Projet Stormshield



08/02/2023

Malgouyres Thomas et Delissen Léa

Mairie de Lillers - Service informatique

Chemin des hallots

62190 Lillers

# Vue d'ensemble

Le projet consiste à adapter un pare-feu Stormshield sn 300 afin de pouvoir l’installer sur un réseau déjà existant.

# Objectifs

Le premier objectif serait installé et d’adapter le pare-feu au réseau et le deuxième serait de bloquer deux sites demandés : YouTube, Facebook.

# Caractéristiques

……

# Grandes étapes

## Installation du pare-feu

Installation du pare-feu sur le réseau.

## Administration du pare-feu

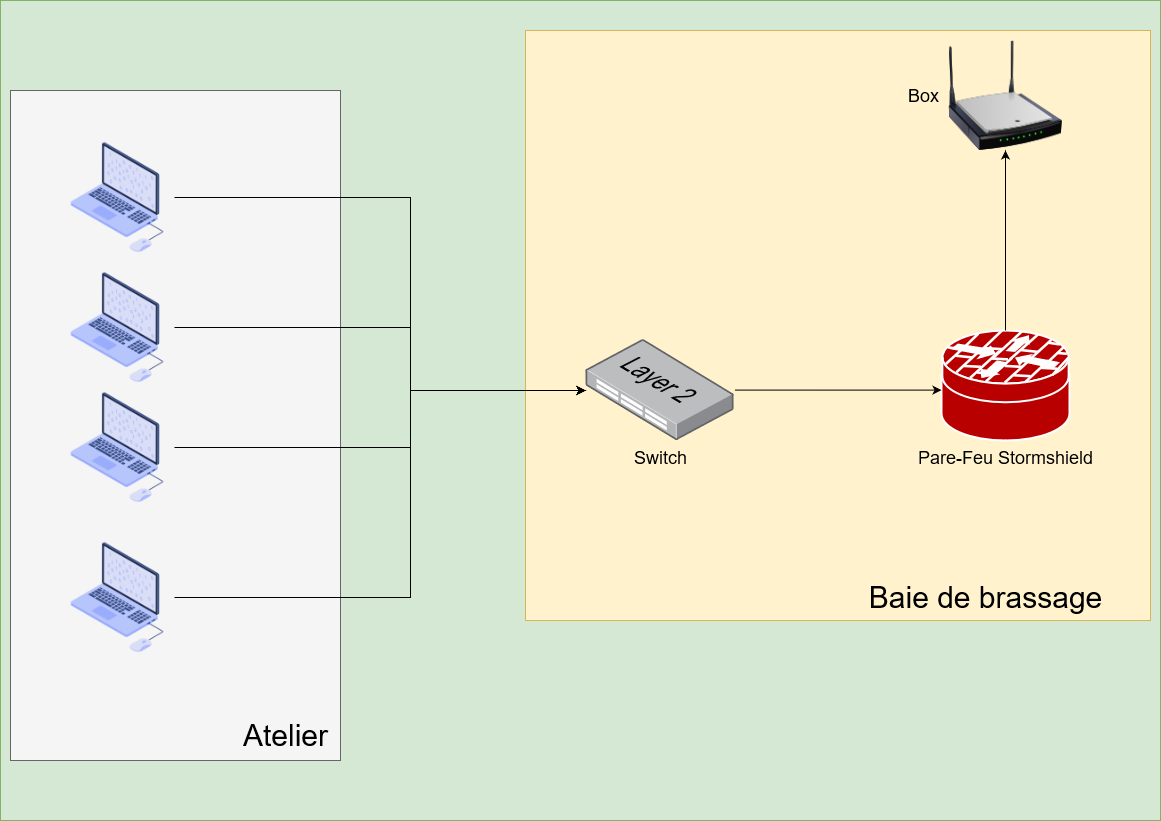
Administration du pare-feu afin qu’il puisse se placer dans le réseau.

## Blocage des sites demander

On va bloquer les sites YouTube et Facebook

# 1. Installation du pare-feu.

Pour correspondre au réseau le pare-feu va être installer entre la box et le switch.



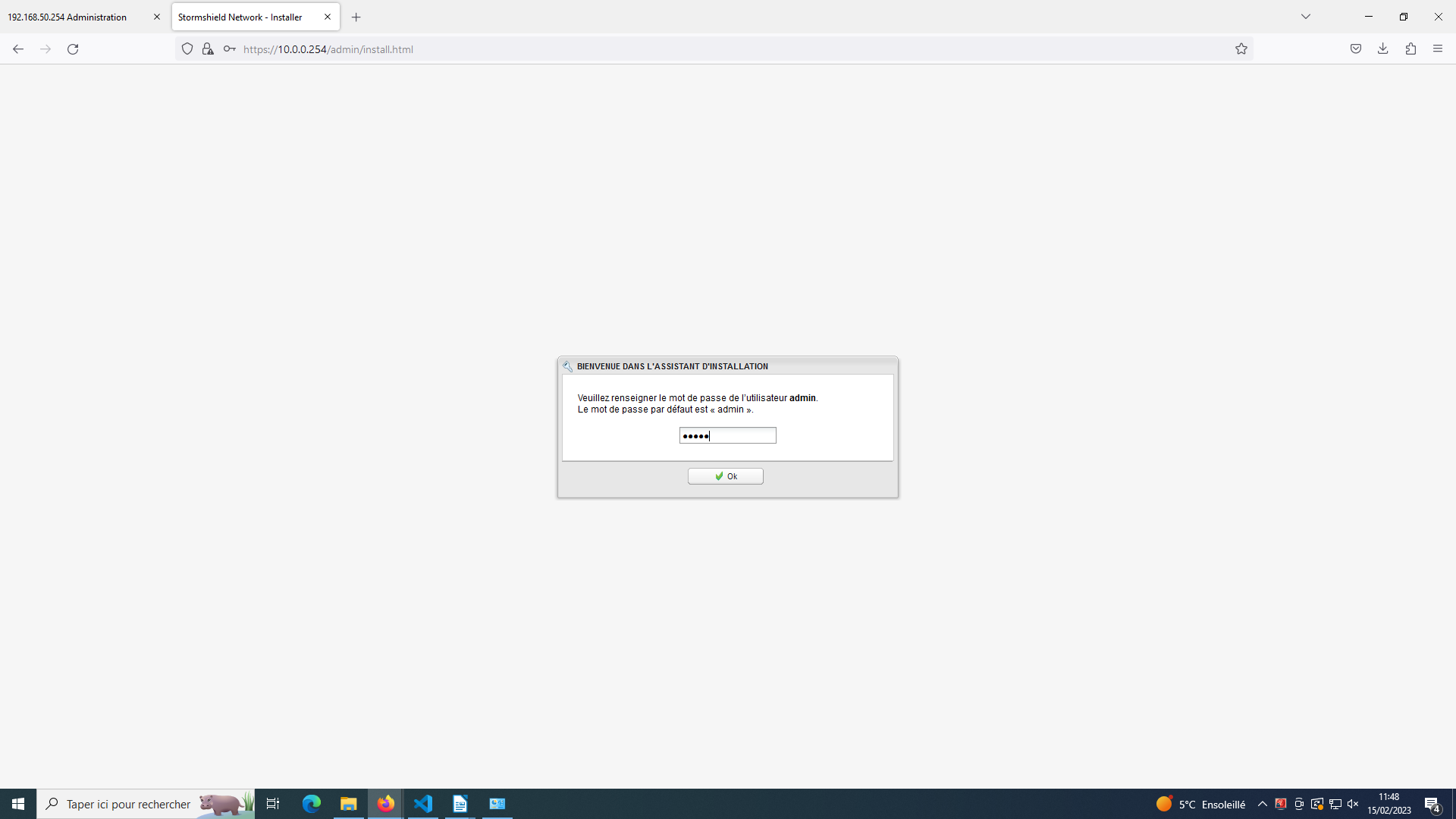
Sur le Pare-Feu les systèmes sont branchés de cette façon :

|  |  |
| --- | --- |
| Système | Port |
| Box | 1 |
| Switch | 2 |
| (Vide) | 3 |
| (Vide) | 4 |
| (Vide) | 5 |
| (Vide) | 6 |
| (Vide) | 7 |
| (Vide) | 8 |

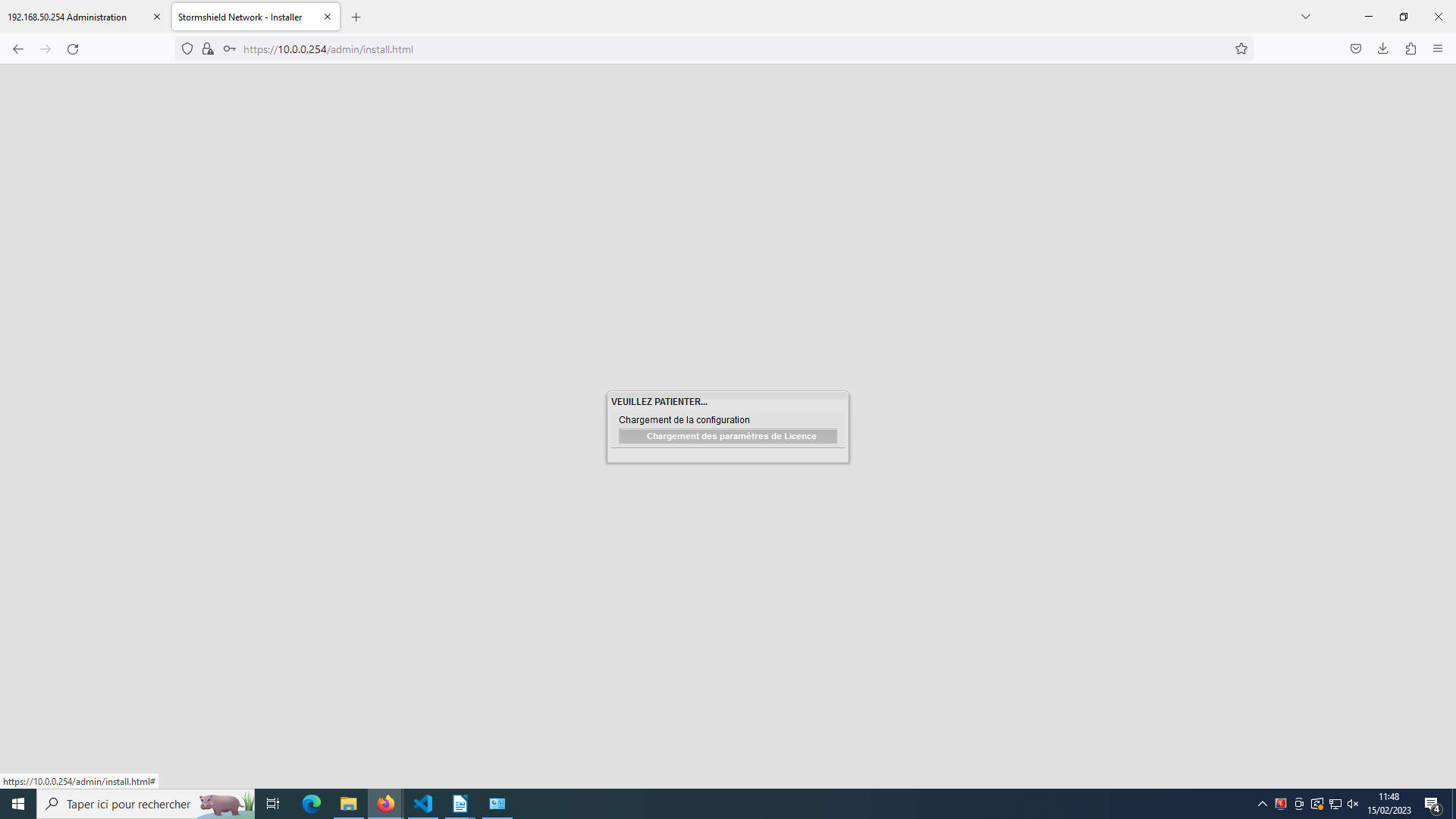
# 1. Administration du pare-feu.

