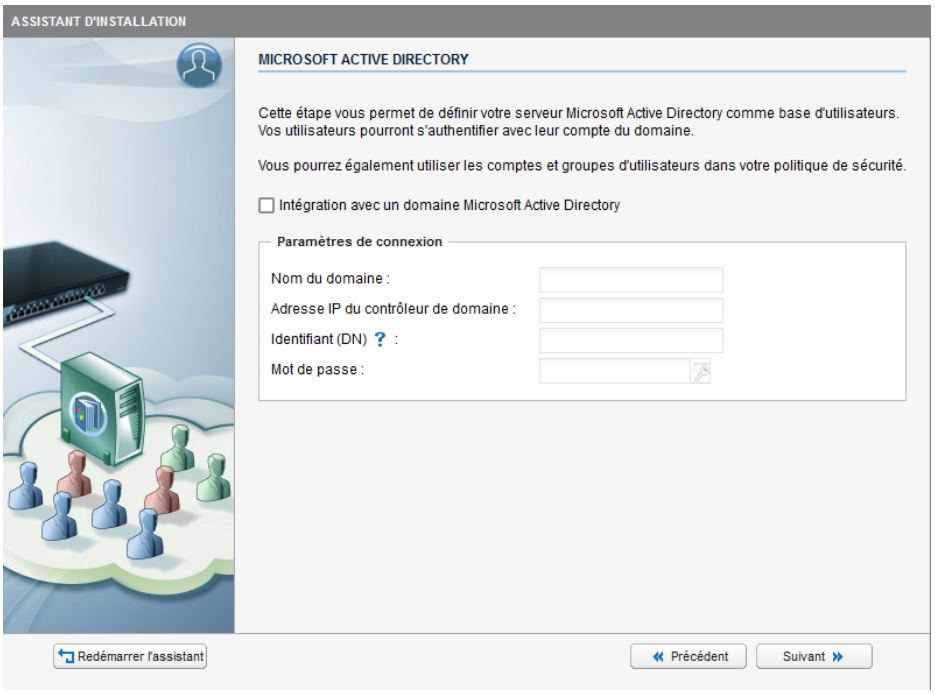
Juste le masque je le change et je mets du /24

Dhcp et zone dns

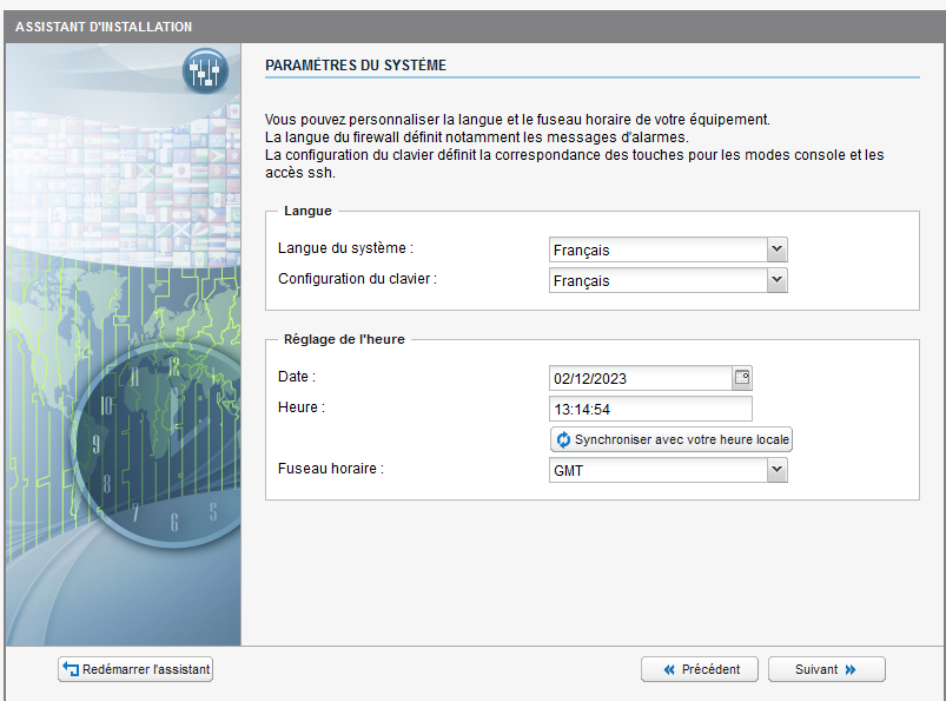


Intégration AD

Pour l’instant je ne l’integre pas à un AD

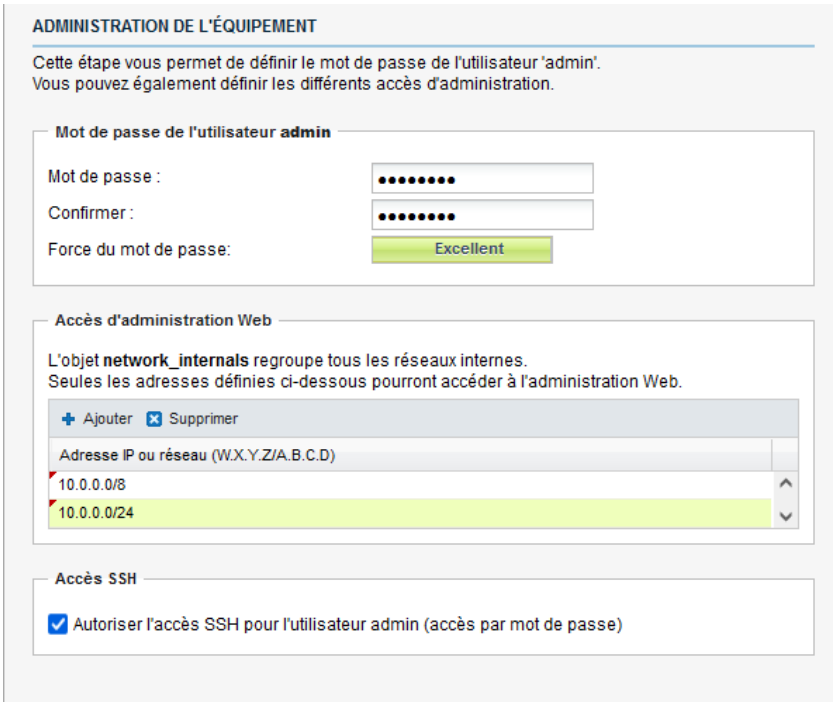


Configuration horaire

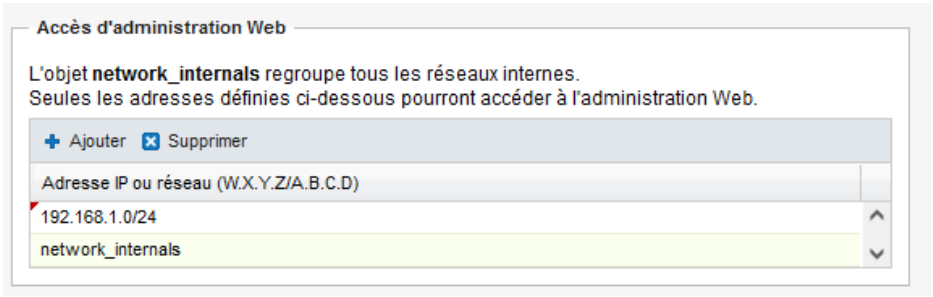


Configuration administration de l'équipement

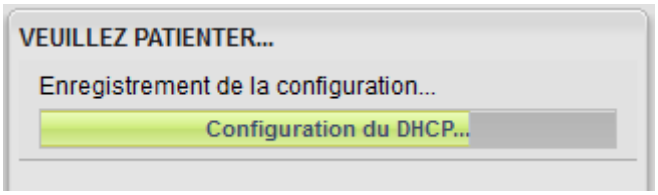
Je mets le sréseaux qui pourront avoir accès à l'interface web



Je définis un mdp et j'active ssh



Mise à jour



Enregistrement

ENREGISTREMENT

Produit

Numéro de série : SN200A25B2816B7

Partenaire : sadek

Mot de passe d'enregistrement (WEB) ? : c7836e93

(•) Nouveau client ( ) Client existant

Société (utilisateur final)

Nom : Sadek

Téléphone : [redacted]

Ville : Paris

Code postal : [redacted]

Pays : France

Adresse : [redacted]

Contact (utilisateur final)

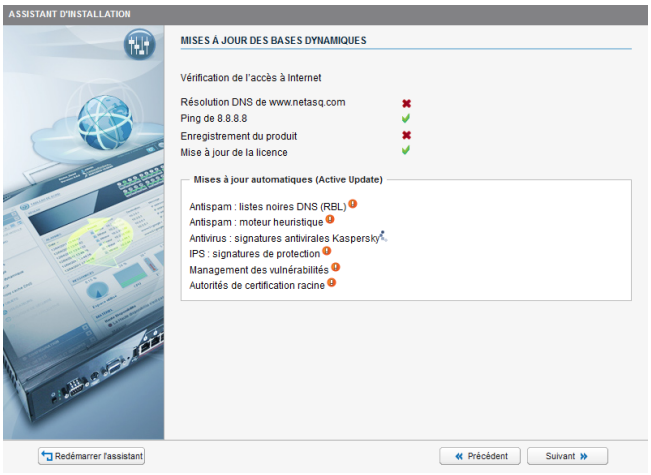
Nom : sadek

Prénom : adel

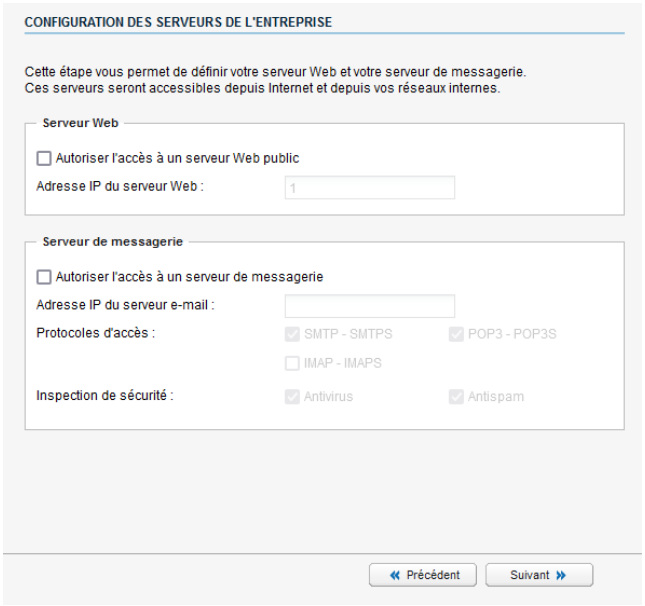
E-mail : asadek@sadek.ovh

« Précédent | Suivant »

