

Table des matières

Introduction	3
Configuration interface out	5
Configuration interface IN	6
Dhcp et zone dns	6
Intégration AD	7
Configuration horaire	7
Configuration administration de l'équipement	8
Mise à jour	9
Enregistrement	9
Mises à jour des bases	11
DNAT serveur web et smtp	11
Filtrage URL	12
IPS/IDS	12
Application	13
Fin de l'installation	13
Accès à l'interface web	14
Règles de filtrage	15
Création objet pour DNS	16
Route par défaut	17
Création d'une règle	18
DNAT	21
Route Statique	23
Mise en place	24
Test depuis un client du réseau interne du Stormshield	25
Connexion annuaire LDAP (AD)	25
Mise en place VPN	28
Test accès depuis IP publique	30
Résolution problème version TLS openvpn mode automatique	32
Très important	35
Filtrage URL	36

Introduction

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

Login par défaut : Admin

Password par défaut : Sur l'étiquette derrière

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

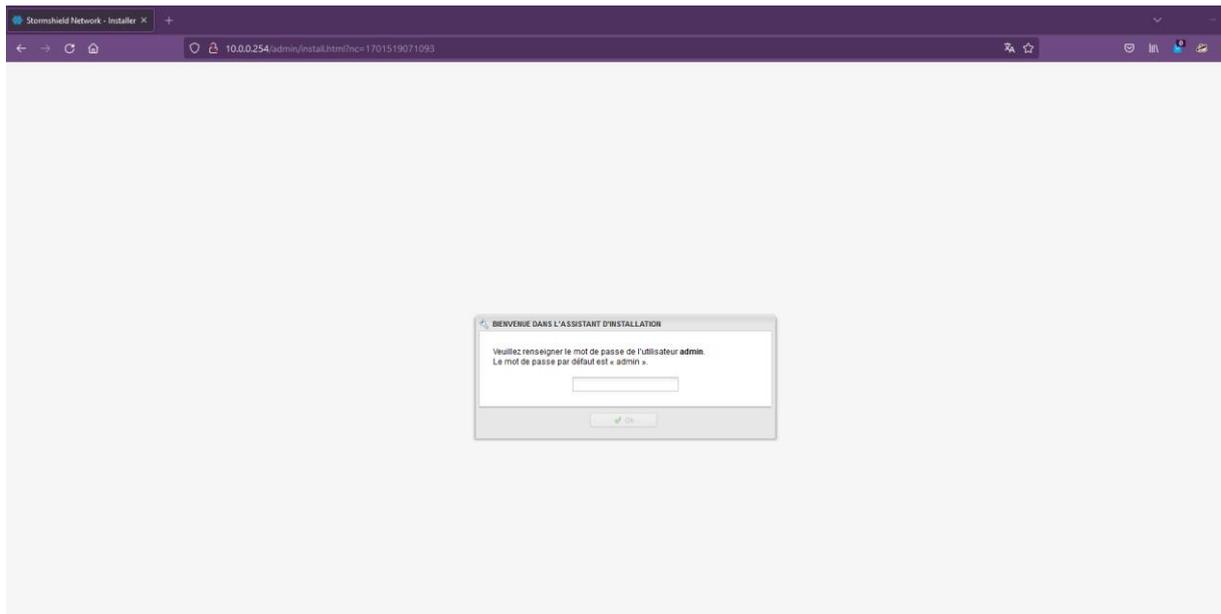
Une fois que j'ai réinitialisé l'ip est 10.0.0.254 /8 et le clavier est en qwerty

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

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

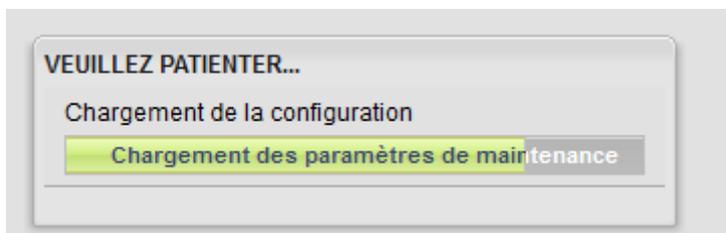
Ensuite remettre enfilter off, ouvrir un Wireshark et se connecter et aussi mettre un masque en /24 pas /8