I. Configuration de l’accès

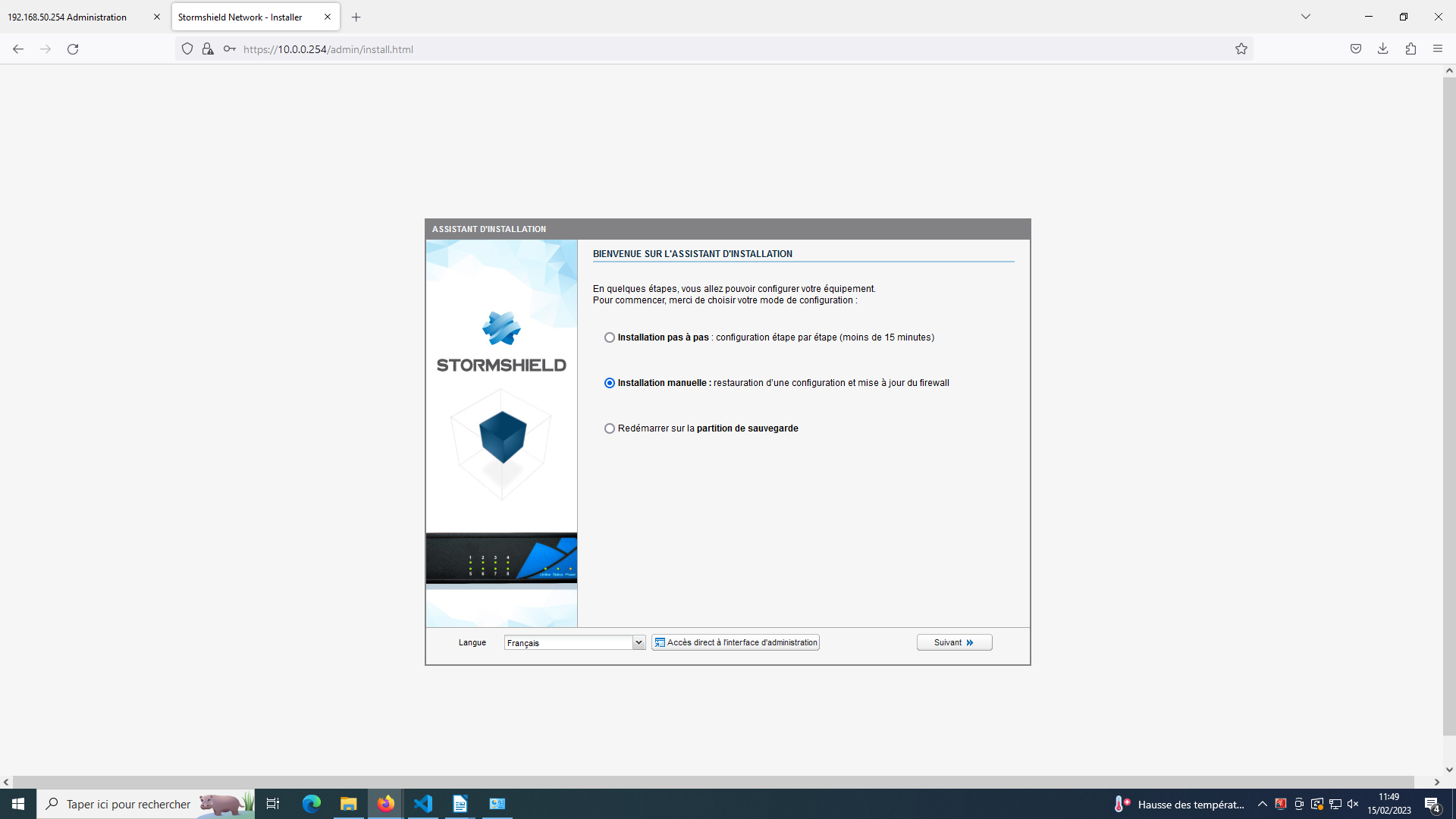
Lors du premier démarrage le Firewall a comme réseau : 10.0.0.0/24. Son interface web est donc sur l’adresse : **10.0.0.254.** Pour se connecter dessus il faudra mettre : <https://10.0.0.254/admin>. Son utilisateur et son mot de passe seront : **admin**.



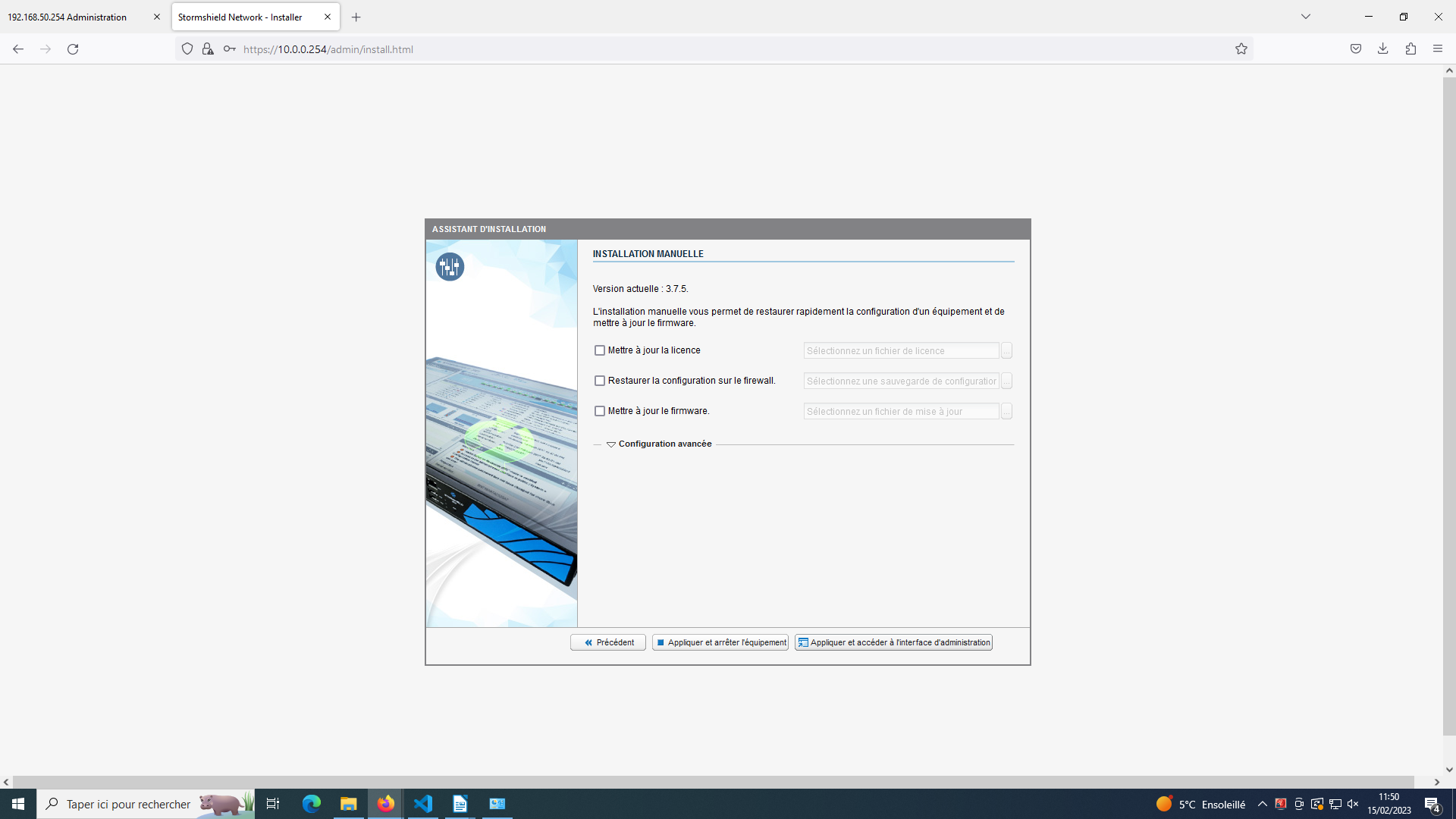
Ensuite le Firewall chargera sa configuration par défaut