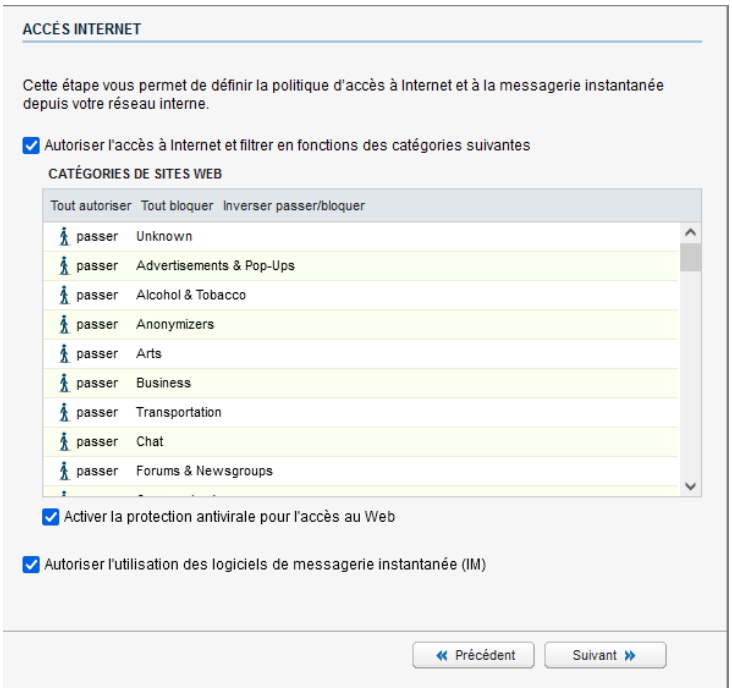
Mises à jour des bases



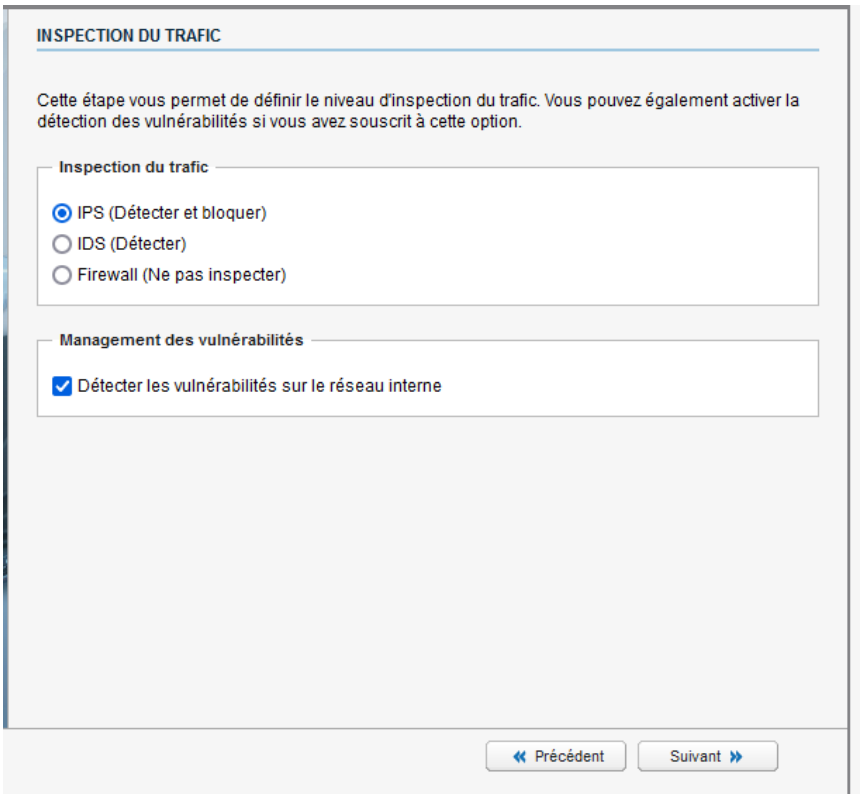
DNAT serveur web et smtp



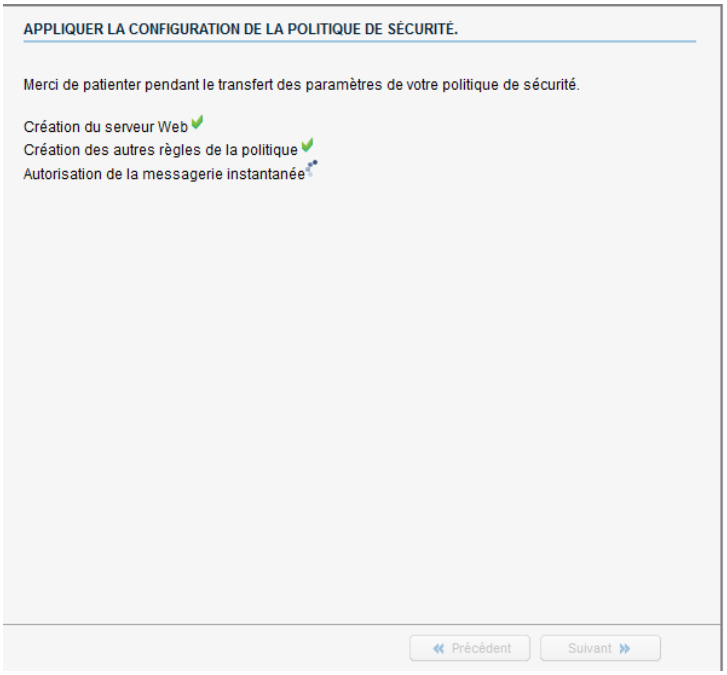
Filtrage URL



IPS/IDS

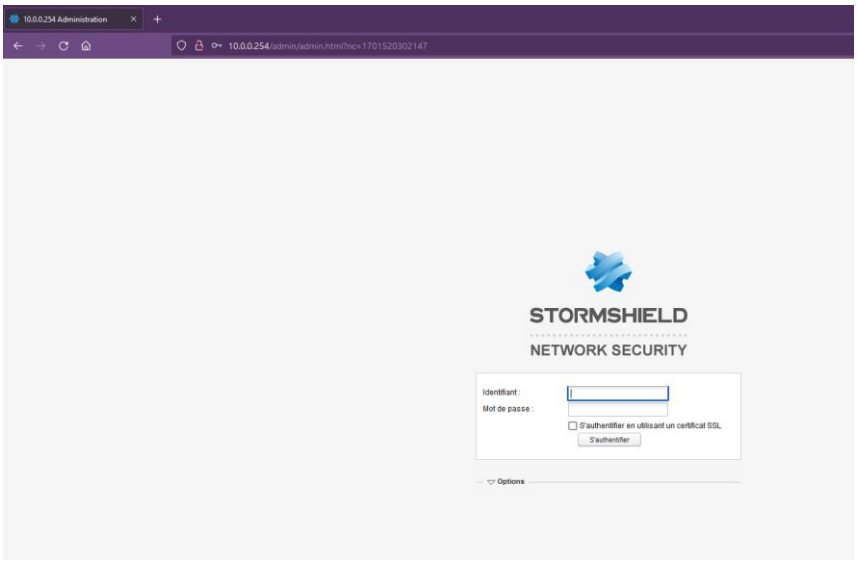


Application

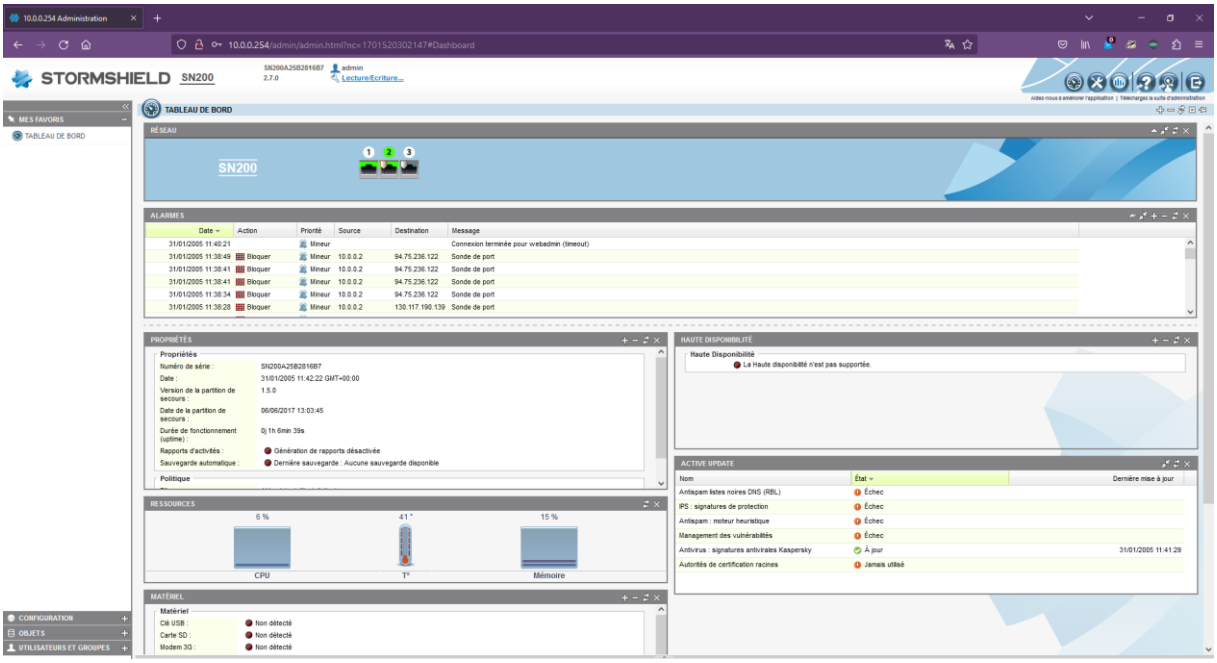


Fin de l'installation

Me voila connecter à l'interface web

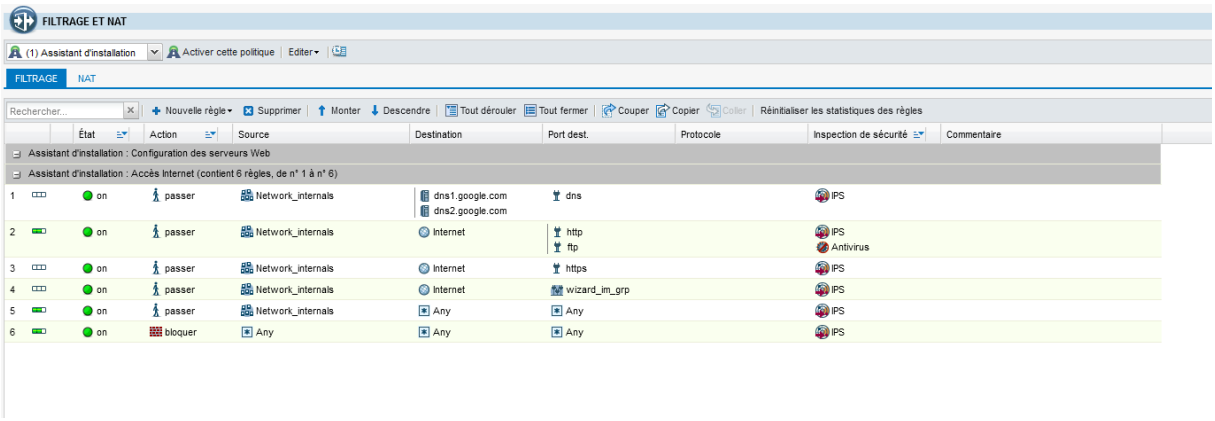


Accès à l'interface web

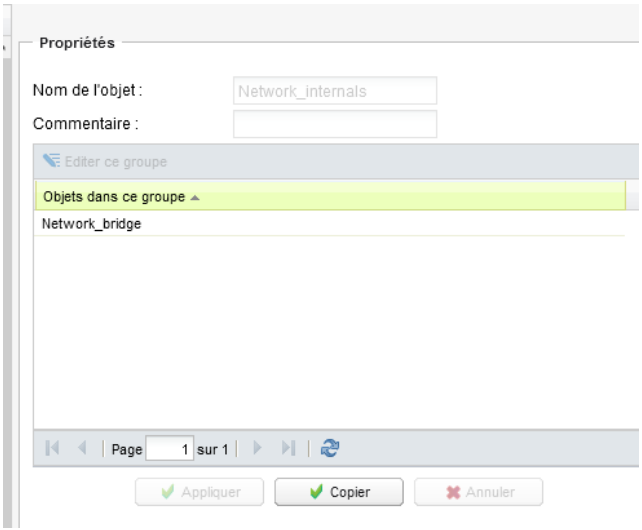


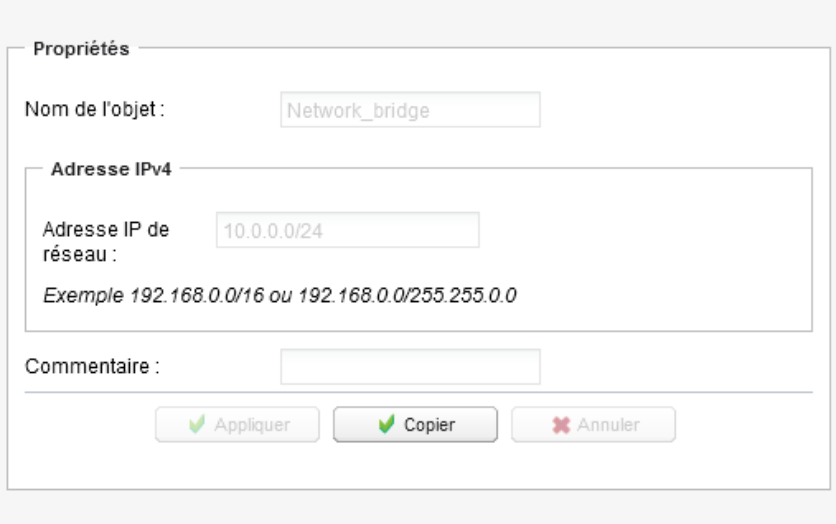
Règles de filtrage