Résultat

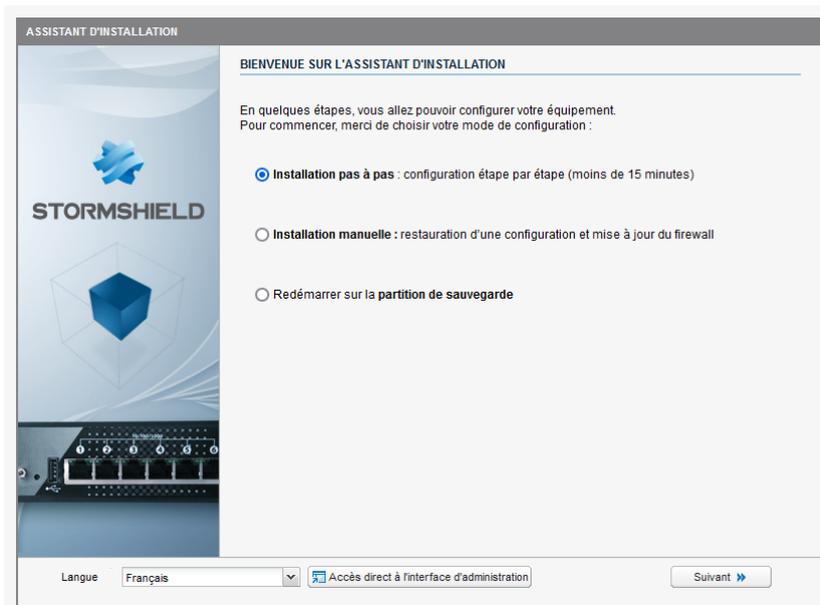


Renseigner le mdp qui est sur le boitier

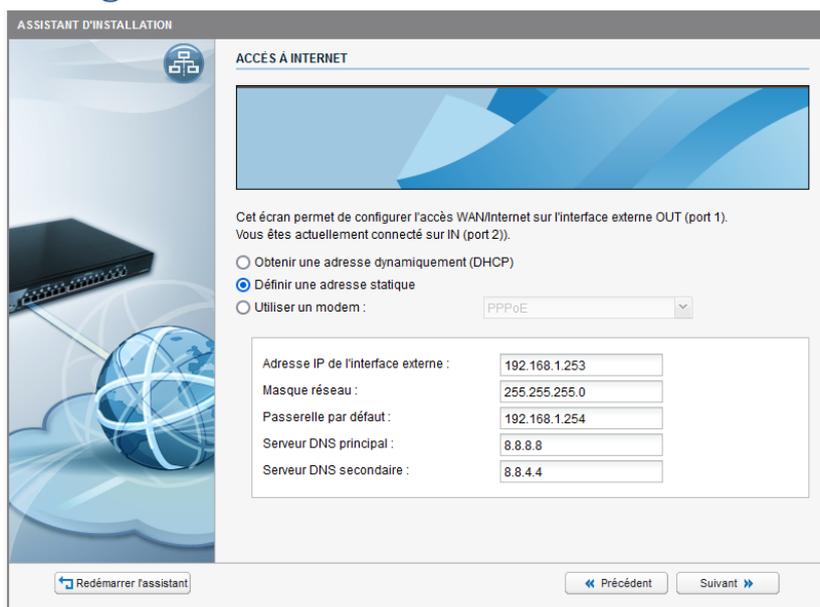
La configuration charge



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

ASSISTANT D'INSTALLATION

CONFIGURATION DU RÉSEAU INTERNE (LAN)

Cet écran permet de configurer le réseau interne de l'entreprise.

Le mode **transparent** crée un pont réseau (bridge) entre l'interface externe (port 1), configurée à l'étape précédente et toutes les interfaces internes (à partir du port 2).

Le mode **translaté** permet de définir un réseau interne, qui s'appliquera à toutes les interfaces à partir du port 2 (donc à l'exclusion de l'interface externe (port 1)).

Vous êtes actuellement connecté sur IN (port 2).

Identique au réseau WAN (mode transparent)
 Définir un réseau interne (mode translaté)

Adresse IP du Firewall :
Masque du réseau interne :

[Redémarrer l'assistant](#) [Précédent](#) [Suivant](#)

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

ASSISTANT D'INSTALLATION

SERVICES RÉSEAUX

Cette étape vous permet de renseigner le suffixe du domaine DNS et d'attribuer des adresses IP sur le réseau interne grâce au serveur DHCP.

Domaine DNS

Nom de domaine :

Attribution d'adresses IP (DHCP)

Activer le serveur DHCP

Première adresse IP disponible :
Dernière adresse IP disponible :

[Redémarrer l'assistant](#) [Précédent](#) [Suivant](#)

Intégration AD

Pour l'instant je ne l'intègre pas à un AD

ASSISTANT D'INSTALLATION

MICROSOFT ACTIVE DIRECTORY

Cette étape vous permet de définir votre serveur Microsoft Active Directory comme base d'utilisateurs. Vos utilisateurs pourront s'authentifier avec leur compte du domaine.

Vous pourrez également utiliser les comptes et groupes d'utilisateurs dans votre politique de sécurité.

Intégration avec un domaine Microsoft Active Directory

Paramètres de connexion

Nom du domaine :

Adresse IP du contrôleur de domaine :

Identifiant (DN) ? :

Mot de passe :

[Redémarrer l'assistant](#) [Précédent](#) [Suivant](#)

Configuration horaire

ASSISTANT D'INSTALLATION

PARAMÈTRES DU SYSTÈME

Vous pouvez personnaliser la langue et le fuseau horaire de votre équipement. La langue du firewall définit notamment les messages d'alarmes. La configuration du clavier définit la correspondance des touches pour les modes console et les accès ssh.

Langue

Langue du système :

Configuration du clavier :

Réglage de l'heure

Date :

Heure :

Synchroniser avec votre heure locale

Fuseau horaire :

[Redémarrer l'assistant](#) [Précédent](#) [Suivant](#)

Configuration administration de l'équipement

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

ADMINISTRATION DE L'ÉQUIPEMENT

Cette étape vous permet de définir le mot de passe de l'utilisateur 'admin'.
Vous pouvez également définir les différents accès d'administration.

Mot de passe de l'utilisateur admin

Mot de passe :

Confirmer :

Force du mot de passe: Excellent

Accès d'administration Web

L'objet **network_internals** regroupe tous les réseaux internes.
Seules les adresses définies ci-dessous pourront accéder à l'administration Web.

+ Ajouter x Supprimer

Adresse IP ou réseau (W.X.Y.Z/A.B.C.D)

10.0.0.0/8	^
10.0.0.0/24	v

Accès SSH

Autoriser l'accès SSH pour l'utilisateur admin (accès par mot de passe)

Je définis un mdp et j'active ssh

Accès d'administration Web

L'objet **network_internals** regroupe tous les réseaux internes.
Seules les adresses définies ci-dessous pourront accéder à l'administration Web.

+ Ajouter x Supprimer

Adresse IP ou réseau (W.X.Y.Z/A.B.C.D)

192.168.1.0/24	^
network_internals	v

Mise à jour

ASSISTANT D'INSTALLATION

MISE À JOUR DES PARAMÈTRES RÉSEAUX

Lors de cette étape, la configuration réseau sera mise à jour.

Branchez le modem ou le routeur de votre opérateur Internet sur l'interface EXTERNE (OUT). Les autres ports réseaux seront considérés comme les réseaux internes de l'entreprise.

Une fois la mise à jour effectuée, vous pouvez décider de :

- Poursuivre la configuration immédiatement
- Arrêter l'équipement



Redémarrer l'assistant << Précédent ■ Appliquer puis arrêter l'équipement ↓ Appliquer et continuer l'assistant

VEUILLEZ PATIENTER...

Enregistrement de la configuration...

Configuration du DHCP...

Enregistrement

ENREGISTREMENT

Produit

Numéro de série :

Partenaire :

Mot de passe d'enregistrement (WEB) ? :

Nouveau client

Client existant

Société (utilisateur final)

Nom : Téléphone :

Ville : Code postal :

Pays :

Adresse :

Contact (utilisateur final)

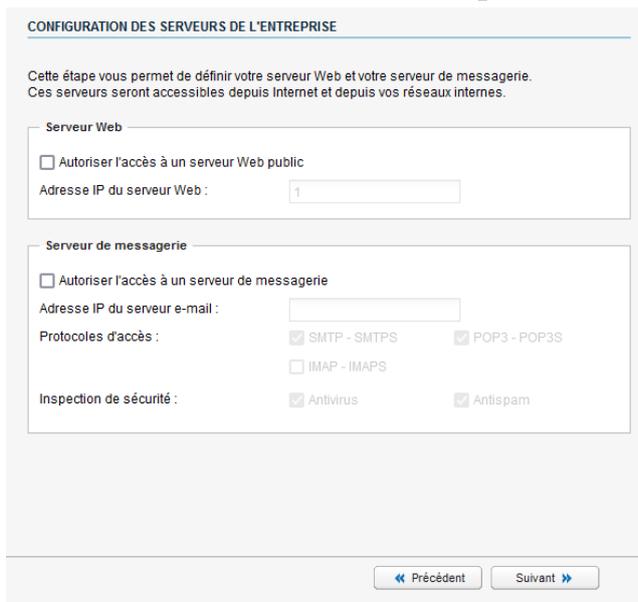
Nom : Prénom :

E-mail :

Mises à jour des bases



DNAT serveur web et smtp



Filtrage URL

ACCÈS INTERNET

Cette étape vous permet de définir la politique d'accès à Internet et à la messagerie instantanée depuis votre réseau interne.