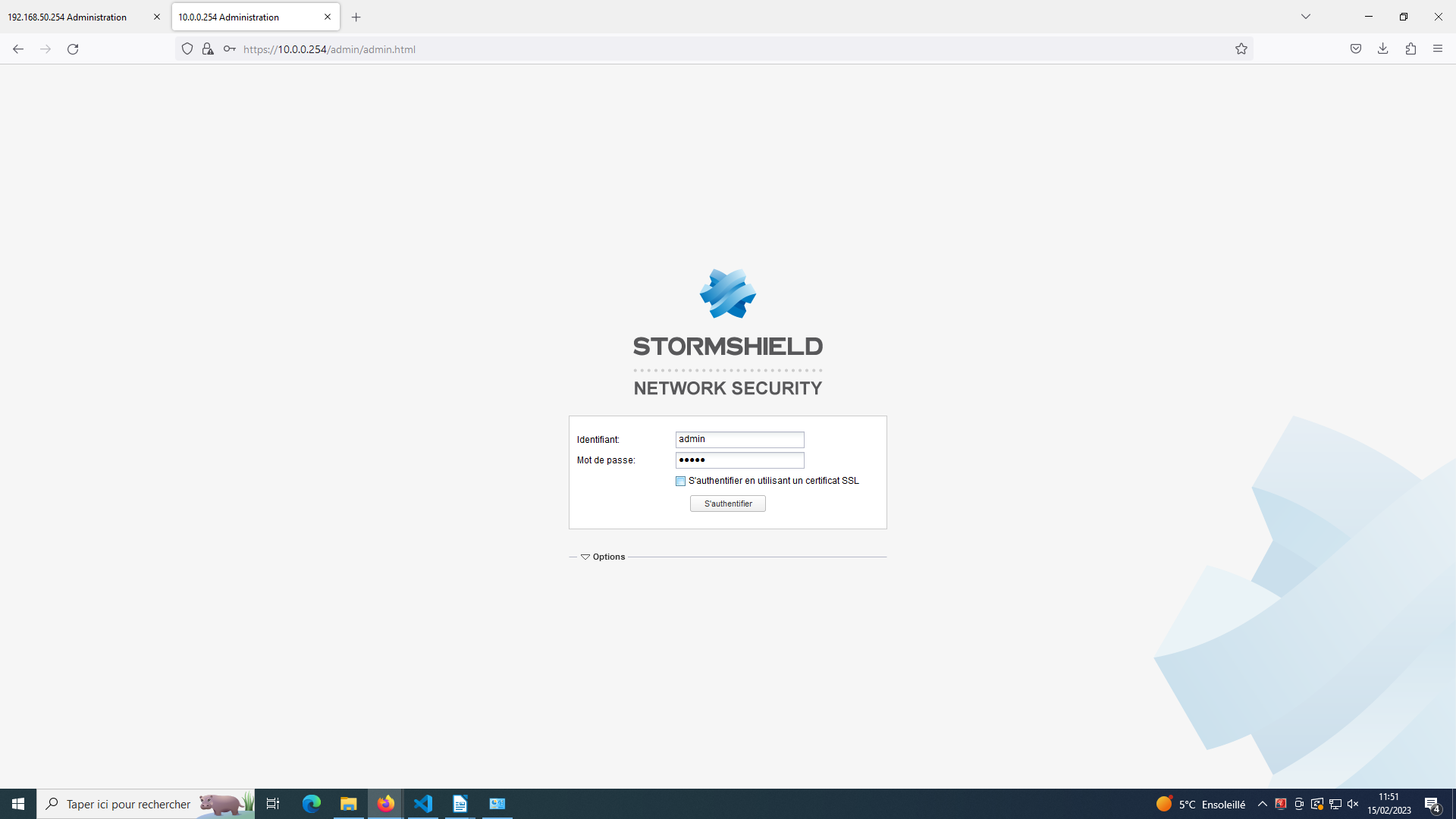
On choisit la configuration manuelle. (Ne pas oublier de mette en Français)

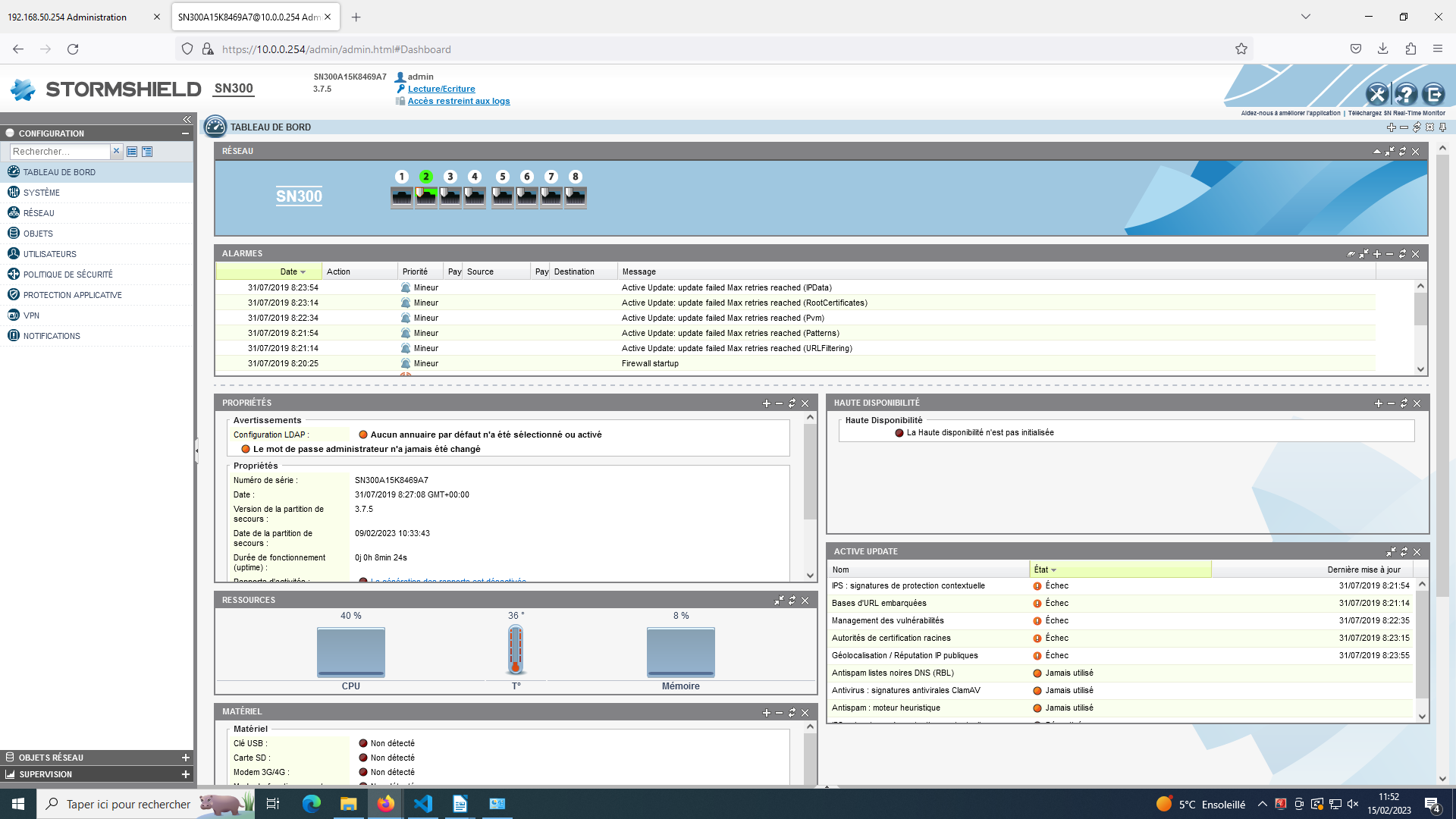


Ensuite on applique afin d’accéder à l’interface web



/ ! \ Rappel : l’identifiant et le mot de passe est : **admin**, par défaut.





II. Configuration du Pare-Feu

L’une des premières configurations à effectuer est de changer l’adresse IP du Lan afin que le Pare-Feu soit dans le même réseaux que les ordinateurs déjà présents.

Pour cela, il faut allez dans :