Pour les consulter il faut aller dans Configuration > Politique de sécurité > Filtrage et NAT



Network internal est un objet qui contient l'objet Network_Bridge

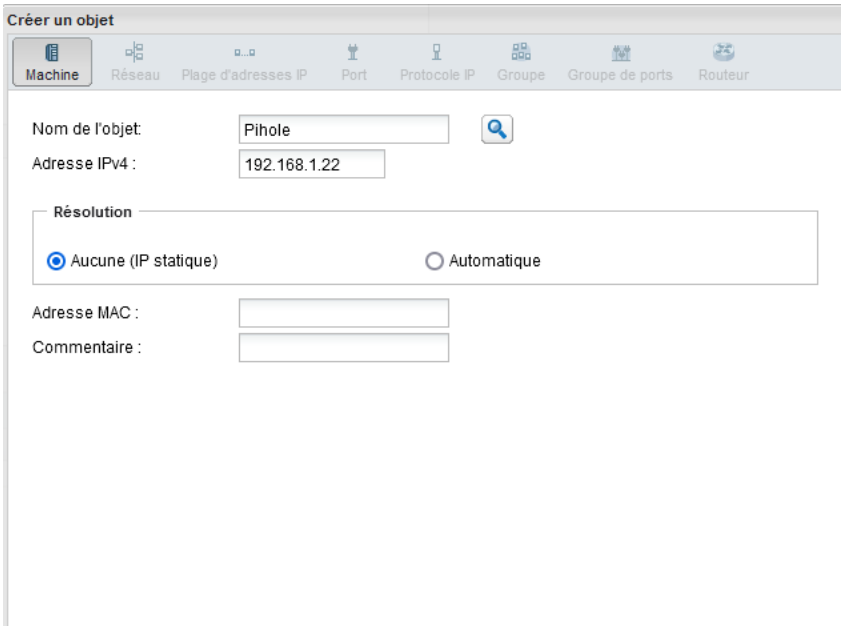


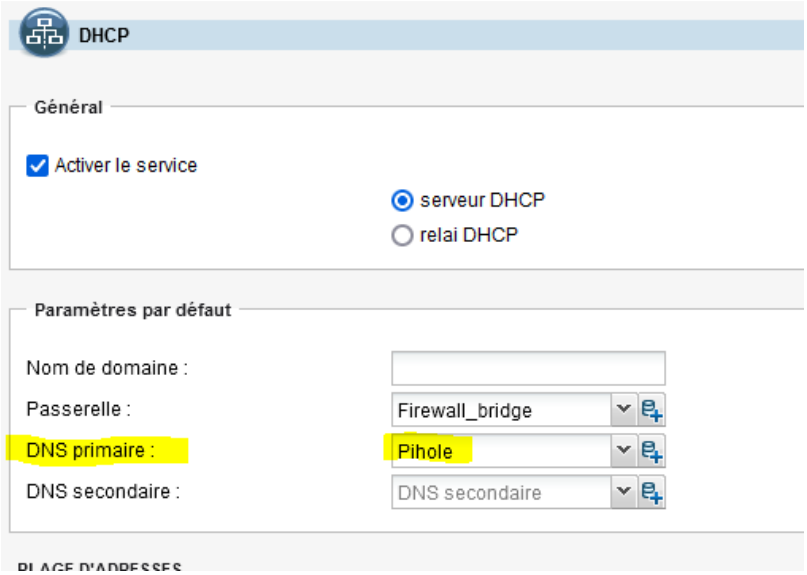


Création objet pour DNS

Je pense qu'avec ce dns tout fonctionne avec des objets

Je crée donc un object pihole

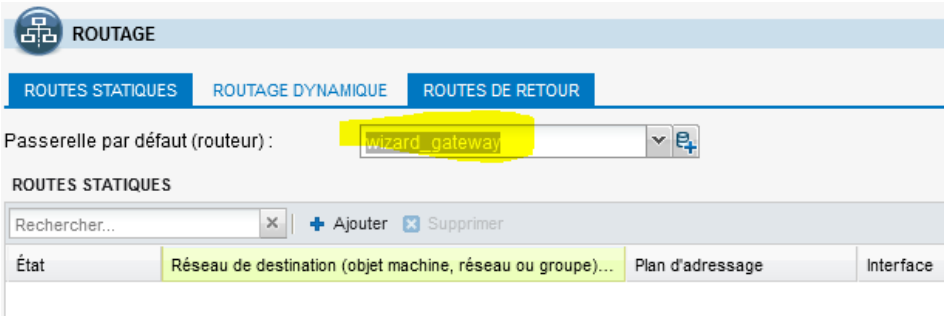


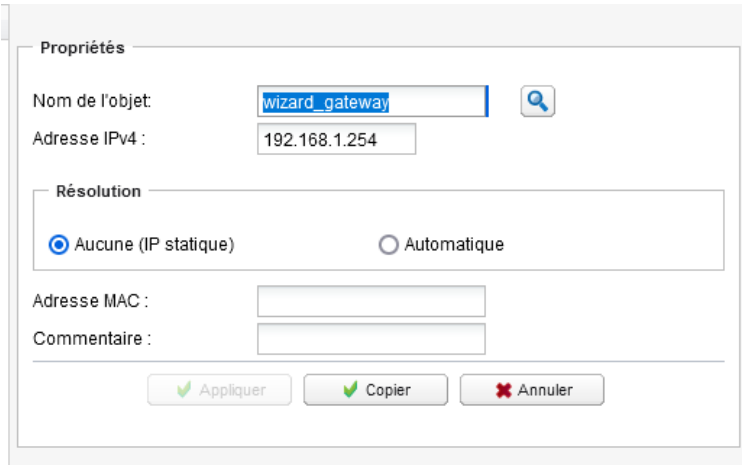


Route par défaut

Dans réseau >routage

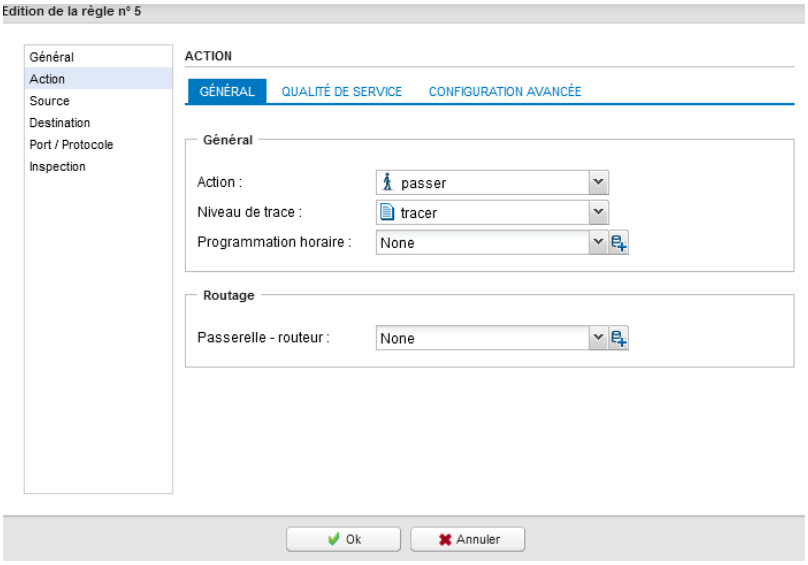
Je peux voir que la passerelle par défaut est un objet