Autoriser l'accès à Internet et filtrer en fonctions des catégories suivantes

CATÉGORIES DE SITES WEB

Tout autoriser Tout bloquer Inverser passer/bloquer

 passer	Unknown
 passer	Advertisements & Pop-Ups
 passer	Alcohol & Tobacco
 passer	Anonymizers
 passer	Arts
 passer	Business
 passer	Transportation
 passer	Chat
 passer	Forums & Newsgroups

Activer la protection antivirale pour l'accès au Web

Autoriser l'utilisation des logiciels de messagerie instantanée (IM)

[<< Précédent](#) [Suivant >>](#)

IPS/IDS

INSPECTION DU TRAFIC

Cette étape vous permet de définir le niveau d'inspection du trafic. Vous pouvez également activer la détection des vulnérabilités si vous avez souscrit à cette option.

Inspection du trafic

IPS (Détecter et bloquer)

IDS (Détecter)

Firewall (Ne pas inspecter)

Management des vulnérabilités

Détecter les vulnérabilités sur le réseau interne

[<< Précédent](#) [Suivant >>](#)

Application

APPLIQUER LA CONFIGURATION DE LA POLITIQUE DE SÉCURITÉ.

Merci de patienter pendant le transfert des paramètres de votre politique de sécurité.

- Création du serveur Web ✓
- Création des autres règles de la politique ✓
- Autorisation de la messagerie instantanée ✗

« Précédent Suivant »

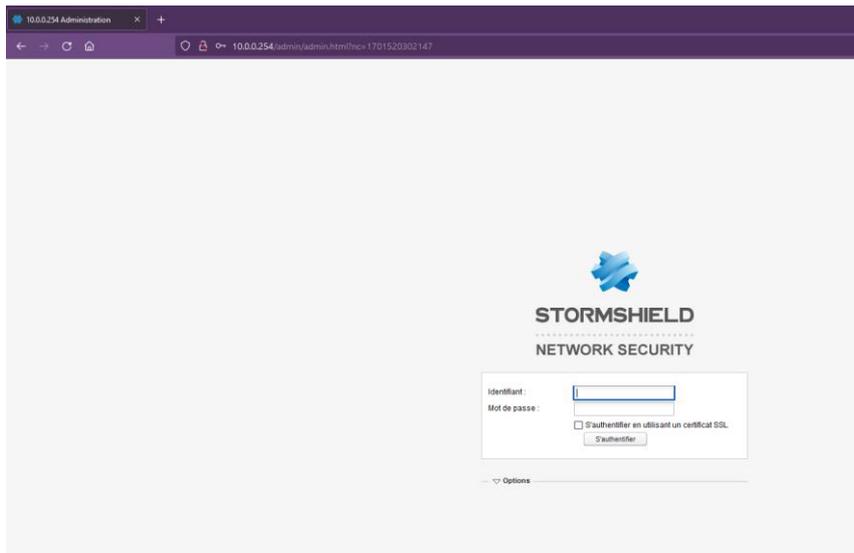
Fin de l'installation

FIN DE L'ASSISTANT

Félicitations, la configuration initiale de votre firewall est terminée.
Vous pouvez maintenant utiliser l'interface d'administration Web.

 Connexion à l'interface de configuration Web

Me voila connecter à l'interface web



Accès à l'interface web

ALARMES

Date	Action	Priorité	Source	Destination	Message
31/01/2005 11:40:21		Mineur			Connexion terminée pour webadmin (timeout)
31/01/2005 11:38:49	Bloquer	Mineur	10.0.0.2	94.75.236.122	Sonde de port
31/01/2005 11:38:41	Bloquer	Mineur	10.0.0.2	94.75.236.122	Sonde de port
31/01/2005 11:38:34	Bloquer	Mineur	10.0.0.2	94.75.236.122	Sonde de port
31/01/2005 11:38:28	Bloquer	Mineur	10.0.0.2	130.117.190.139	Sonde de port

PROPRIÉTÉS

Propriétés
 Numéro de série : SN200A238281687
 Date : 31/01/2005 11:42:22 GMT+00:00
 Version de la partition de secours : 1.5.0
 Date de la partition de secours : 06/06/2017 13:03:45
 Durée de fonctionnement (uptime) : 0j 1h 6m 39s
 Rapports d'activités : Génération de rapports désactivée
 Sauvegarde automatique : Dernière sauvegarde : Aucune sauvegarde disponible

RESSOURCES

CPU: 6% | Température: 41° | Mémoire: 15%

MATERIEL

Matériel
 Clé USB: Non détecté
 Carte SD: Non détecté
 Modem 3G: Non détecté

HAUTE DISPONIBILITÉ

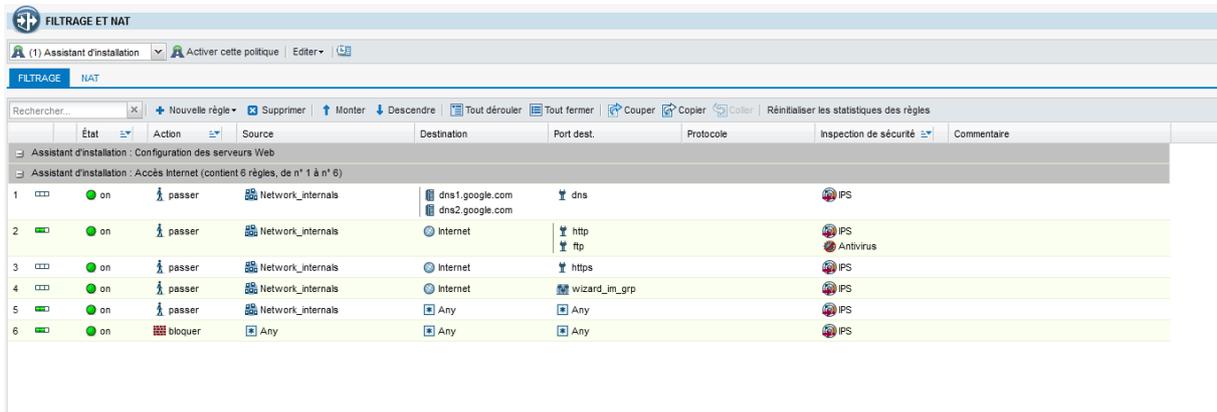
Haute Disponibilité
 La haute disponibilité n'est pas supportée.