* Réseaux
* Interface
* Bridge

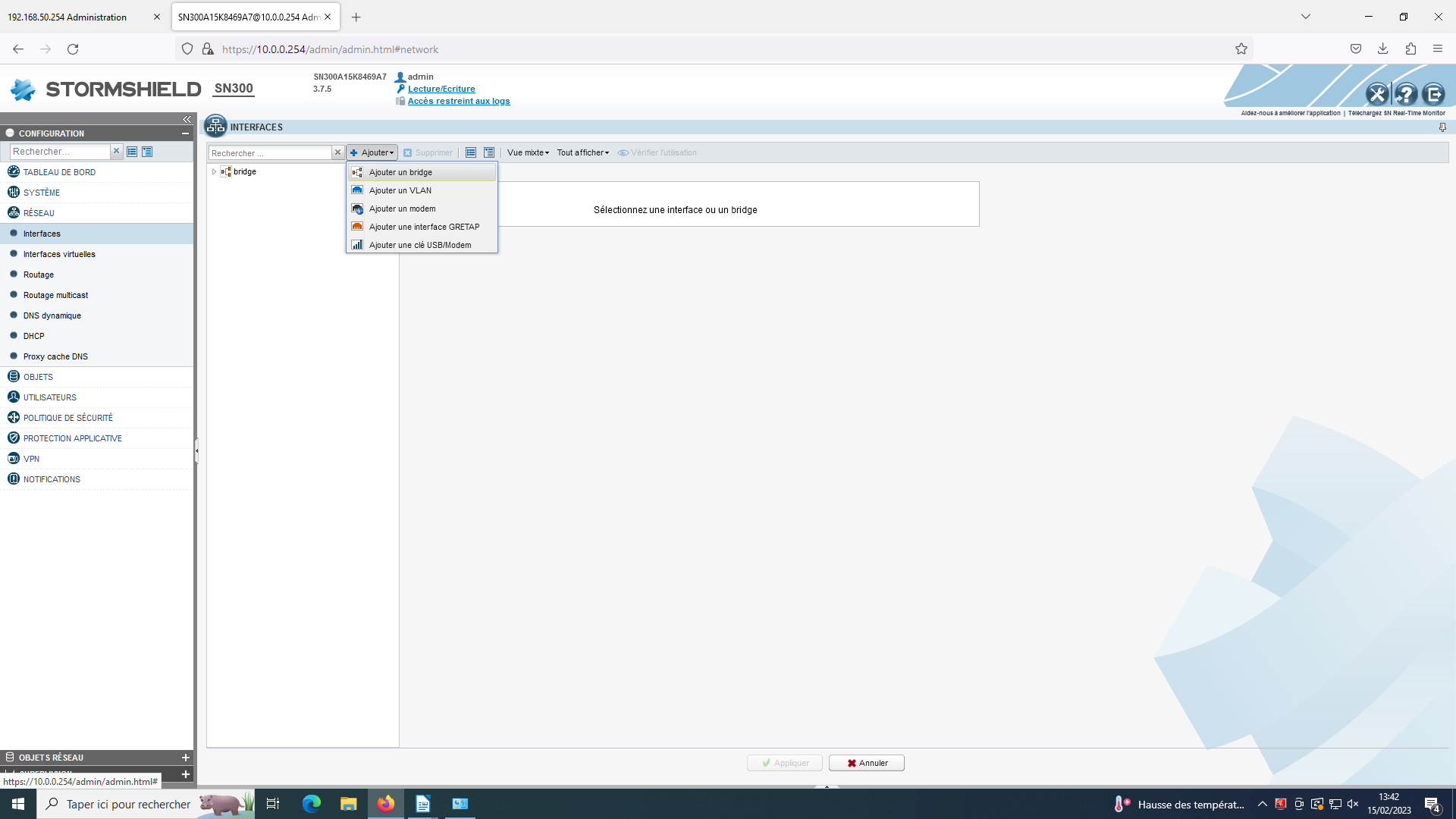
Une image contenant texte

Description générée automatiquement

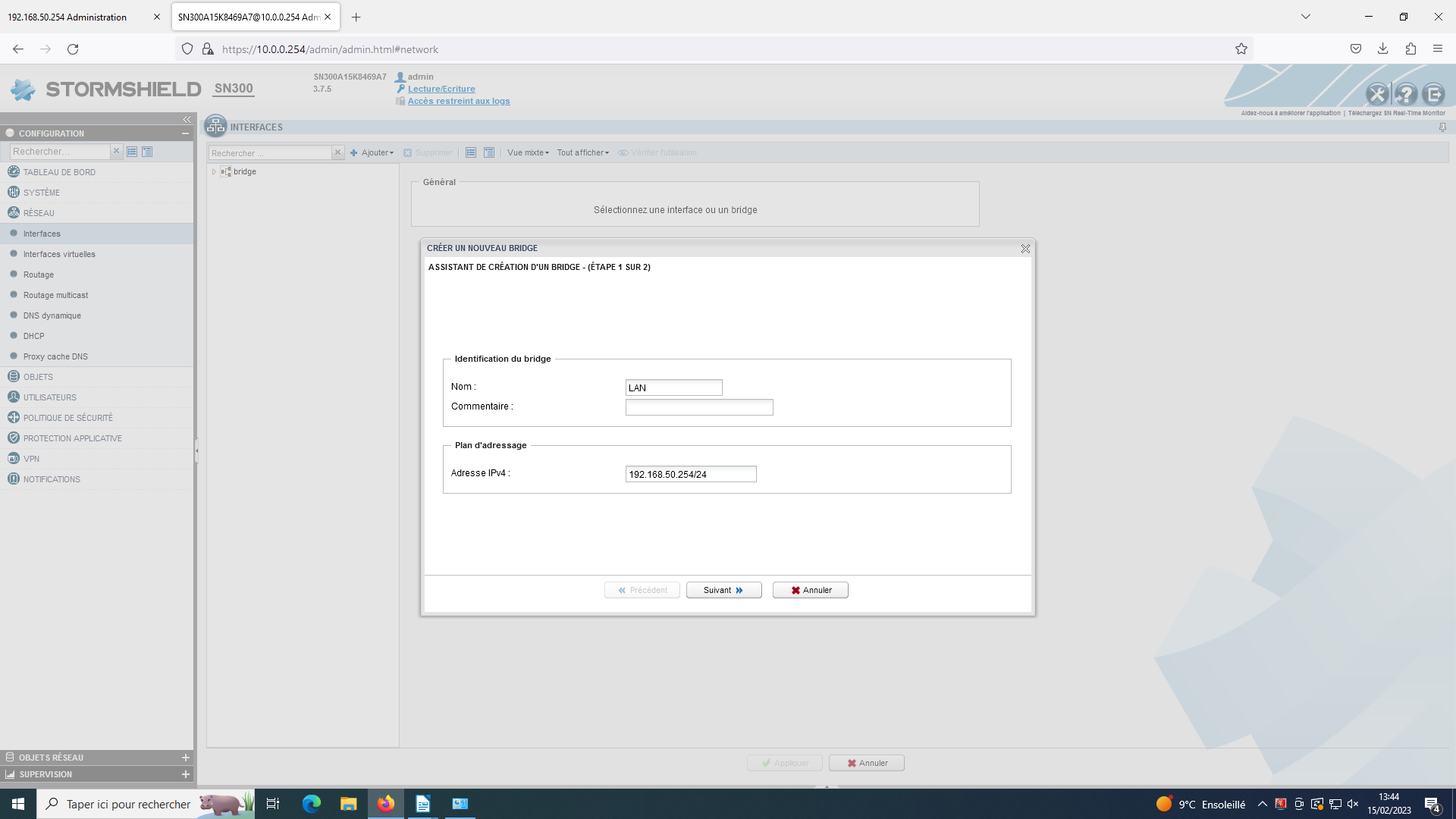
Par défaut les interfaces seront toutes dans le même bridge. Pour sortir l’interface Lan du bridge il faut alors lui administrer une adresse IP ou la placer dans un autre bridge. Ce qui est conseiller est de placer le port Lan dans un autre bridge, dans le cas où il faudrait ajouter un autre port dans le même réseau (un switch interne). Donc nous allons créer un nouveau bridge.

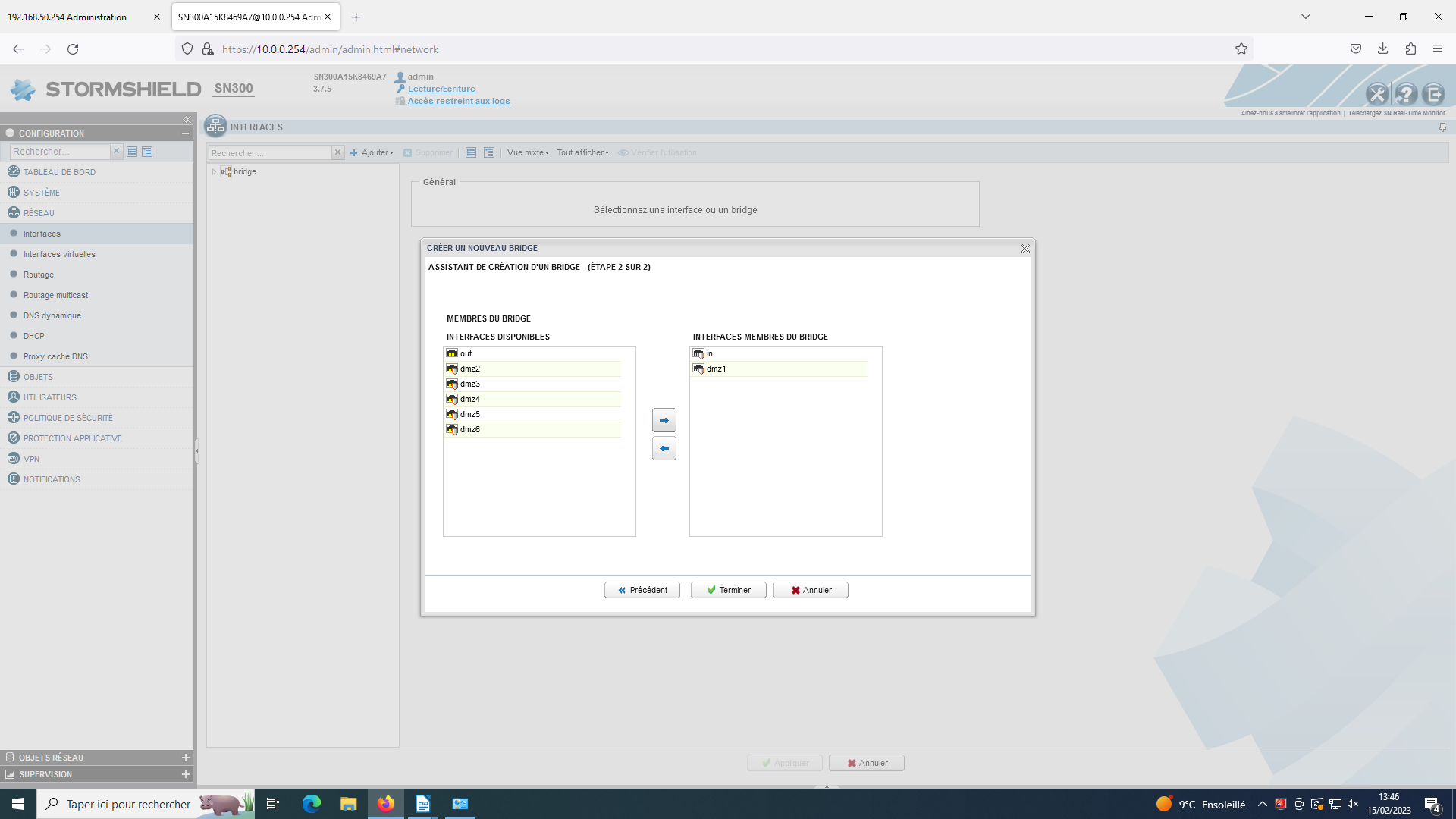
Allez dans :

* Ajouter
* Ajouter un bridge



Ensuite, il faut donnée un nom et une adresse IP avec son masque en CIDR au nouveau bridge, (dans l’exemple le bridge s’appelle « LAN » et il a pour adresse « 192.168.50.254/24)

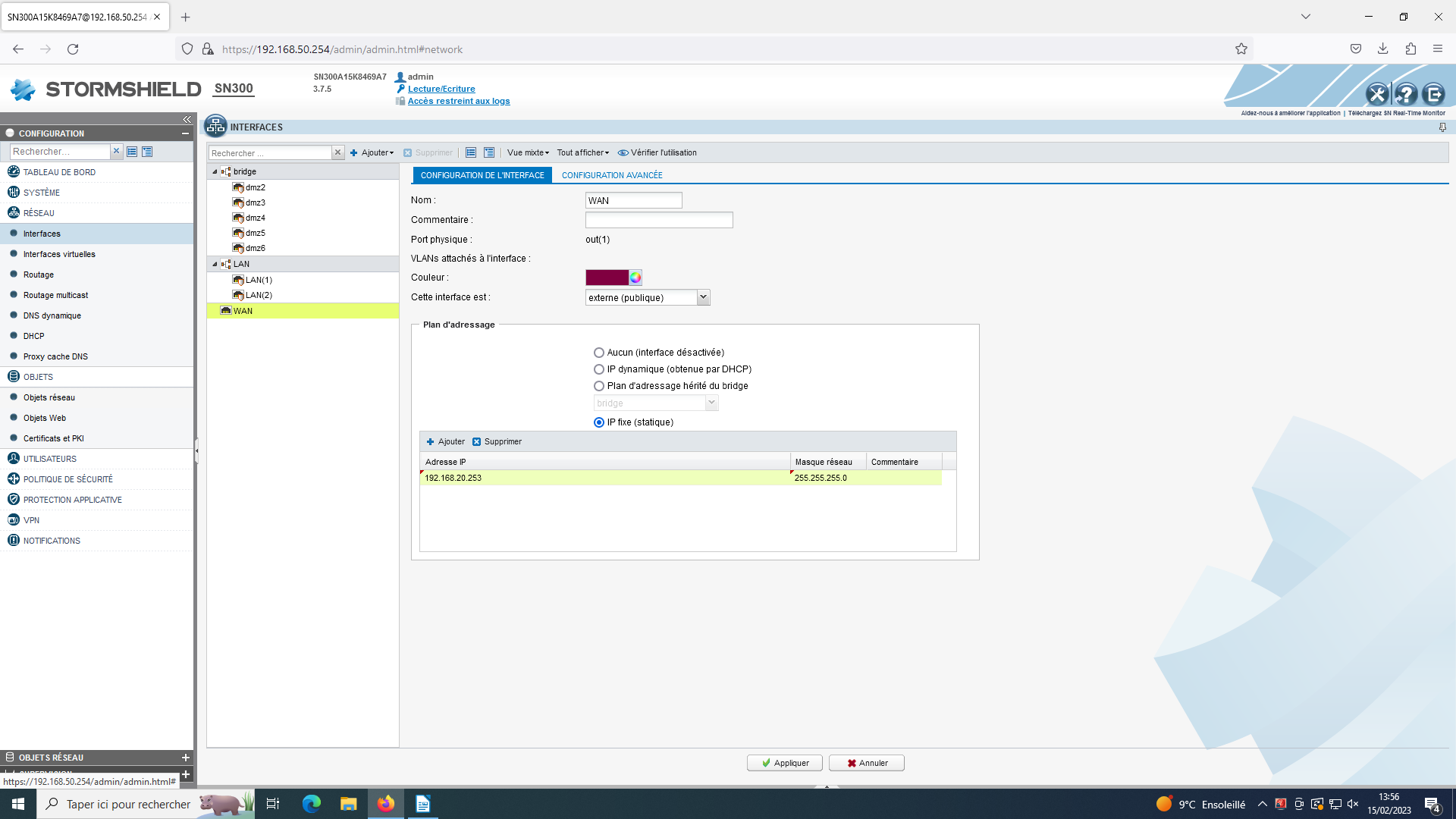


Puis il faut choisir les ports qui seront dans le LAN (dans l’exemple : le port in et le port dmz1 sont sélectionner pour être ajouter aux bridge)