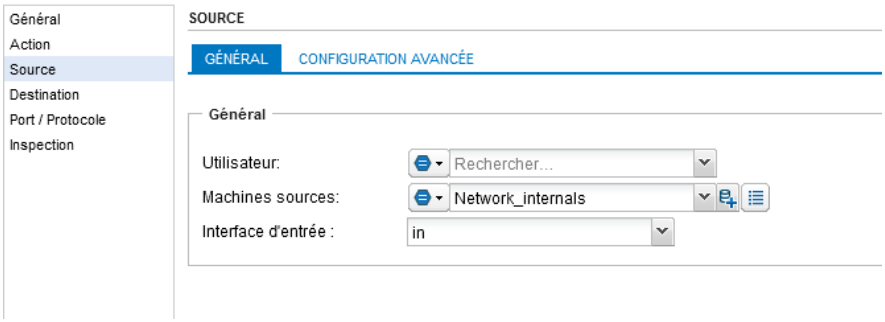


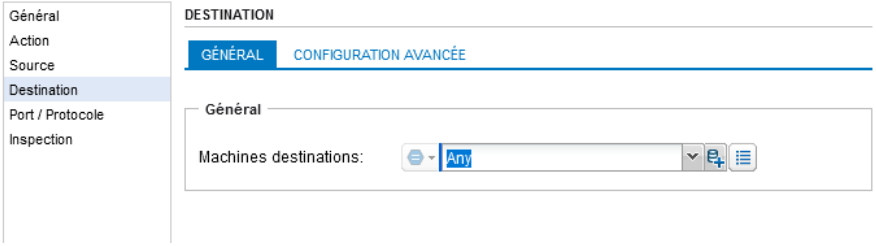


Création d'une règle

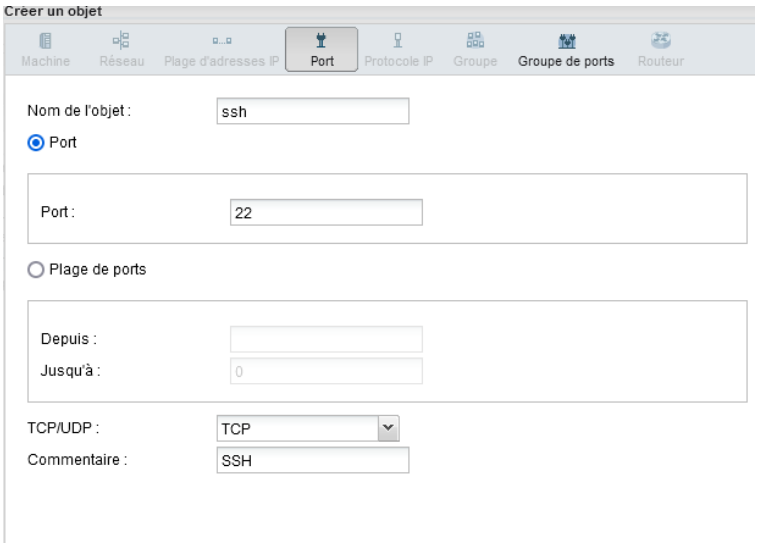
Je veux créer une regle qui me permettra d'utiliser ssh (port 22)



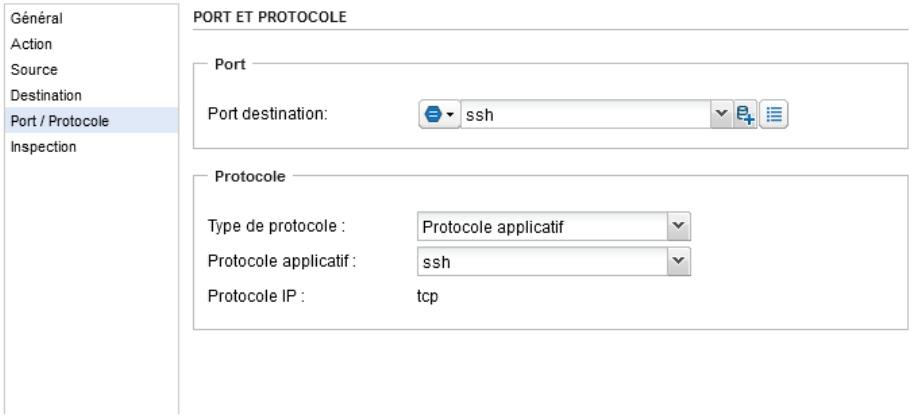


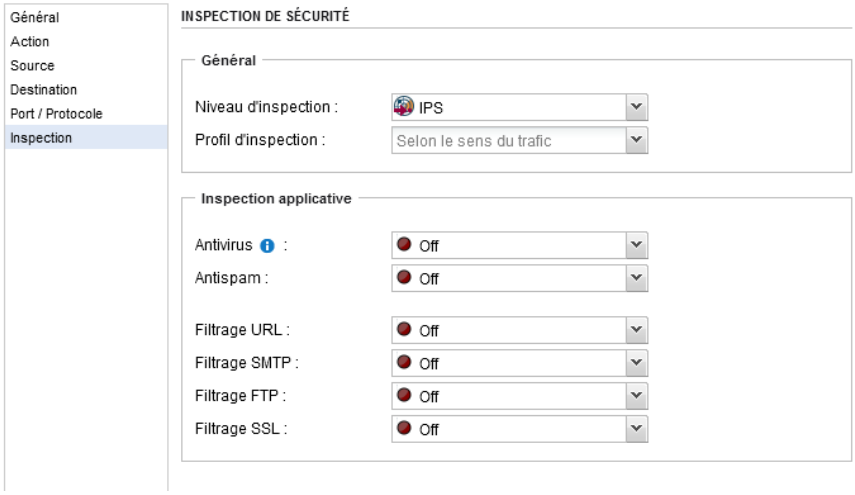


Il n’ya pas d’objet ssh j’en crée un dans la foulée

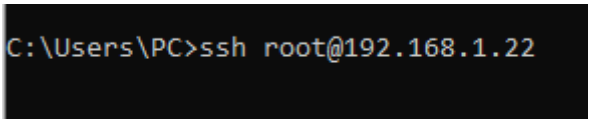


On peut aussi dire que l’on veut que sa soit que le protocole ssh applicatif qui pourra accéder au port 22

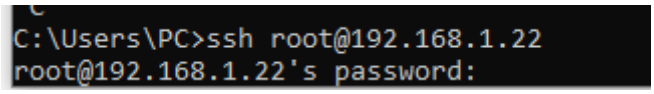




Avant activation de la règle



Après activation de la règle

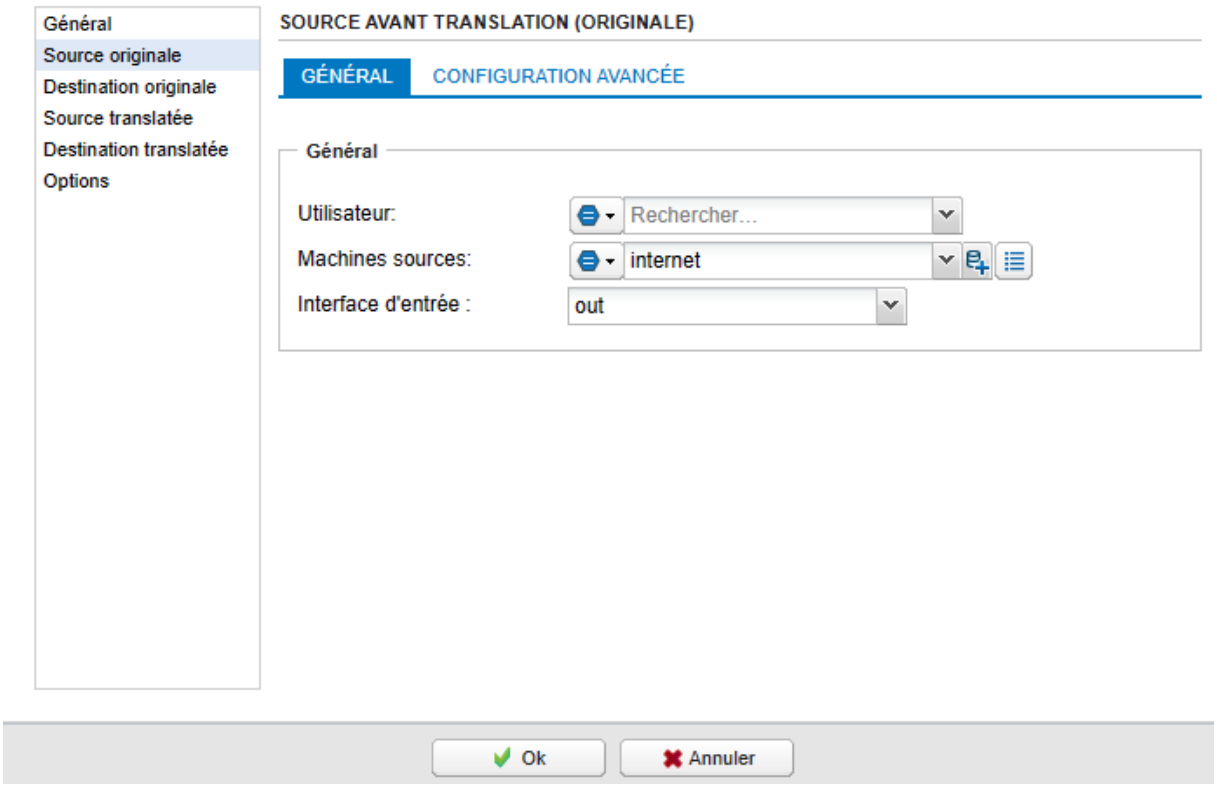


DNAT

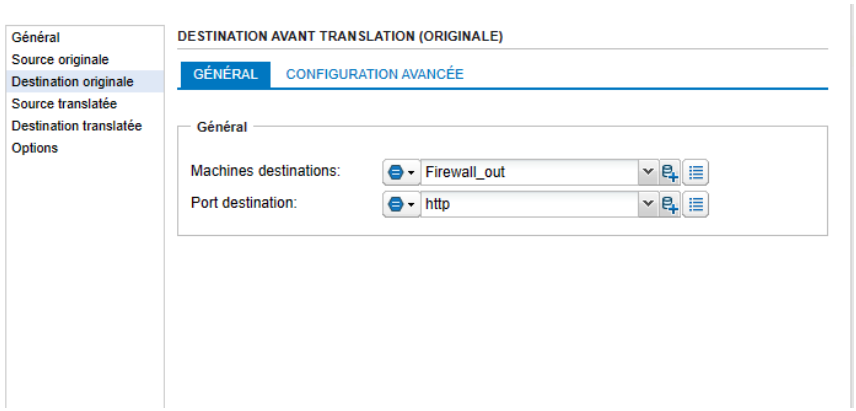
On va voir comment mettre en place une regle de DNAT