ACTIVE UPDATE

Item	État	Dernière mise à jour
Antispam listes noires DNS (DBL)	Échec	
IPS : signatures de protection	Échec	
Antispam : moteur heuristique	Échec	
Management des vulnérabilités	Échec	
Antivirus : signatures antivirus Kaspersky	À jour	31/01/2005 11:41:29
Autorité de certification racines	Jamais utilisé	

Règles de filtrage

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



The screenshot shows the Mikrotik Firewall Rule configuration interface. The title is "FILTRAGE ET NAT". Below the title, there are tabs for "FILTRAGE" and "NAT". The main area displays a list of rules under the "Assistant d'installation : Accès Internet (contient 6 règles, de n° 1 à n° 6)" section. The rules are as follows:

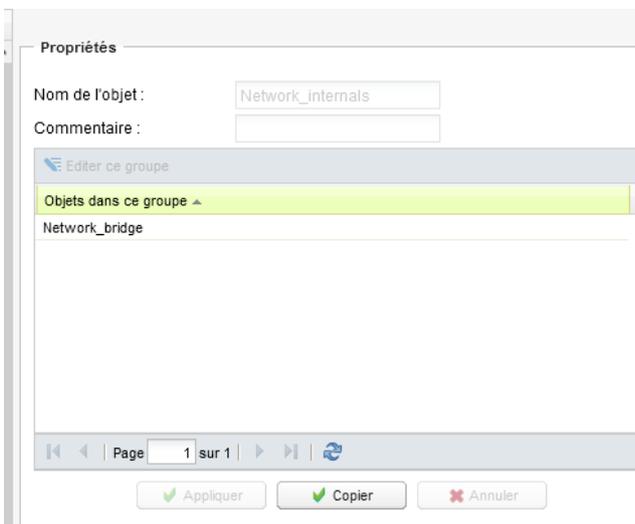
État	Action	Source	Destination	Port dest.	Protocole	Inspection de sécurité	Commentaire
1	on	passer	Network_internals	dns1.google.com dns2.google.com	dns	IPS	
2	on	passer	Network_internals	Internet	http ftp	IPS Antivirus	
3	on	passer	Network_internals	Internet	https	IPS	
4	on	passer	Network_internals	Internet	wizard_in_grp	IPS	
5	on	passer	Network_internals	Any	Any	IPS	
6	on	bloquer	Any	Any	Any	IPS	

Network internal est un objet qui contient l'objet Network_Bridge



The screenshot shows the Mikrotik Object configuration interface. It displays two objects:

Network_bridge	10.0.0.0/255.255.255.0
Network_internals	



The screenshot shows the Mikrotik Object Properties configuration interface. The "Propriétés" section is active, showing the following fields:

- Nom de l'objet: Network_internals
- Commentaire: (empty)

Below the fields, there is a button "Editer ce groupe" and a section "Objets dans ce groupe" containing the object "Network_bridge". At the bottom, there are navigation and action buttons: "Page 1 sur 1", "Appliquer", "Copier", and "Annuler".

Propriétés

Nom de l'objet :

Adresse IPv4

Adresse IP de réseau :

Exemple 192.168.0.0/16 ou 192.168.0.0/255.255.0.0

Commentaire :

Création objet pour DNS

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

Je crée donc un objet pihole

Créer un objet

Machine Réseau Plage d'adresses IP Port Protocole IP Groupe Groupe de ports Routeur

Nom de l'objet : 🔍

Adresse IPv4 :

Résolution

Aucune (IP statique) Automatique

Adresse MAC :

Commentaire :

DHCP

Général

Activer le service

serveur DHCP
 relai DHCP

Paramètres par défaut

Nom de domaine :

Passerelle :

DNS primaire :

DNS secondaire :

PLAGE D'ADRESSES

Route par défaut

Dans réseau > routage

Je peux voir que la passerelle par défaut est un objet

ROUTAGE

ROUTES STATIQUES | ROUTAGE DYNAMIQUE | ROUTES DE RETOUR

Passerelle par défaut (routeur) :

ROUTES STATIQUES

Rechercher... |

État	Réseau de destination (objet machine, réseau ou groupe)...	Plan d'adressage	Interface
------	--	------------------	-----------

Propriétés

Nom de l'objet :

Adresse IPv4 :

Résolution

Aucune (IP statique) Automatique

Adresse MAC :

Commentaire :

Création d'une règle

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

Edition de la règle n° 5

Général
Action
Source
Destination
Port / Protocole
Inspection

ACTION

GÉNÉRAL QUALITÉ DE SERVICE CONFIGURATION AVANCÉE

Général

Action : passer

Niveau de trace : tracer

Programmation horaire : None

Routage

Passerelle - routeur : None

Ok Annuler

Général
Action
Source
Destination
Port / Protocole
Inspection

SOURCE

GÉNÉRAL CONFIGURATION AVANCÉE

Général

Utilisateur: Rechercher...