On peut changer le nom des ports, pour cela il faut cliquez sur le port voulu puis changer son nom et appliquer (dans l’exemple les ports in et dmz1 sont renommer pour LAN(1) et LAN(2))

Pour avoir accès à internet sur les ordinateurs il y a plusieurs configurations à faire mais la première est de changer l’adresse IP du Wan.

Il faut aussi sortir l’interface out(WAN) du bridge afin d’avoir accès a internet.Il faut donc lui assigner une adress IP(dans l’ex 192.168.20.253), cliquez sur l’interface puis cliquez sur ip static et entrez l’adresse ip.

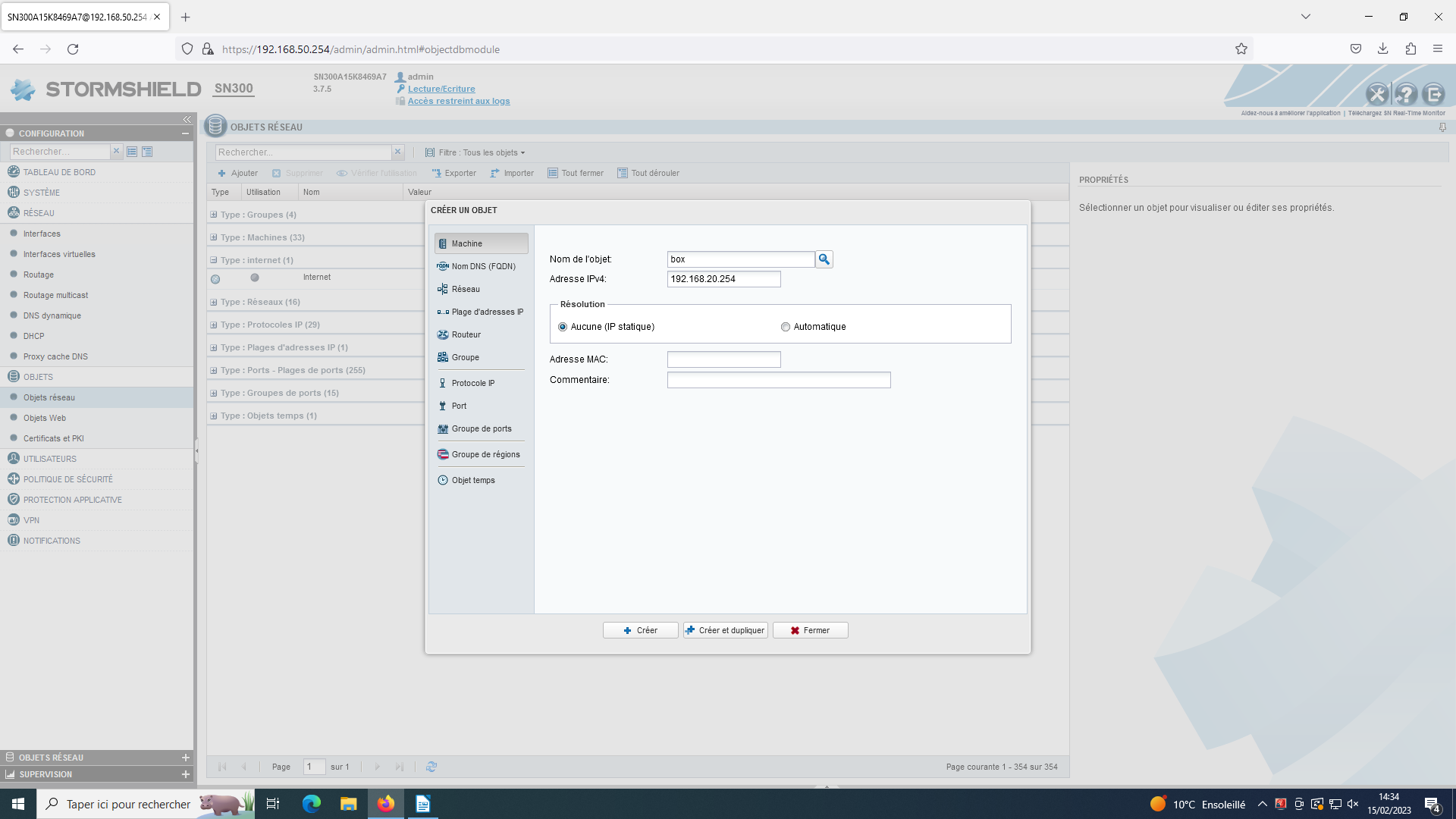


Ensuite il faut crée une route pour avoir accès a la box, pour cela il faut crée un objet routeur pour que l’on puisse l’ajouter comme paserelle dans le routage, puis crée un objet machine que l’on met dans l’objet routeur.

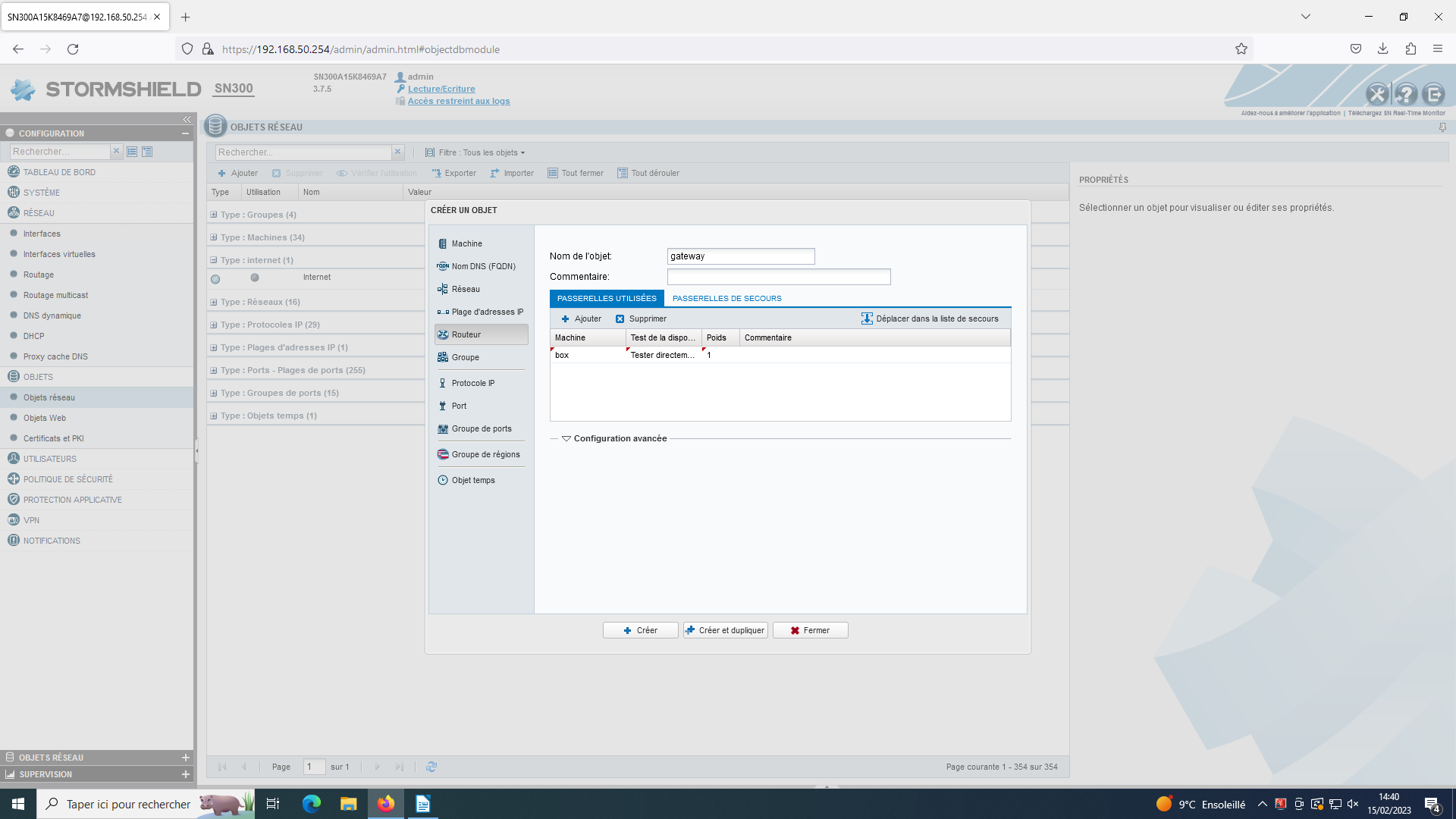
Allez dans « object réseau », puis cliquez sur « ajouter »