Politique de sécurité > Filtrage et Nat > NAT

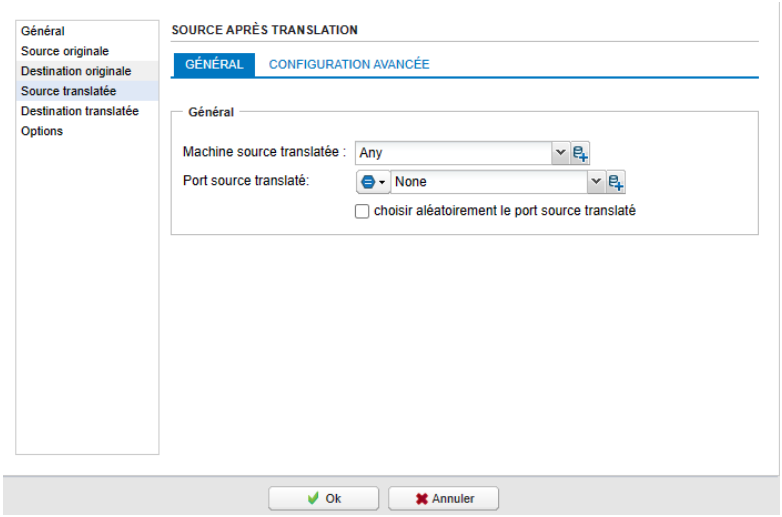
Ensuite je crée une règle



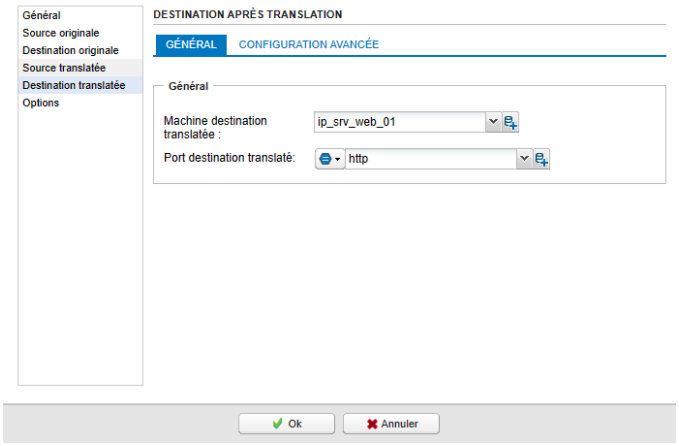
Ensuite je dis que la destination avant la translation est l'ip du firewall sur sa patte externe et le port de destination

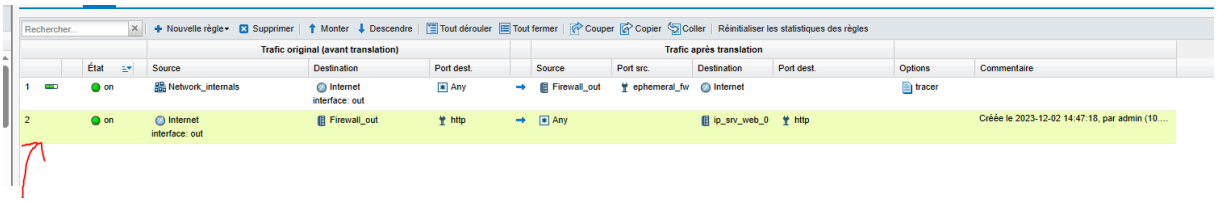


Ensuite je définis vers qui sera transferer le paquet son ip et port bien faire attention « Source après translation » sa sera l'IP source du paquet est ce que on la modifie ou non en l'occurrence ici non

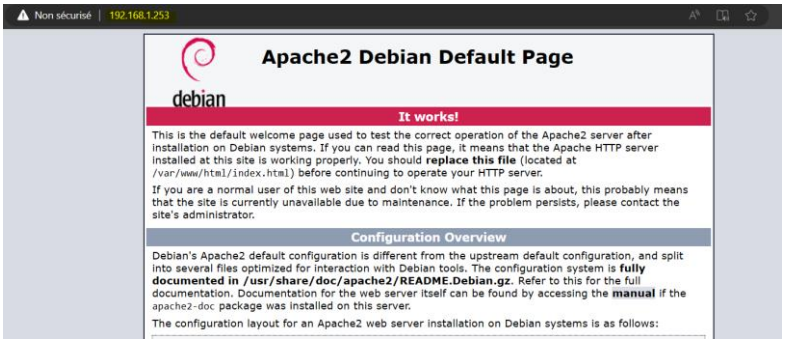


Ici c'est la destination apres la translation pour enfin mapper le port du routeur au port de notre machine





Résultat



Route Statique

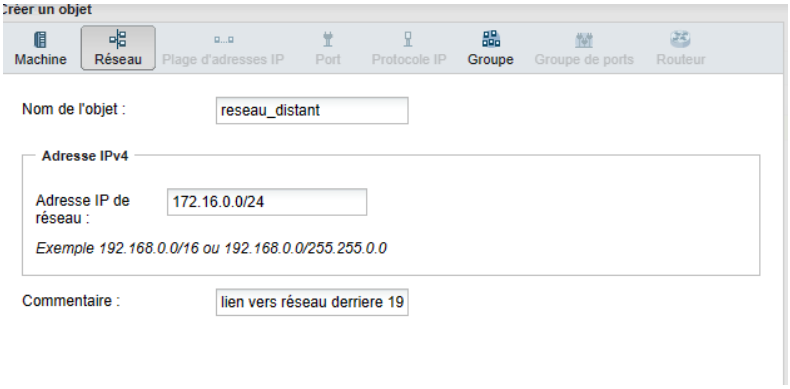
Dans le réseau de l'interface out il y'a un routeur son IP est 192.168.1.22 il doit permettre d'acceder au réseau 172.16.0.254 (auquel il est relier à un vpn ssl site to site)

Du coup il faut que je crée une route qui dit que pour atteindre le réseau 172.16.0.0/24 il faut passer par 192.168.1.22 en utilisant mon interface out avec l'ip 192.168.1.253

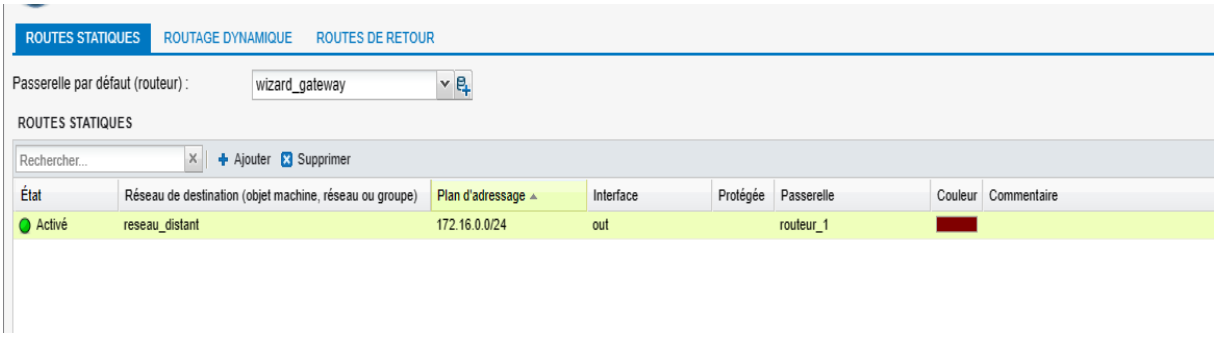
Mise en place

Il faut se rendre dans Réseau > Routage > Routes Statiques

Je crée d'abord un objet

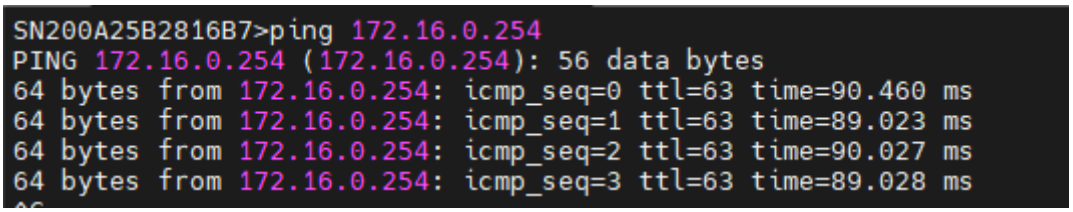


Routeur_1 = 192.168.1.22



Je n'omets surtout pas de mettre en place du nat sur ce routeur (routeur 1)

Je me connecte en ssh sur mon Stormshield et je vérifie que je peux pinguer le routeur du nouveau réseau sois 172.16.0.254



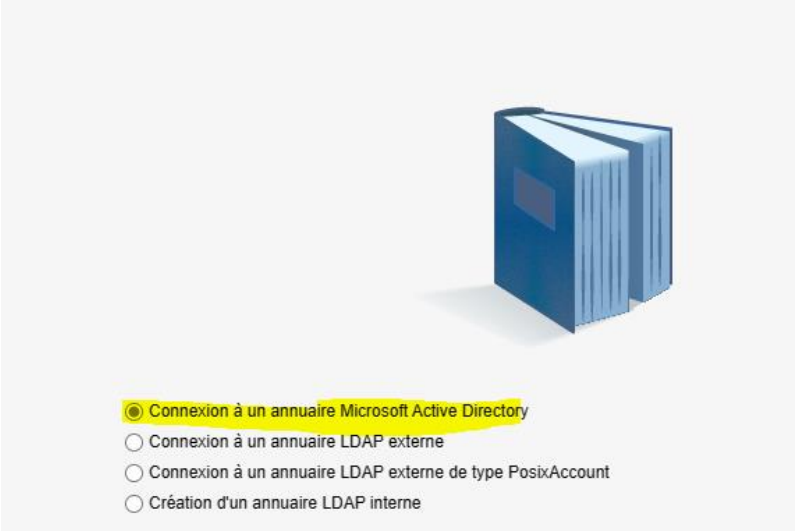
Test depuis un client du réseau interne du Stomshield

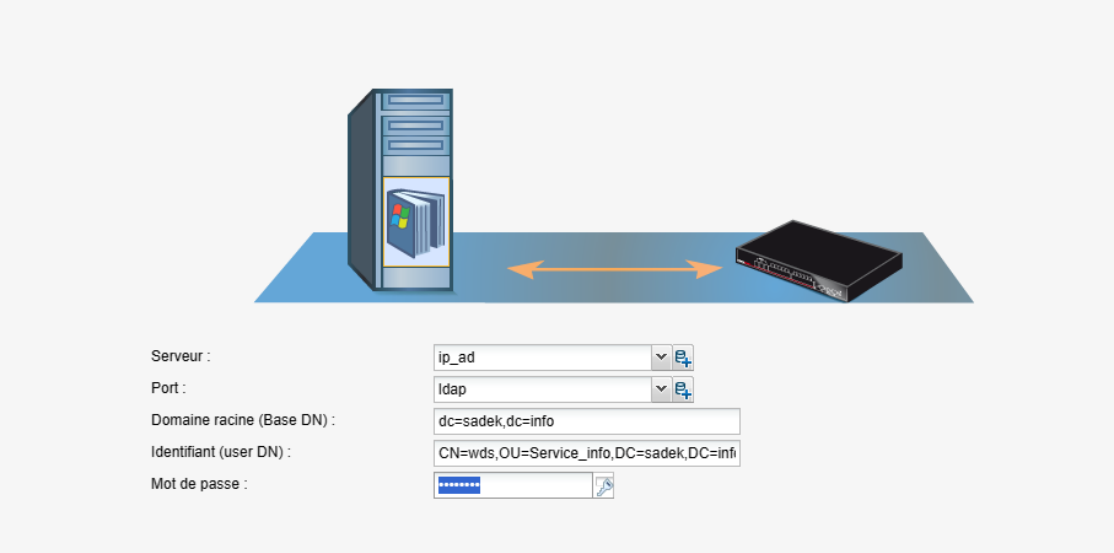
```
C:\Users\PC>ping 172.16.0.254

Envoi d'une requête 'Ping'  172.16.0.254 avec 32 octets de données :
Réponse de 172.16.0.254 : octets=32 temps=97 ms TTL=63
Réponse de 172.16.0.254 : octets=32 temps=93 ms TTL=63
Réponse de 172.16.0.254 : octets=32 temps=92 ms TTL=63
```