Machines sources: Network_internals

Interface d'entrée : in

Général
Action
Source
Destination
Port / Protocole
Inspection

DESTINATION

GÉNÉRAL CONFIGURATION AVANCÉE

Général

Machines destinations: Any

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

Créer un objet

Machine Réseau Plage d'adresses IP **Port** Protocole IP Groupe Groupe de ports Routeur

Nom de l'objet :

Port

Port :

Plage de ports

Depuis :

Jusqu'à :

TCP/UDP :

Commentaire :

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

Général
Action
Source
Destination
Port / Protocole
Inspection

PORT ET PROTOCOLE

Port

Port destination:

Protocole

Type de protocole :

Protocole applicatif :

Protocole IP : tcp

Général
Action
Source
Destination
Port / Protocole
Inspection

INSPECTION DE SÉCURITÉ

Général

Niveau d'inspection :

Profil d'inspection :

Inspection applicative

Antivirus :

Antispam :

Filtrage URL :

Filtrage SMTP :

Filtrage FTP :

Filtrage SSL :

Avant activation de la règle

```
C:\Users\PC>ssh root@192.168.1.22
```

Après activation de la règle

```
C:\Users\PC>ssh root@192.168.1.22  
root@192.168.1.22's password:
```

DNAT

On va voir comment mettre en place une règle de DNAT

Politique de sécurité > Filtrage et Nat > NAT

Ensuite je crée une règle

- Général
- Source originale
- Destination originale
- Source tradatée
- Destination tradatée
- Options

SOURCE AVANT TRANSLATION (ORIGINALE)

GÉNÉRAL CONFIGURATION AVANCÉE

Général

Utilisateur:

Machines sources:

Interface d'entrée :

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

DESTINATION AVANT TRANSLATION (ORIGINALE)

GÉNÉRAL CONFIGURATION AVANCÉE

Général

Machines destinations: Firewall_out

Port destination: http

Ensuite je définis vers qui sera transférer 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

SOURCE APRÈS TRANSLATION

GÉNÉRAL CONFIGURATION AVANCÉE

Général

Machine source tradatée : Any

Port source tradaté : None

choisir aléatoirement le port source tradaté

Ok Annuler

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

DESTINATION APRÈS TRANSLATION

GÉNÉRAL CONFIGURATION AVANCÉE

Général

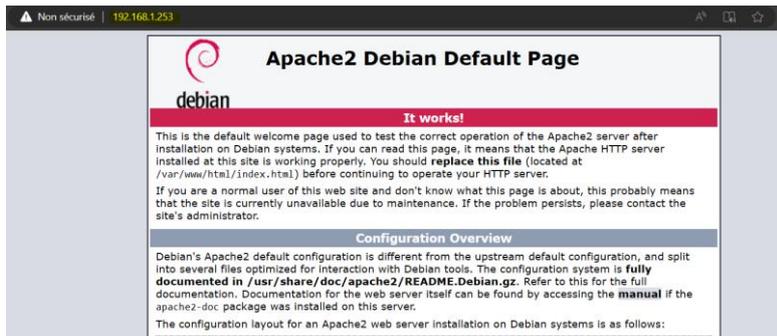
Machine destination tradatée : ip_srv_web_01

Port destination tradaté : http

Ok Annuler

Trafic original (avant translation)				Trafic après translation				Options	Commentaire	
	État	Source	Destination	Port dest.	Source	Port src.	Destination	Port dest.		
1	on	Network_internals	Internet interface: out	Any	Firewall_out	ephemeral_fw	Internet		tracer	
2	on	Internet interface: out	Firewall_out	http	Any		ip_snr_web_0	http		Créée le 2023-12-02 14:47:18, par admin (10...

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'accéder au réseau 172.16.0.254 (auquel il est relié 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

Créer un objet

Machine Réseau Plage d'adresses IP Port Protocole IP Groupe Groupe de ports Routeur

Nom de l'objet : reseau_distant

Adresse IPv4

Adresse IP de réseau : 172.16.0.0/24

Exemple 192.168.0.0/16 ou 192.168.0.0/255.255.0.0

Commentaire : lien vers réseau derriere 19

Routeur_1 = 192.168.1.22

ROUTES STATIQUES ROUTAGE DYNAMIQUE ROUTES DE RETOUR

Passerelle par défaut (routeur) : wizard_gateway

ROUTES STATIQUES

Rechercher... Ajouter Supprimer

État	Réseau de destination (objet machine, réseau ou groupe)	Plan d'adressage	Interface	Protégée	Passerelle	Couleur	Commentaire
Activé	reseau_distant	172.16.0.0/24	out		routeur_1		

Je n'ometts 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 soit 172.16.0.254

```
SN200A25B2816B7>ping 172.16.0.254
PING 172.16.0.254 (172.16.0.254): 56 data bytes
64 bytes from 172.16.0.254: icmp_seq=0 ttl=63 time=90.460 ms
64 bytes from 172.16.0.254: icmp_seq=1 ttl=63 time=89.023 ms
64 bytes from 172.16.0.254: icmp_seq=2 ttl=63 time=90.027 ms
64 bytes from 172.16.0.254: icmp_seq=3 ttl=63 time=89.028 ms
```

Test depuis un client du réseau interne du Stormshield

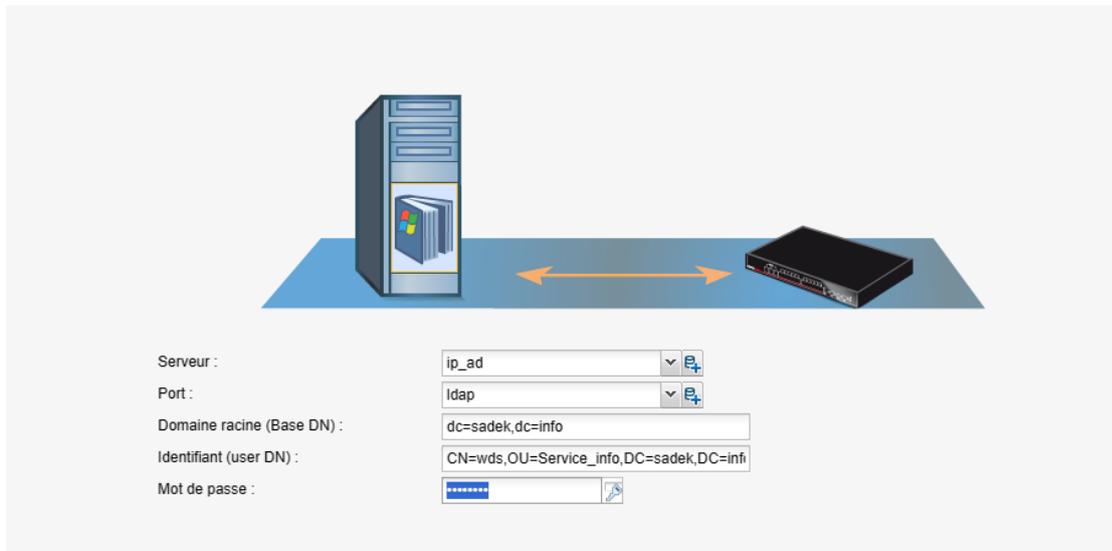
```
C:\Users\PC>ping 172.16.0.254
Envoi d'une requête 'Ping' 172.16.0.254 avec 32 octets de données :
Réponse de 172.16.0.254 : octets=32 temps=97 ms TTL=63
Réponse de 172.16.0.254 : octets=32 temps=93 ms TTL=63
Réponse de 172.16.0.254 : octets=32 temps=92 ms TTL=63
```