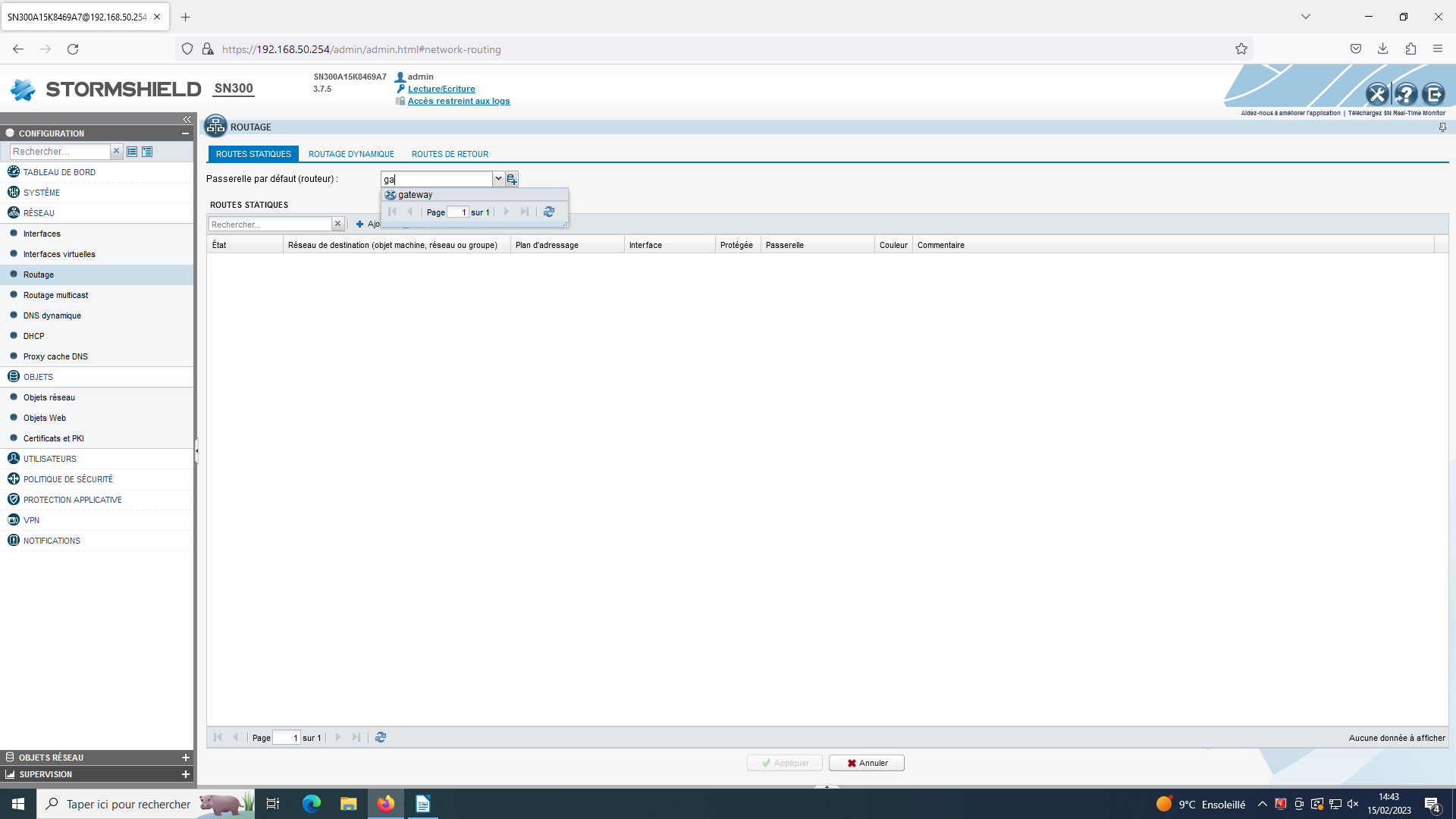
On va commencer par crée un object machine pour lui assigner l’adresse ip de la box(l’adresse lan de la box, dans ex nom : box, adresse ip :192.168.20.254)



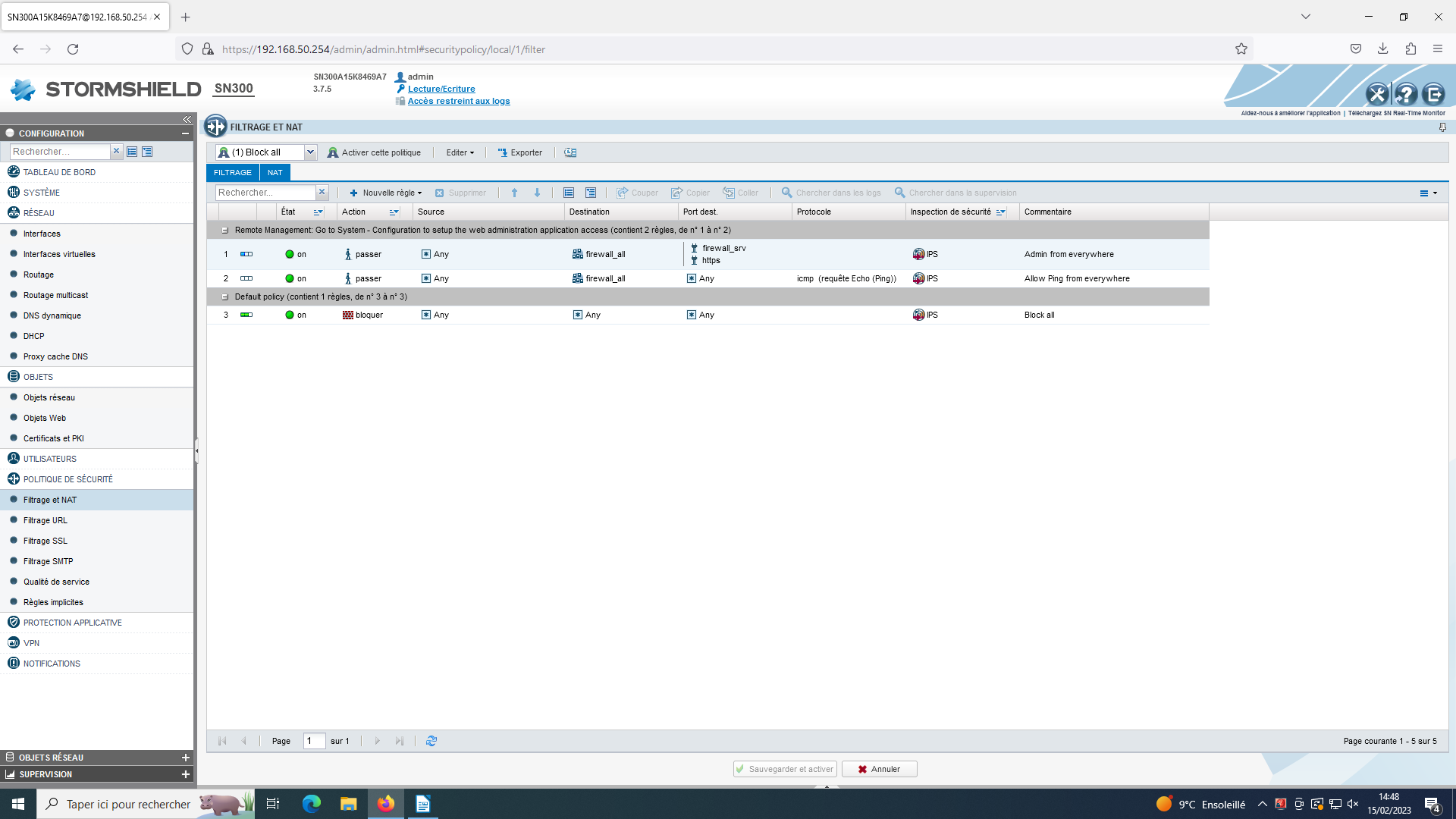
apres avoir appuyer sur « crée », il faut crée un objet routeur pour cela toujours dans « objet réseaux », cliquez sur « ajouté » et sur « routeur ». Donnez un nom a l’objet routeur (dans ex gateway) et ensuite cliquez sur ajouter dans « passerelle utiliser » et entrez le nom de l’objet machine(box), puis cliquez sur crée.



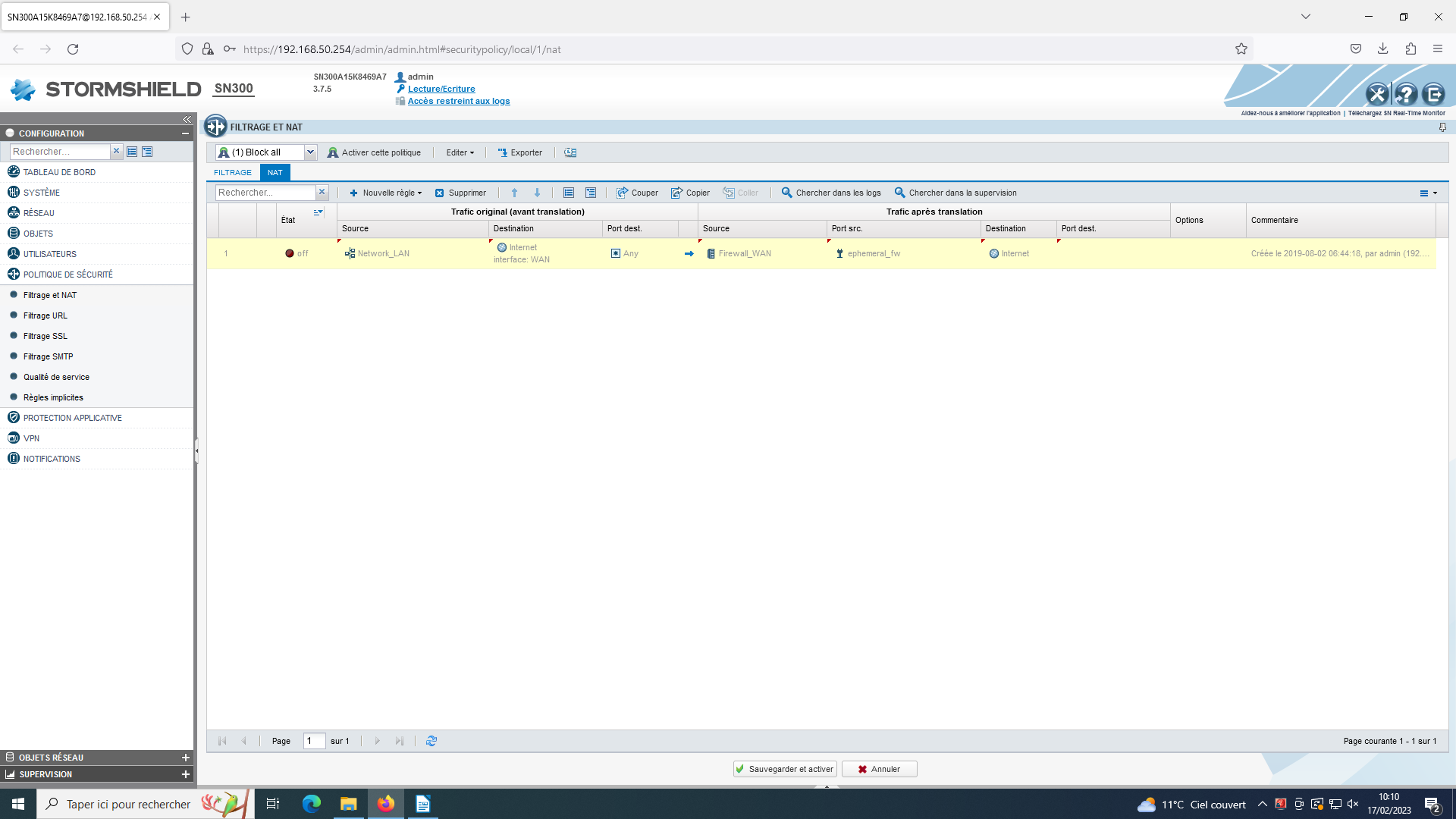
Allez dans « réseau », « Routage » et sellection l’objet routeur dans passerelle par defaut.