Connexion annuaire LDAP (AD)

Maintenant que dans le chapitre plus haut j'ai créé une route vers mon réseau avec mes serveur, je vais connecter mon stormshield à mon annuaire LDAP

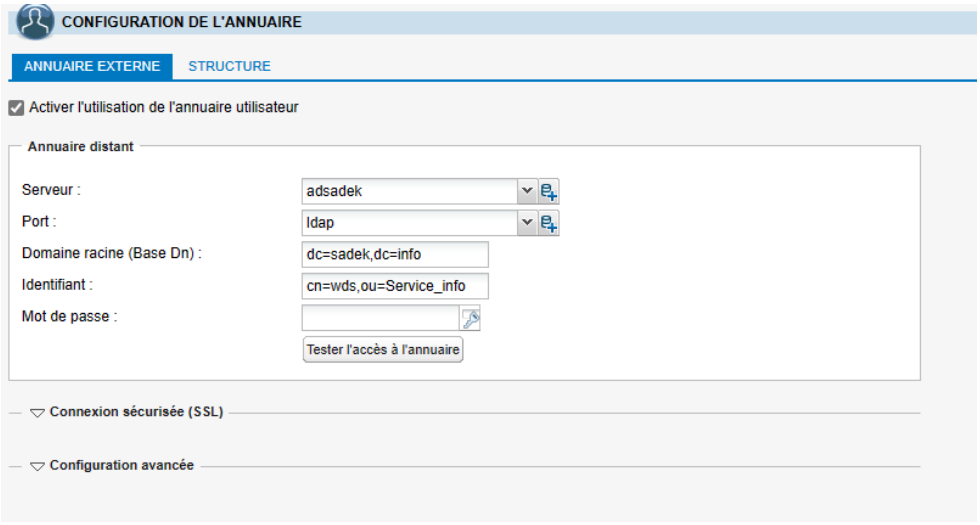
Il faut d'abord se rendre dans Utilisateur > Configuration de l'annuaire



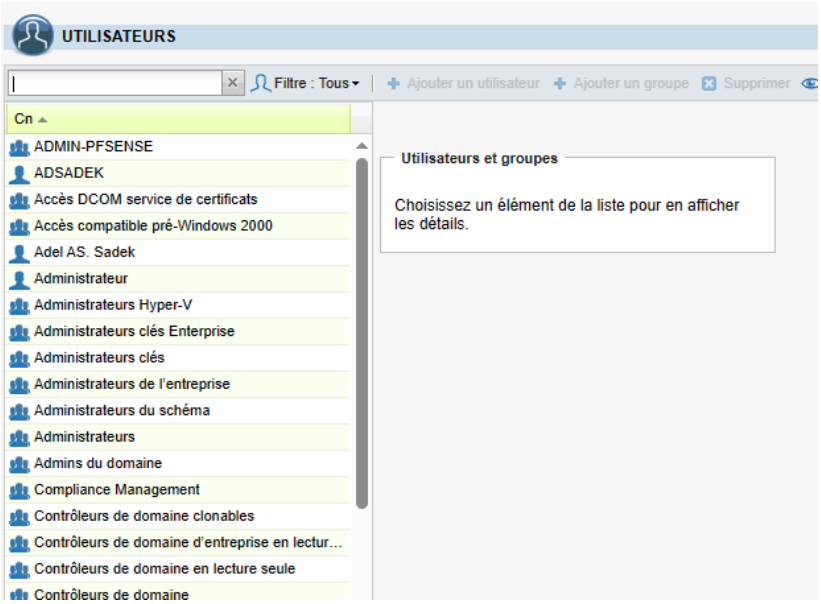


Problème sur l'authentification LDAP on verra ça plus tard

Update : J'ai trouvé l'erreur il fallait que je mette tout en minuscule et que dans l'id sa soit juste la partie qu'il n'y a pas plus sois UO → User , j'ai donc renseigné les champs comme ceci

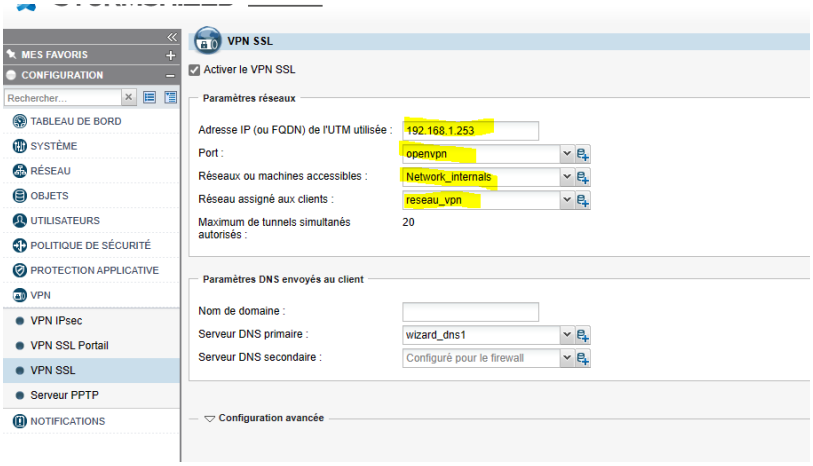


Dans Configuration > Utilisateurs, je peux lancer une recherche d'users dans l'annuaire



Mise en place VPN

Il faut se rendre dans Configuration > VPN > VPN SSL



Ici j'ai défini l'ip de l'interface out de mon FW pour réceptionner les connexions vpn depuis cette derniere(rectification si le firewall est derrière un routeur et qu'il y'a règle de PAT mettre IP, de ce routeur et le port de ce routeur et ne pas oublier règle de filtrage pour autoriser réseau vpn etc etc)

Ensuite je définis un port d'écoute j'ai créé un objet qui écoute sur le port 443 (je préfère TCP)

Ensuite je dis quels réseaux ou machines accessible pour qu'en échange le FW configure les routes nécessaires

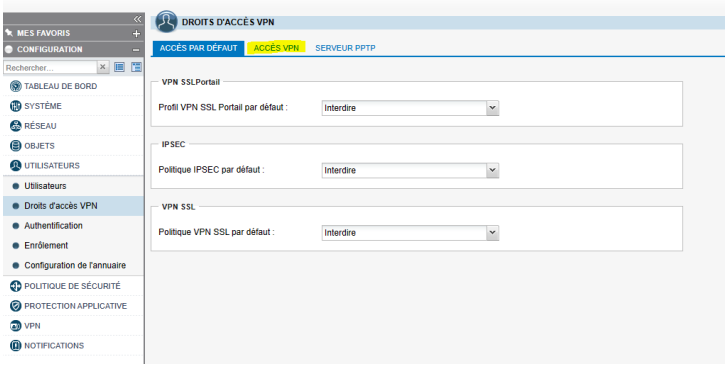
Je crée aussi un objet qui contient le réseau ou mes clients seront dedans.

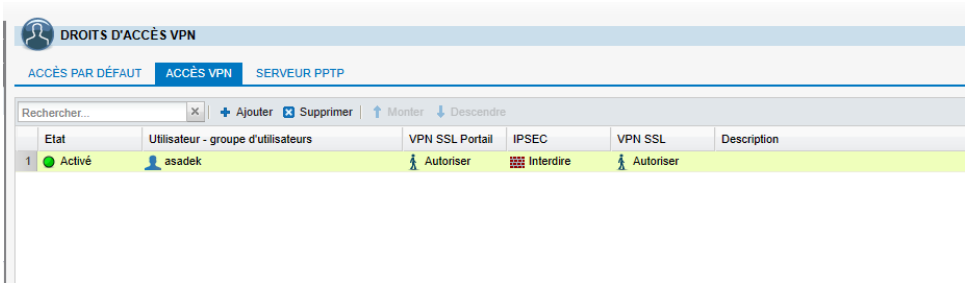
Il faut ensuite que j'installe le client vpn

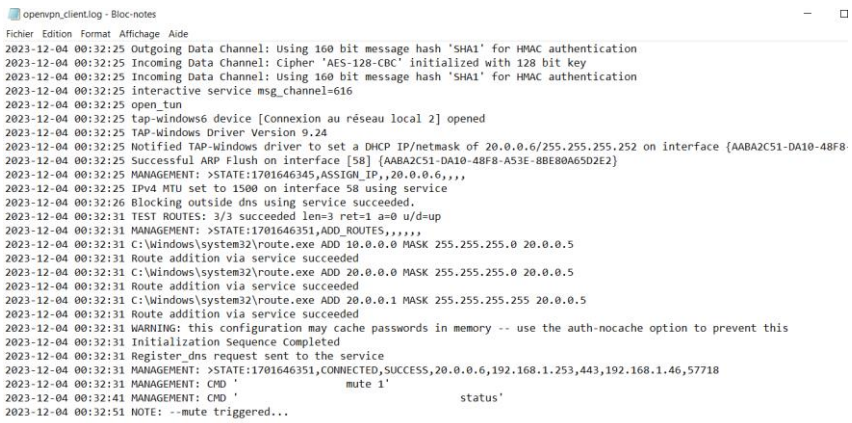
Il faut activer le portail SSL sur les interfaces externes pour que le VPN fonctionne

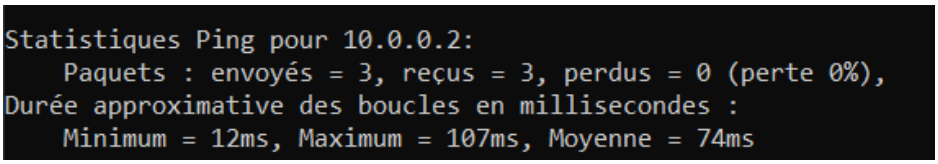
Il faut aussi autoriser l'user à utiliser le vpn

Il faut se rendre dans Configuration > Utilisateurs > Droits d'accès VPN


MES FAVORIS
CONFIGURATION
Rechercher...
TABLEAU DE BORD
SYSTÈME
RÉSEAU
OBJETS
UTILISATEURS
Utilisateurs
Droits d'accès VPN
Authentification
Enrôlement
Configuration de l'annuaire
POLITIQUE DE SÉCURITÉ
PROTECTION APPLICATIVE
VPN
NOTIFICATIONS
DROITS D'ACCÈS VPN
ACCÈS PAR DÉFAUT
ACCÈS VPN
SERVEUR PPTP
VPN SSLPortail
Profil VPN SSL Portail par défaut :
Interdire
IPSEC
Politique IPSEC par défaut :
Interdire
VPN SSL
Politique VPN SSL par défaut :
Interdire