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

CONFIGURATION DE L'ANNUAIRE

ANNUAIRE EXTERNE STRUCTURE

Activer l'utilisation de l'annuaire utilisateur

Annuaire distant

Serveur :  

Port :  

Domaine racine (Base Dn) :

Identifiant :

Mot de passe : 

— Connexion sécurisée (SSL)

— Configuration avancée

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

UTILISATEURS

x  Filtre : Tous + Ajouter un utilisateur + Ajouter un groupe x Supprimer 

Cn ▲

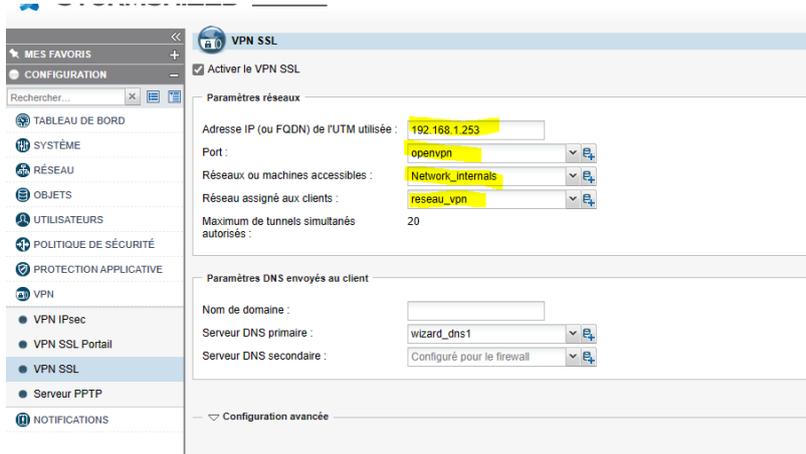
- ADMIN-PFSENSE
- ADSADEK
- Accès DCOM service de certificats
- Accès compatible pré-Windows 2000
- Adei AS. Sadek
- Administrateur
- Administrateurs Hyper-V
- Administrateurs clés Enterprise
- Administrateurs clés
- Administrateurs de l'entreprise
- Administrateurs du schéma
- Administrateurs
- Admins du domaine
- Compliance Management
- Contrôleurs de domaine clonables
- Contrôleurs de domaine d'entreprise en lectur...
- Contrôleurs de domaine en lecture seule
- Contrôleurs de domaine

Utilisateurs et groupes

Choisissez un élément de la liste pour en afficher les détails.

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 dernière (**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

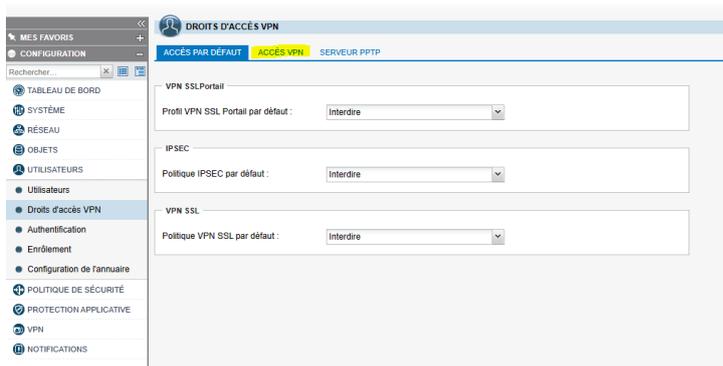
Je crée aussi un objet qui contient le réseau ou mes clients seront dedans.

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'utilisateur à utiliser le vpn

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



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

```

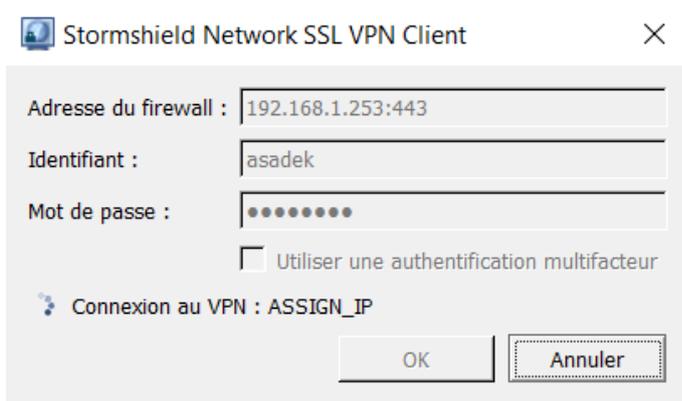
openvpn_client.log - Bloc-notes
Fichier Edition Format Affichage Aide
2023-12-04 00:32:25 Outgoing Data Channel: Using 160 bit message hash 'SHA1' for HMAC authentication
2023-12-04 00:32:25 Incoming Data Channel: Cipher 'AES-128-CBC' initialized with 128 bit key
2023-12-04 00:32:25 Incoming Data Channel: 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-8BE80A6502E2}
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.
Server:      UnKnown
Address: 8.8.8.8
```



Stormshield Network SSL VPN Client

Adresse du firewall : 192.168.1.253:443

Identifiant : asadek

Mot de passe : ●●●●●●

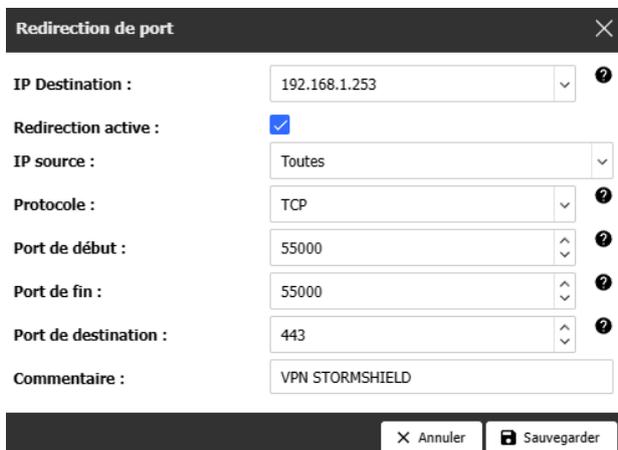
Utiliser une authentification multifacteur

Connexion au VPN : ASSIGN_IP

OK Annuler

Test accès depuis IP publique

Je crée ma règle de PAT



Redirection de port

IP Destination : 192.168.1.253

Redirection active :