Pour avoir accès a internet il faut aussi crée un passage par lequel le LAN passeras pour atteindre le Wan pour pouvoir sortir sur internet.



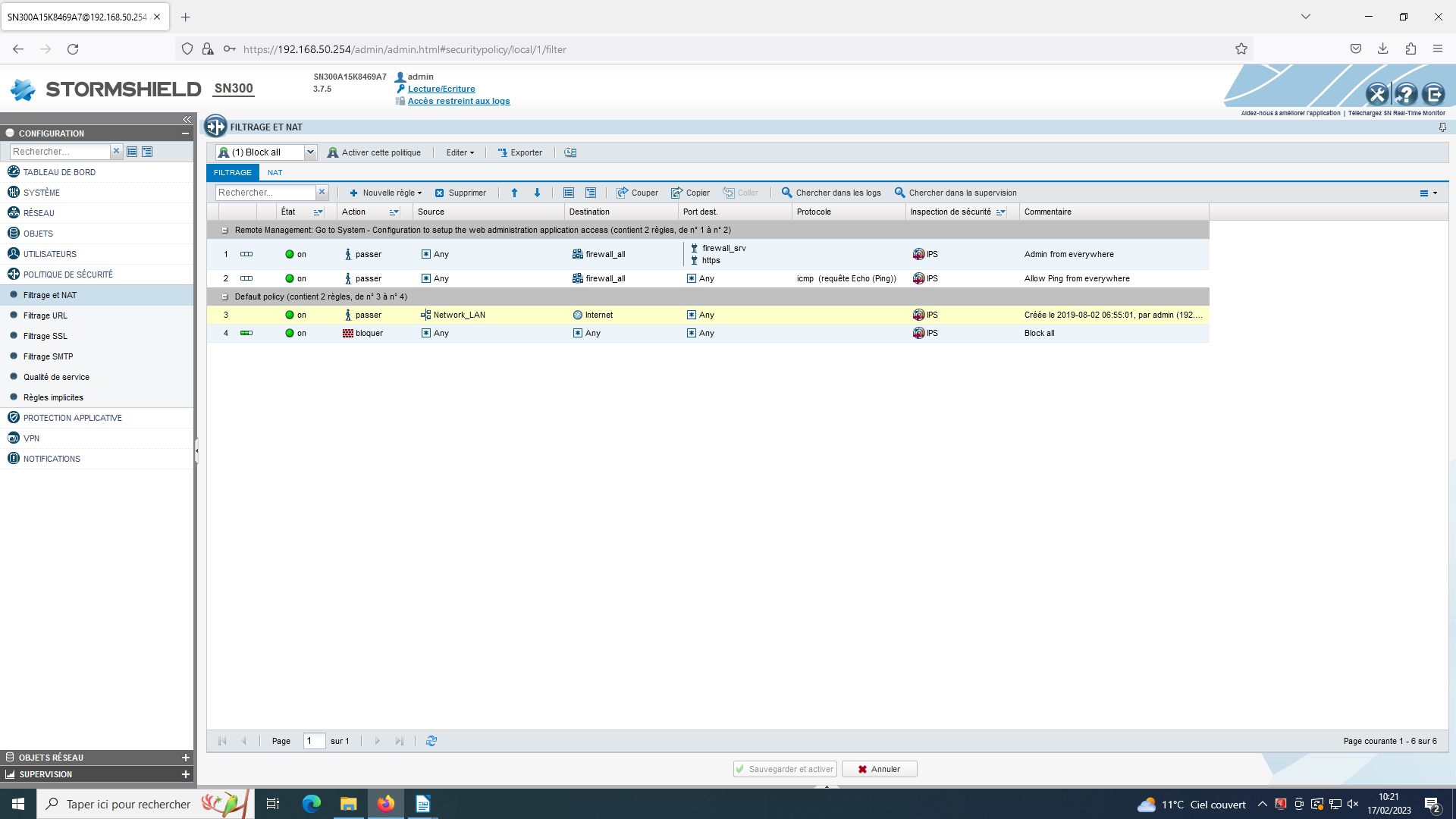
Allez dans « Politique de Sécurité », « Filtrage et NAT », puis sur « NAT » et « Nouvelle règle », « règle simple »

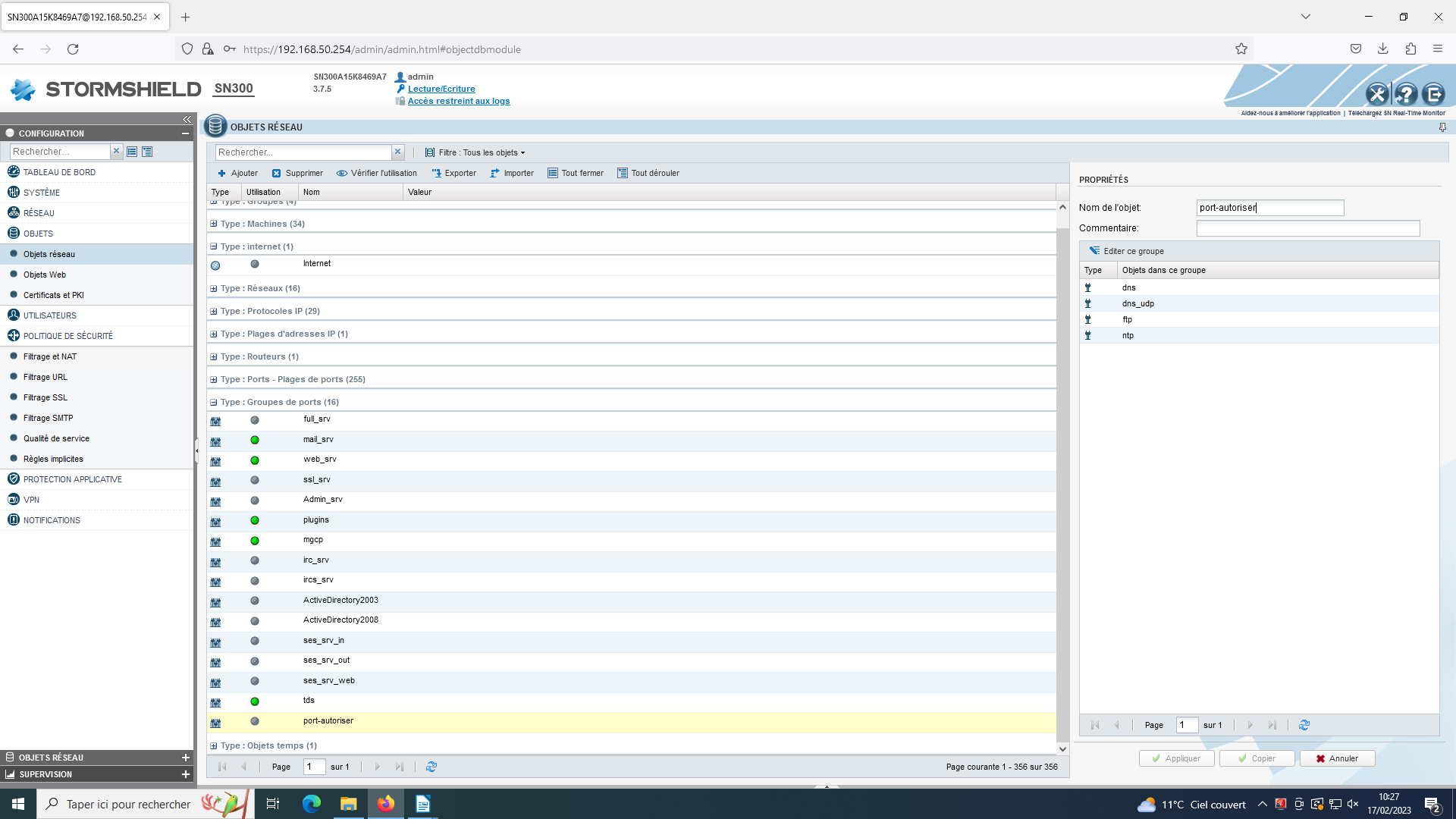


|  |  |  |  |
| --- | --- | --- | --- |
| Trafic original | Source | Network lan | Réseaux du LAN |
| Destination | Internet, interface wan | On veut allez sur internet donc on va passez par l’interface wan |
| Port destination | Any | Tout les ports en destination |
| TRANSLATION | | | |
| Trafic après translation | Source | Firewall Wan | Il passe par l’interface wan, firewall wan |
| Port destination | ephemeral\_fw | Tout les ports apres translation |
| Destination | Internet | Notre but internet |

Pour sortir sur internet il faut encore pourvoir etre autoriser, dans le filtrage si le reseau lan n’est pas autoriser alors il ne pourras pas allez sur internet.

Crée une « nouvelle règle », « regle simple », qui a pour action « passer » …..Ne pas oubliez de monter la règle afin qu’elle passe avant les autres( en fonction des priorité qui se font de haut en bas)(règle 3)

Pour filtrer les ports qui pemette seulement d’allez sur internet on peut les ajouté dans « port destination » un par un ou alors on peut crée un groupe de port pour le port qui permet d’accès a internet

Allez dans « Objets », « objets reseau », « ajouté », « groupe de port », donnez un nom au groupe est ajouté les port concerner par ce groupe :