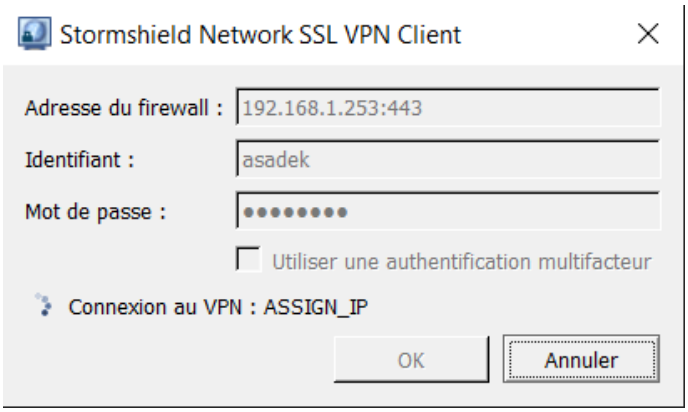

DROITS D'ACCÈS VPN
ACCÈS PAR DÉFAUT
ACCÈS VPN
SERVEUR PPTP
Rechercher...
Ajouter
Supprimer
Monter
Descendre
Etat
Utilisateur - groupe d'utilisateurs
VPN SSL Portail
IPSEC
VPN SSL
Description
1
Activé
asadek
Autoriser
Interdire
Autoriser


openvpn_client.log - Bloc-notes
Fichier Edition Format Affichage Aide
2023-12-04 00:32:25 Outgoing Data Channel: Using 160 bit message hash 'SHA1' for HMAC authentication
2023-12-04 00:32:25 Incoming Data Channel: Cipher 'AES-128-CBC' initialized with 128 bit key
2023-12-04 00:32:25 Incoming Data Channel: Using 160 bit message hash 'SHA1' for HMAC authentication
2023-12-04 00:32:25 interactive service msg_channel=616
2023-12-04 00:32:25 open_tun
2023-12-04 00:32:25 tap-windows6 device [Connexion au réseau local 2] opened
2023-12-04 00:32:25 TAP-Windows Driver Version 9.24
2023-12-04 00:32:25 Notified TAP-Windows driver to set a DHCP IP/netmask of 20.0.0.6/255.255.255.252 on interface {AABA2C51-DA10-48F8
2023-12-04 00:32:25 Successful ARP Flush on interface [58] {AABA2C51-DA10-48F8-A53E-8BE80A65D2E2}
2023-12-04 00:32:25 MANAGEMENT: >STATE:1701646345,ASSIGN_IP,,20.0.0.6,,,,
2023-12-04 00:32:25 IPv4 MTU set to 1500 on interface 58 using service
2023-12-04 00:32:26 Blocking outside dns using service succeeded.
2023-12-04 00:32:31 TEST ROUTES: 3/3 succeeded len=3 ret=1 a=0 u/d=up
2023-12-04 00:32:31 MANAGEMENT: >STATE:1701646351,ADD_ROUTES,,,,,,
2023-12-04 00:32:31 C:\Windows\system32\route.exe ADD 10.0.0.0 MASK 255.255.255.0 20.0.0.5
2023-12-04 00:32:31 Route addition via service succeeded
2023-12-04 00:32:31 C:\Windows\system32\route.exe ADD 20.0.0.0 MASK 255.255.255.0 20.0.0.5
2023-12-04 00:32:31 Route addition via service succeeded
2023-12-04 00:32:31 C:\Windows\system32\route.exe ADD 20.0.0.1 MASK 255.255.255.255 20.0.0.5
2023-12-04 00:32:31 Route addition via service succeeded
2023-12-04 00:32:31 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
2023-12-04 00:32:31 Initialization Sequence Completed
2023-12-04 00:32:31 Register_dns request sent to the service
2023-12-04 00:32:31 MANAGEMENT: >STATE:1701646351,CONNECTED,SUCCESS,20.0.0.6,192.168.1.253,443,192.168.1.46,57718
2023-12-04 00:32:31 MANAGEMENT: CMD '   mute 1'
2023-12-04 00:32:41 MANAGEMENT: CMD '   status'
2023-12-04 00:32:51 NOTE: --mute triggered...


Statistiques Ping pour 10.0.0.2:
Paquets : envoyés = 3, reçus = 3, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
Minimum = 12ms, Maximum = 107ms, Moyenne = 74ms

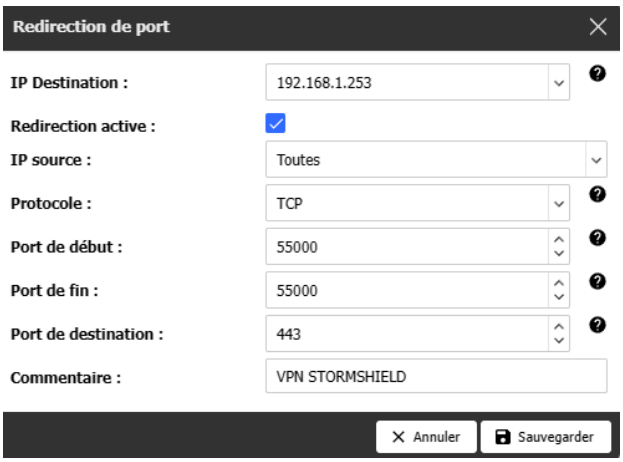
Tout accès extérieur est interdit

```
C:\Users\adels>nslookup google.com
DNS request timed out.
    timeout was 2 seconds.
Serveur :   UnKnown
Address:  8.8.8.8
```

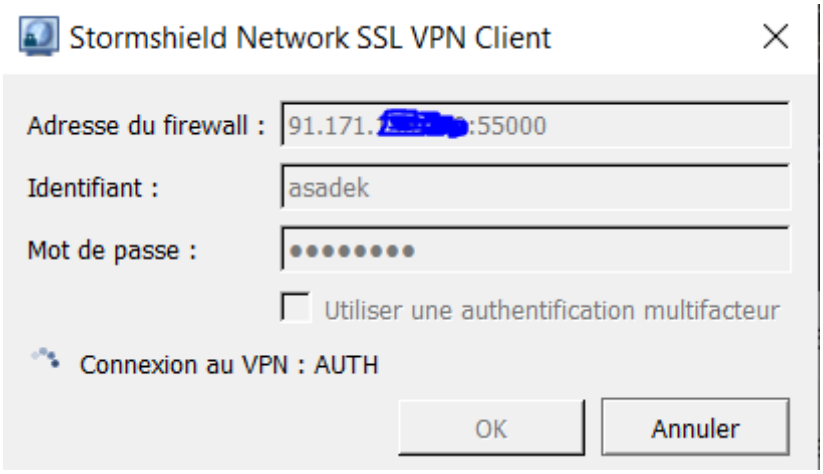


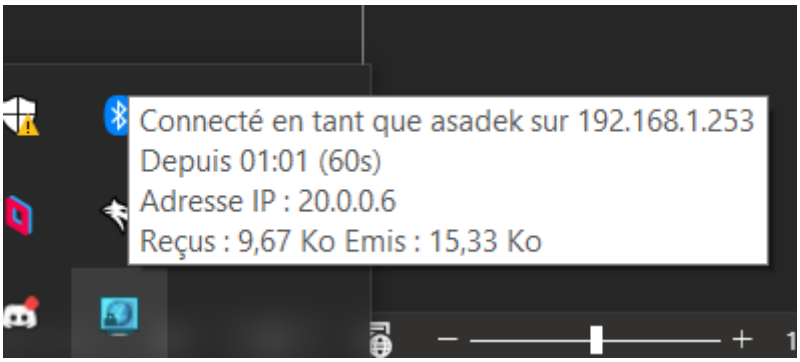
Test accès depuis IP publique

Je crée ma règle de PAT



Test


Stormshield Network SSL VPN Client
Adresse du firewall :
91.171.
:55000
Identifiant :
asadek
Mot de passe :
Utiliser une authentification multifacteur
Connexion au VPN : AUTH
OK
Annuler

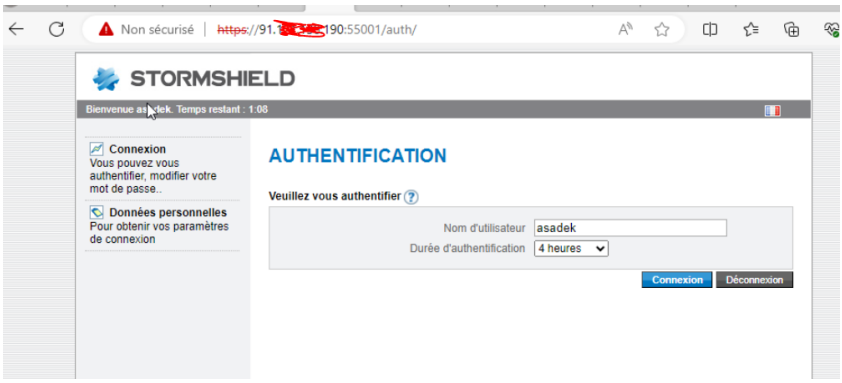

Connecté en tant que asadek sur 192.168.1.253
Depuis 01:01 (60s)
Adresse IP : 20.0.0.6
Reçus : 9,67 Ko Emis : 15,33 Ko

Résolution problème version TLS openvpn mode automatique

J'ai fait face à énormément de problème avec ce serveur openvpn car il est très ancien sa version de TLS est 1.0.