IP source : Toutes

Protocole : TCP

Port de début : 55000

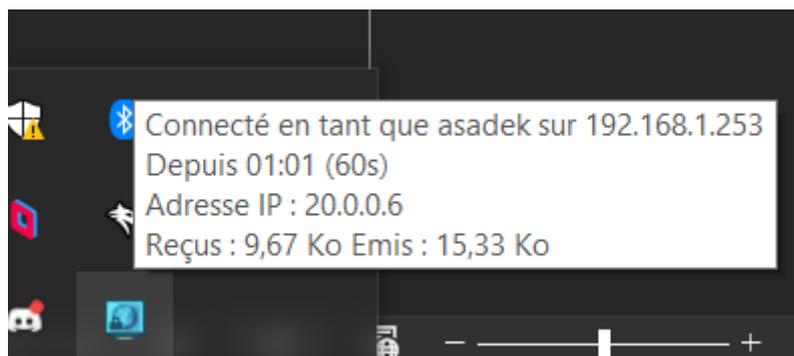
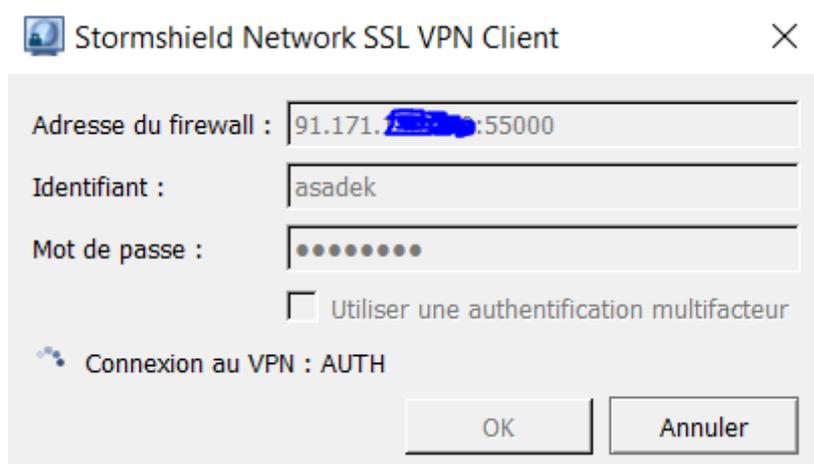
Port de fin : 55000

Port de destination : 443

Commentaire : VPN STORMSHIELD

Annuler Sauvegarder

Test

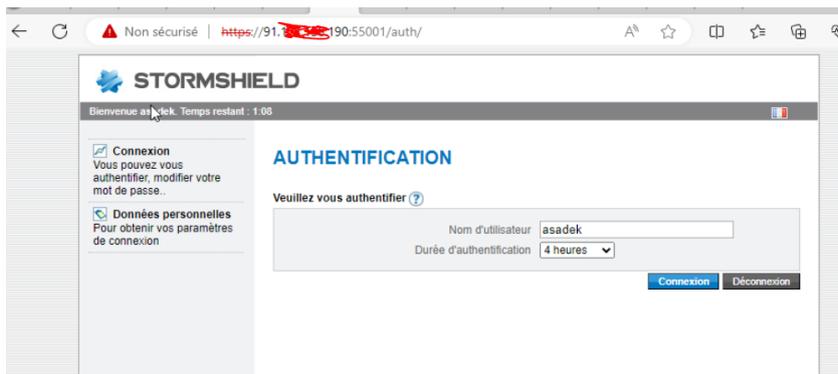


Résolution problème version TLS openvpn mode automatique

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

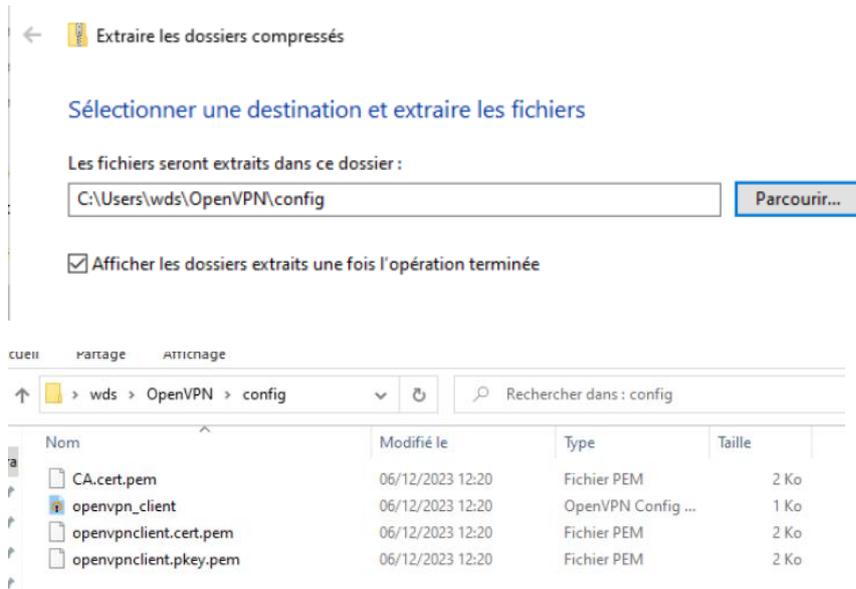
Le client stormshield récent bug beaucoup il faut donc utiliser le client openvpn GUI

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)

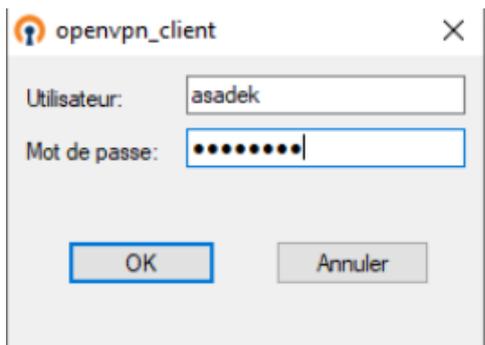
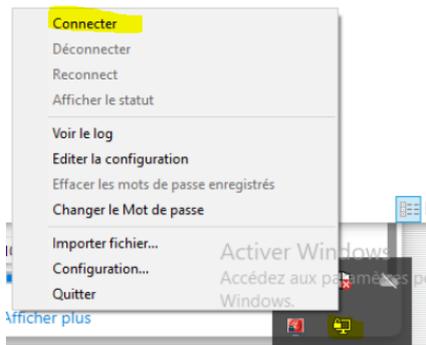
```
client
dev tun
proto tcp
remote 91.192.168.190 443
```

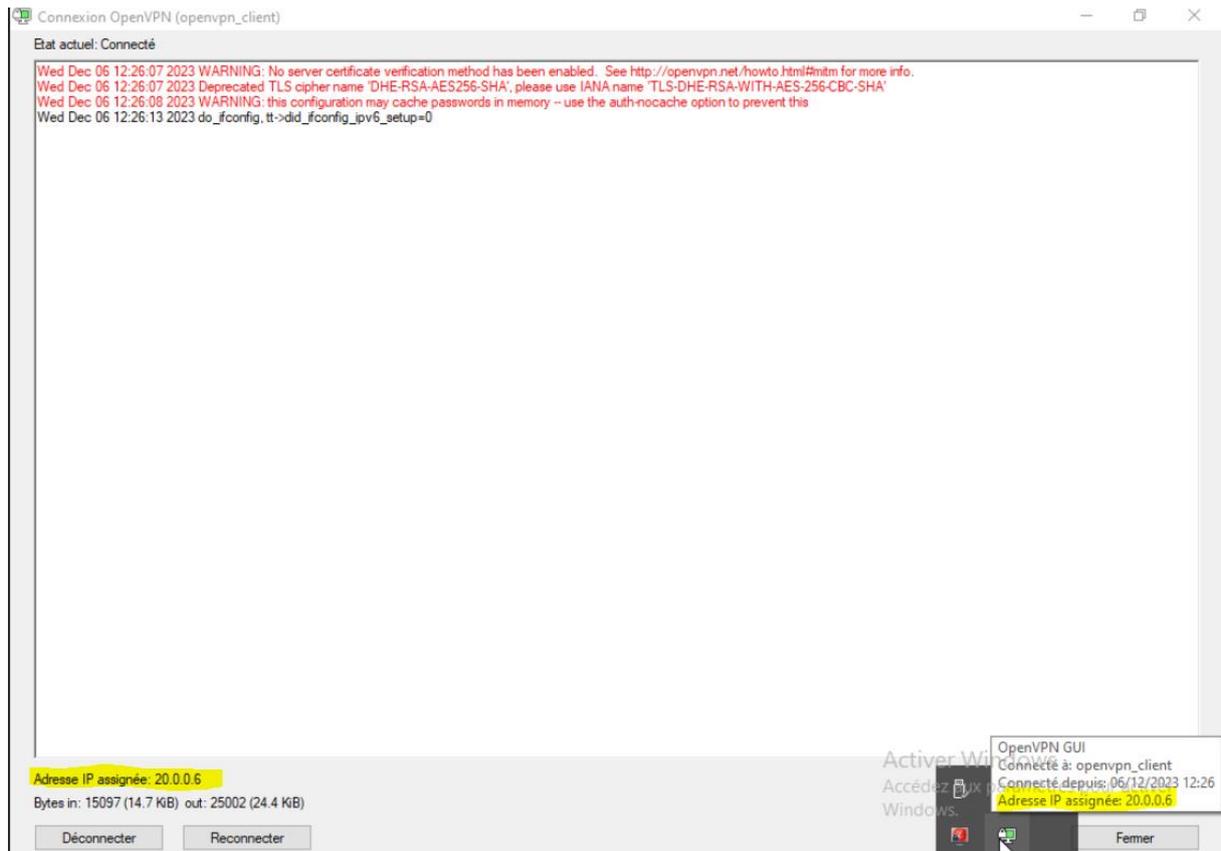
Par ça

```
client
dev tun
proto tcp
remote 91.192.168.190 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 réussi il faut modifier fichier de conf et mettre verb à « 5 » si on veut plus de log pour debugger

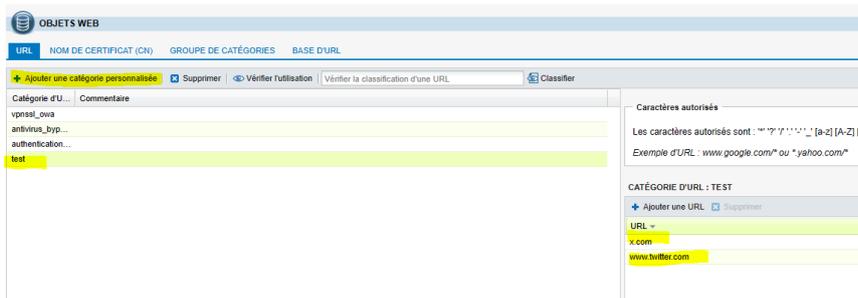
Très important

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.

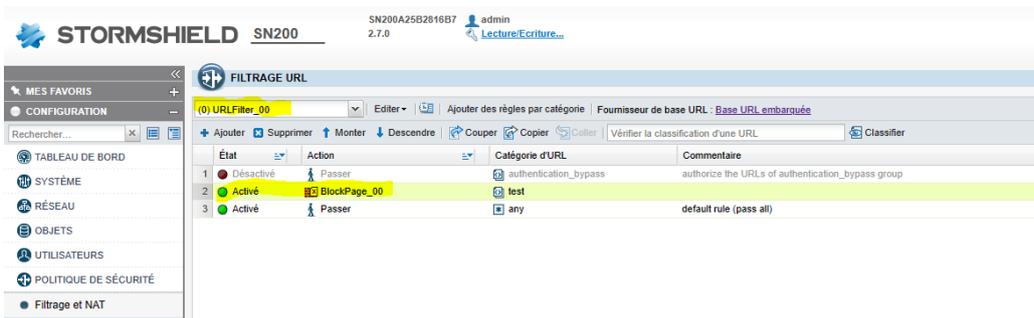
Filtrage URL

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

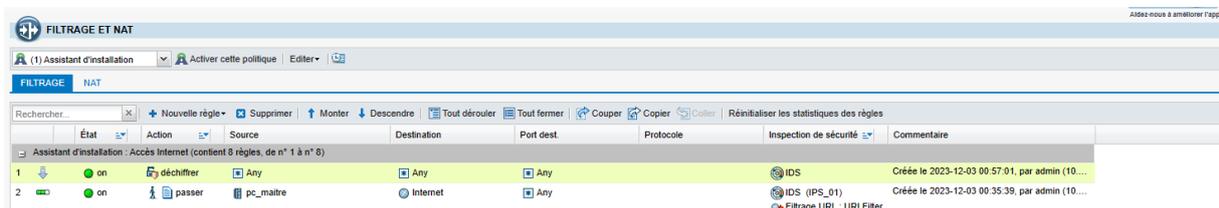
Configuration > Objets > Objets Web



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 règle 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](#).