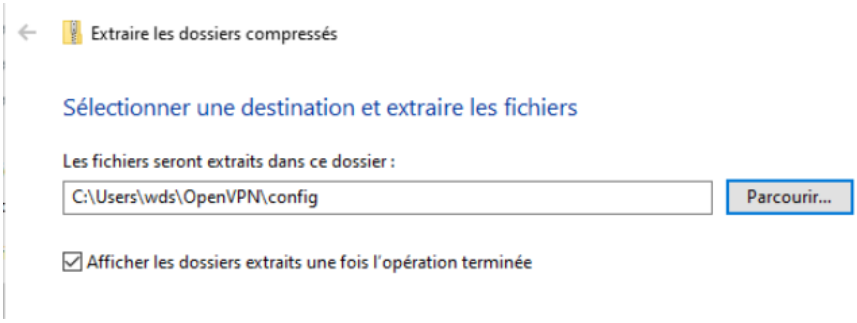
Le client stormshield récent bug beaucoup il faut donc utiliser le client openvpn GUI

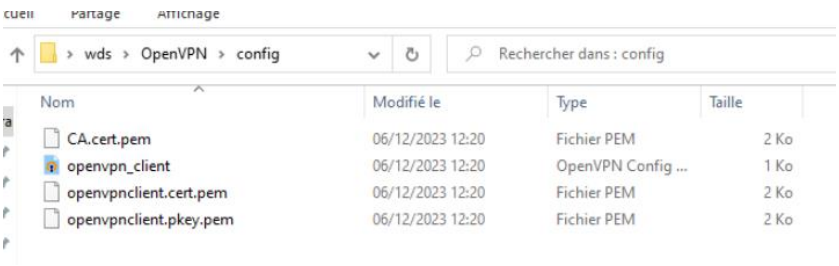
Déjà accéder à l'interface graphique du Firewall depuis l'extérieur et s'identifier



Il faut télécharger le fichier de config ici

Ensuite extraire l'archive ici > Dans le dossier openvpn de l'user





Ensuite ouvrir le fichier client dans un notepad

Remplacer ça (CAS REGLE DE PAT)

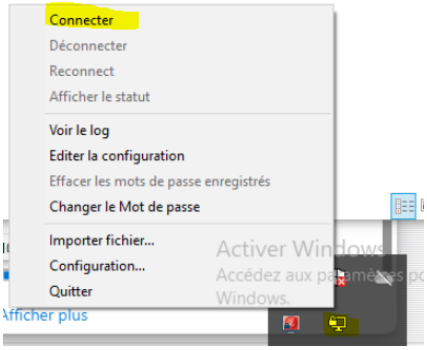
```
client
dev tun
proto tcp
remote 91.[redacted].190 443
```

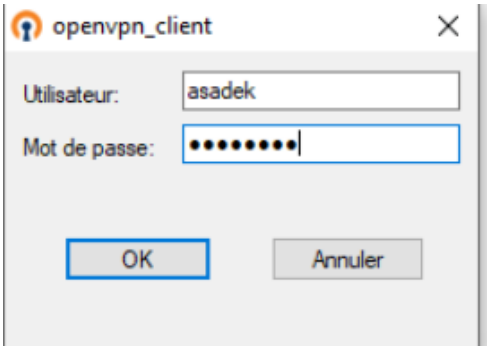
Par ça

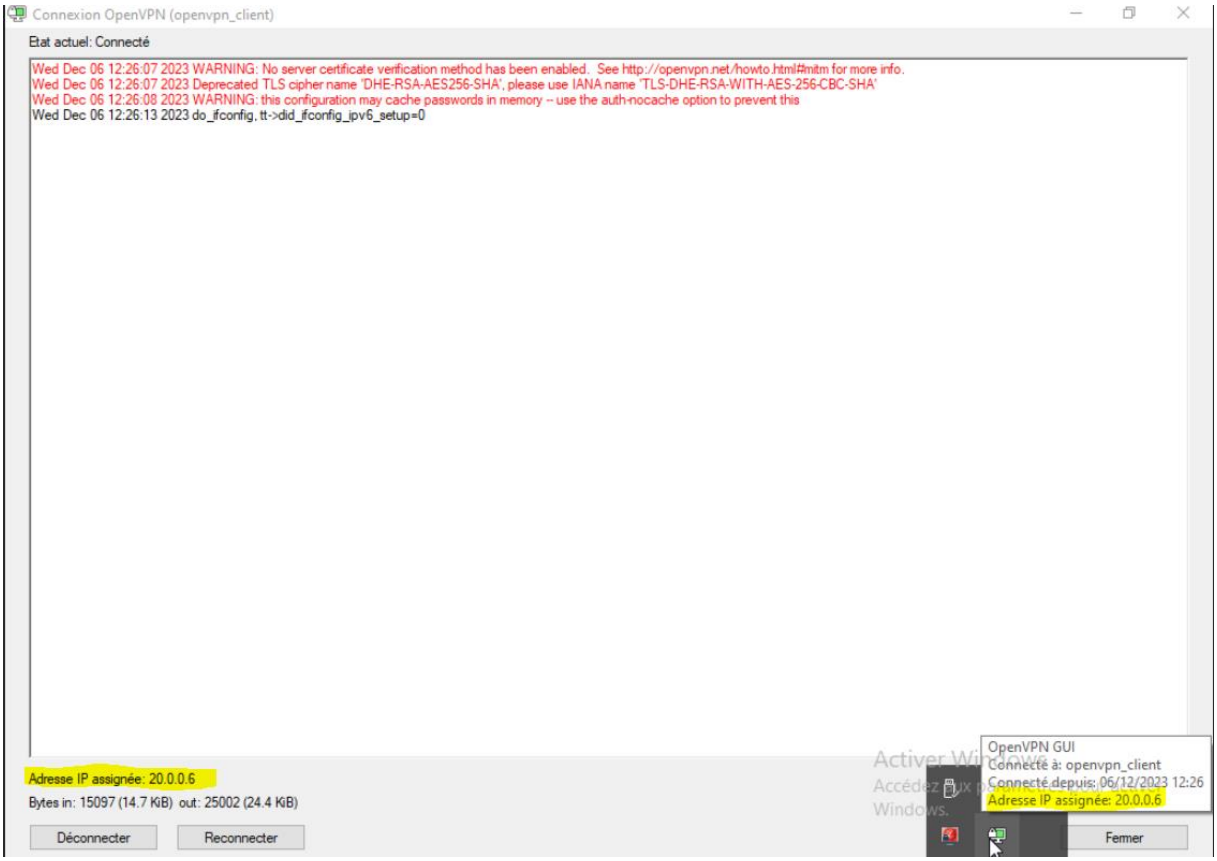
```
client
dev tun
proto tcp
remote 91.[redacted].190 55001
```

Car le fichier de base le firewall ne sait pas que derrière il y'a une règle de PAT qui redirige le port 55001 de ma box vers son port 443 c'est transparent pour lui donc il ne le prend pas en compte c'est pour cela il est impératif de modifier le port lorsqu'il y'a une règle de PAT et que le port DST sur tête de réseau est différent que firewall

Ensuite se connecter depuis le petit onglet openvpn, dans le cas ou il y’a plusieurs config choisir sa config et cliquer sur se connecter







On voit bien que la connexion a réussit il faut modifier fichier de conf et mettre verb à « 5 » si on veut plus de log pour debuger

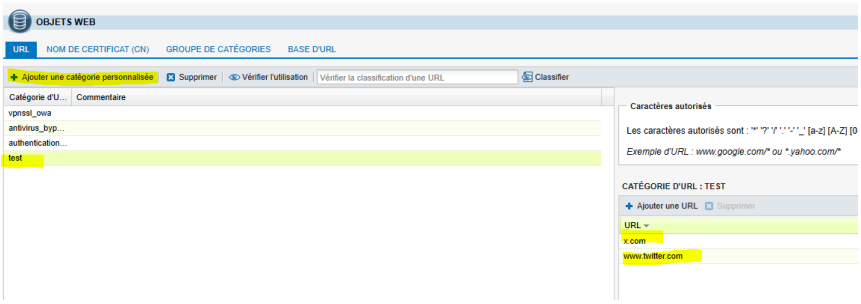
Très important

Comme c'est une ancienne version d'openvpn coté firewall il faut un ancien client openvpn qui accepte la version 1.0 de TLS car j'ai eu une erreur avec les nouvelles versions j'ai donc la version d'openvpn de 2018 coté client.

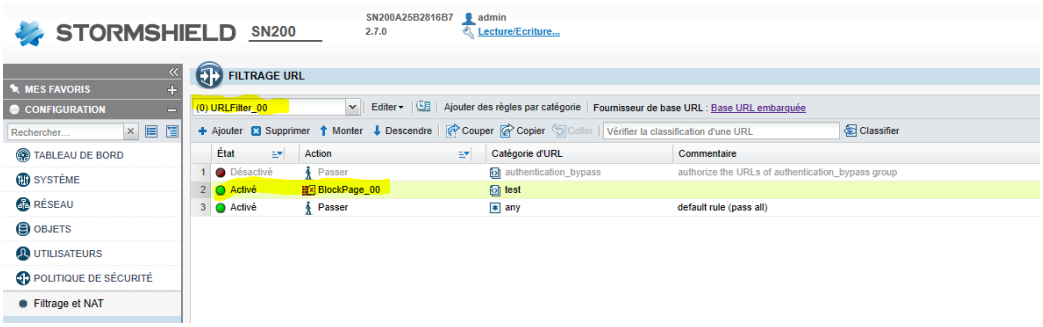
Filtrage URL

Pour mettre en place le filtrage URL il faut d'abord crée un objet web qui regroupe nos URLS

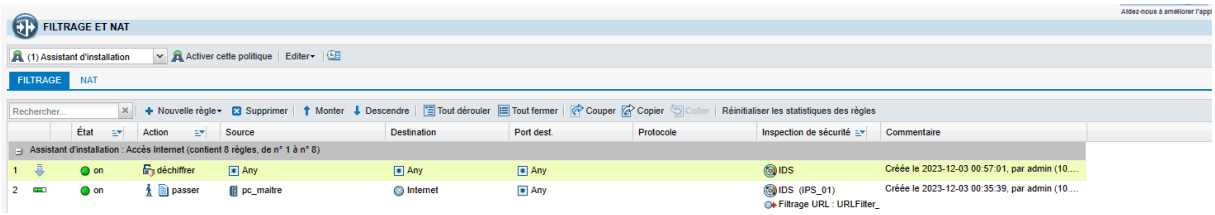
Configuration > Objets > Objets Web



Ensuite on se rend dans Configuration > Filtrage URL et on bloque ou passe le trafic



Ensuite il faut déchiffrer ce trafic avant de le filtrer donc créer une regle qui filtre



Sauf qu'il y'a un probleme de certificat comme c'est du filtrage transparent

La solution est de mettre en place le filtrage pour https parceque la c'est que pour du http ce qui est mis en place

Les différentes étapes du filtrage SSL sont les suivantes :

1. Le proxy SSL intercepte les connexions du client sur le port TCP/443.
2. Il effectue les négociations SSL avec le serveur web au nom du client.
3. Il analyse le certificat envoyé par le serveur. En cas de non conformité du certificat, l'accès au serveur est bloqué.
4. Si le certificat est conforme, le proxy SSL consulte les règles de filtrage SSL :
    - Bloquer sans déchiffrer : il bloque les connexions,
    - Passer sans déchiffrer : il laisse passer les connexions,
    - Déchiffrer : il déchiffre le flux qui est ensuite évalué par les règles de filtrage suivantes.
5. Si l'action est Déchiffrer, le proxy SSL génère un certificat usurpé (fake certificate) et le présente au client qui vérifie le certificat. Si le certificat de l'autorité signataire n'a pas été installé dans le navigateur ou dans le système et déclaré comme autorité de confiance, un message d'erreur s'affiche.
6. Si le certificat est présent, le trafic est sécurisé. Les protections applicatives sont appliquées (e.g., anti-virus, antispam, sandboxing).

NOTE
Les étapes 5 et 6 ont lieu uniquement si vous appliquez la méthode de filtrage AVEC déchiffrement des flux SSL.