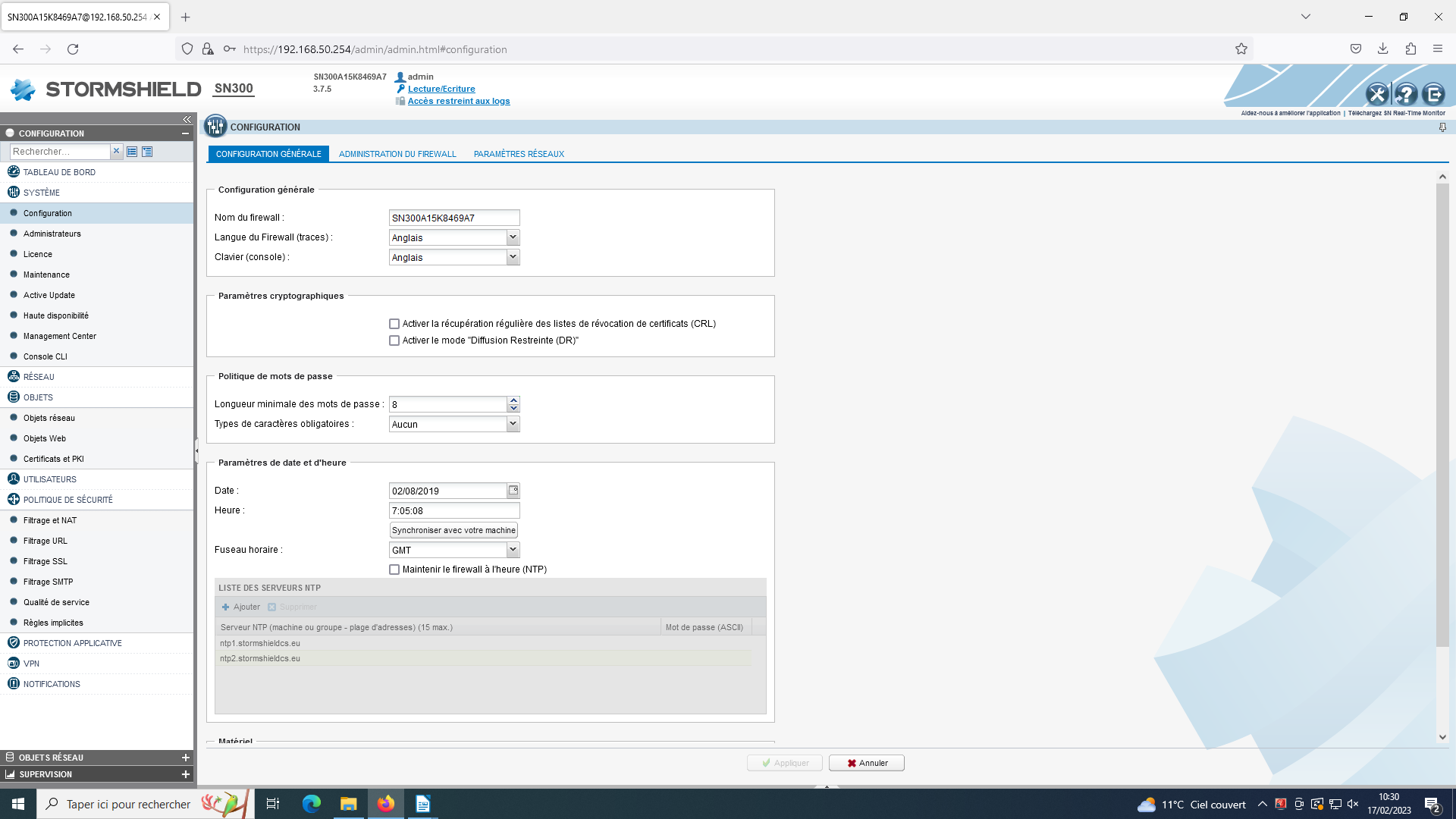
-dns

-dns\_udp

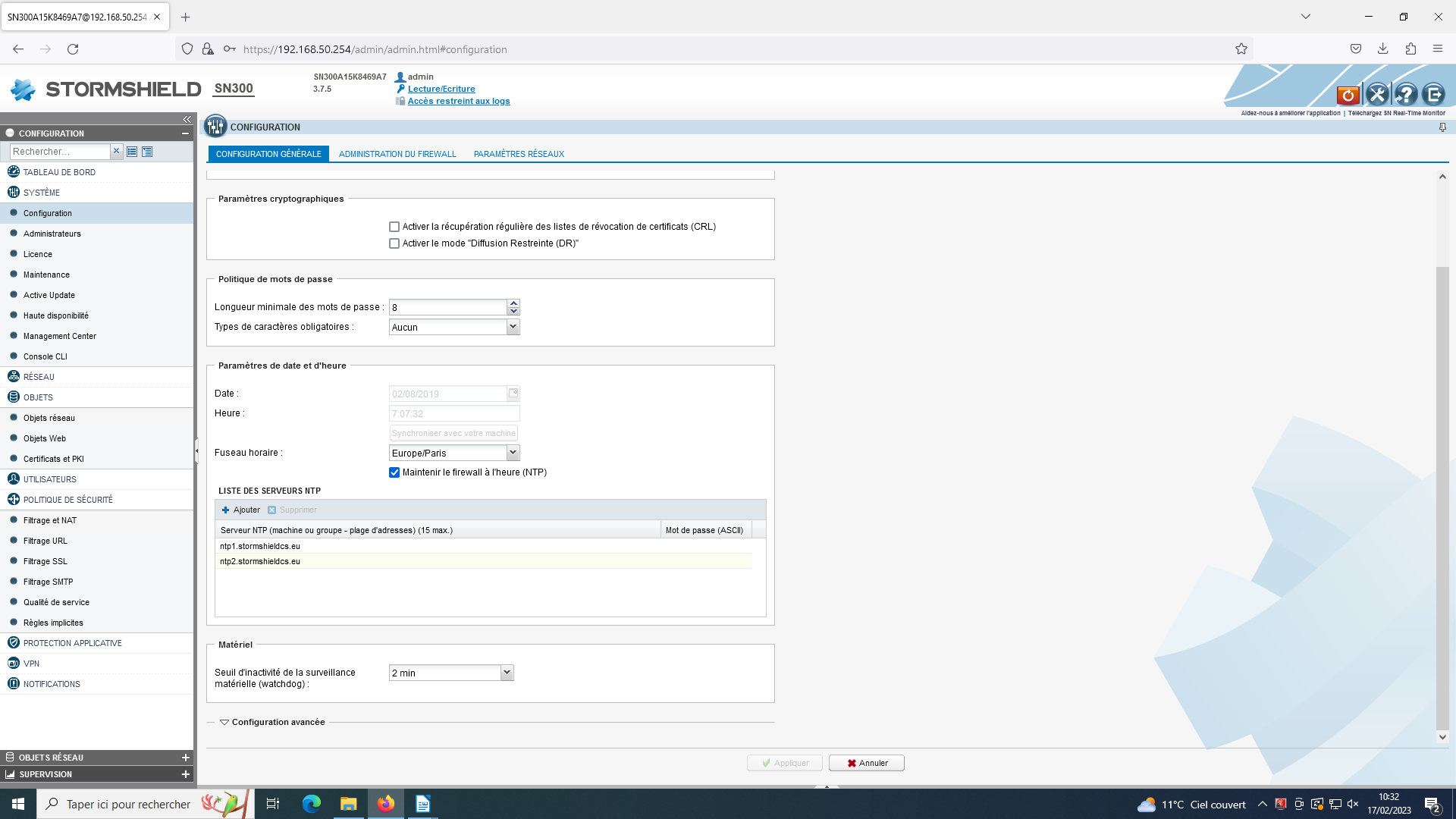
-ftp

-ntp

Votre FireWall peut accédez a internet, en théorie mais il n’est pas a l’heure donc cela ne fonctionneras pas. Pour règle ce problème il faut allez dans « Système », « configuration », « paramètre de date et heure ».



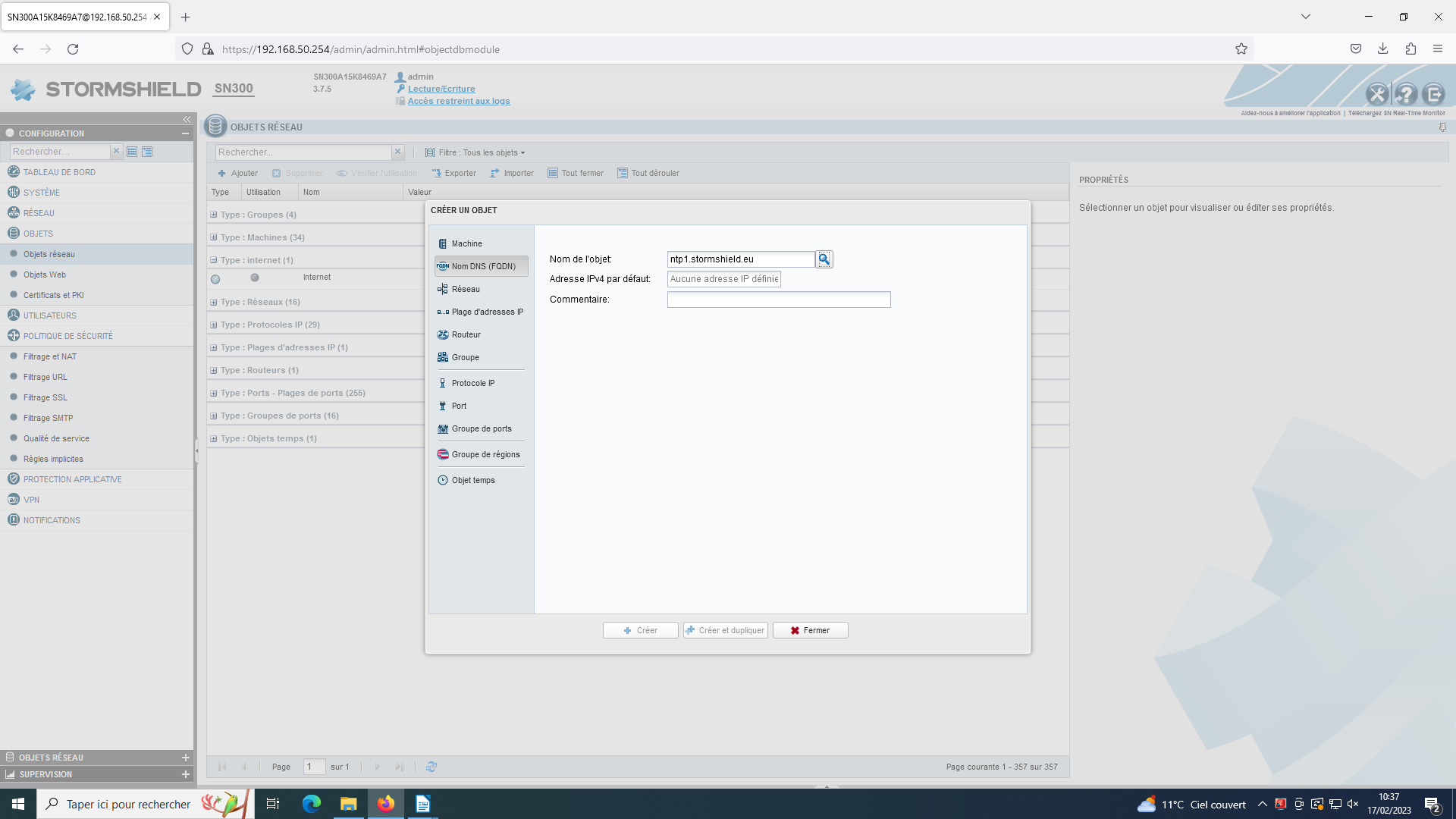
cliquez sur « Maintenir le firewall à l’heure(NTP) », et entrez dans « fuseau horaire » « Europe/Paris »



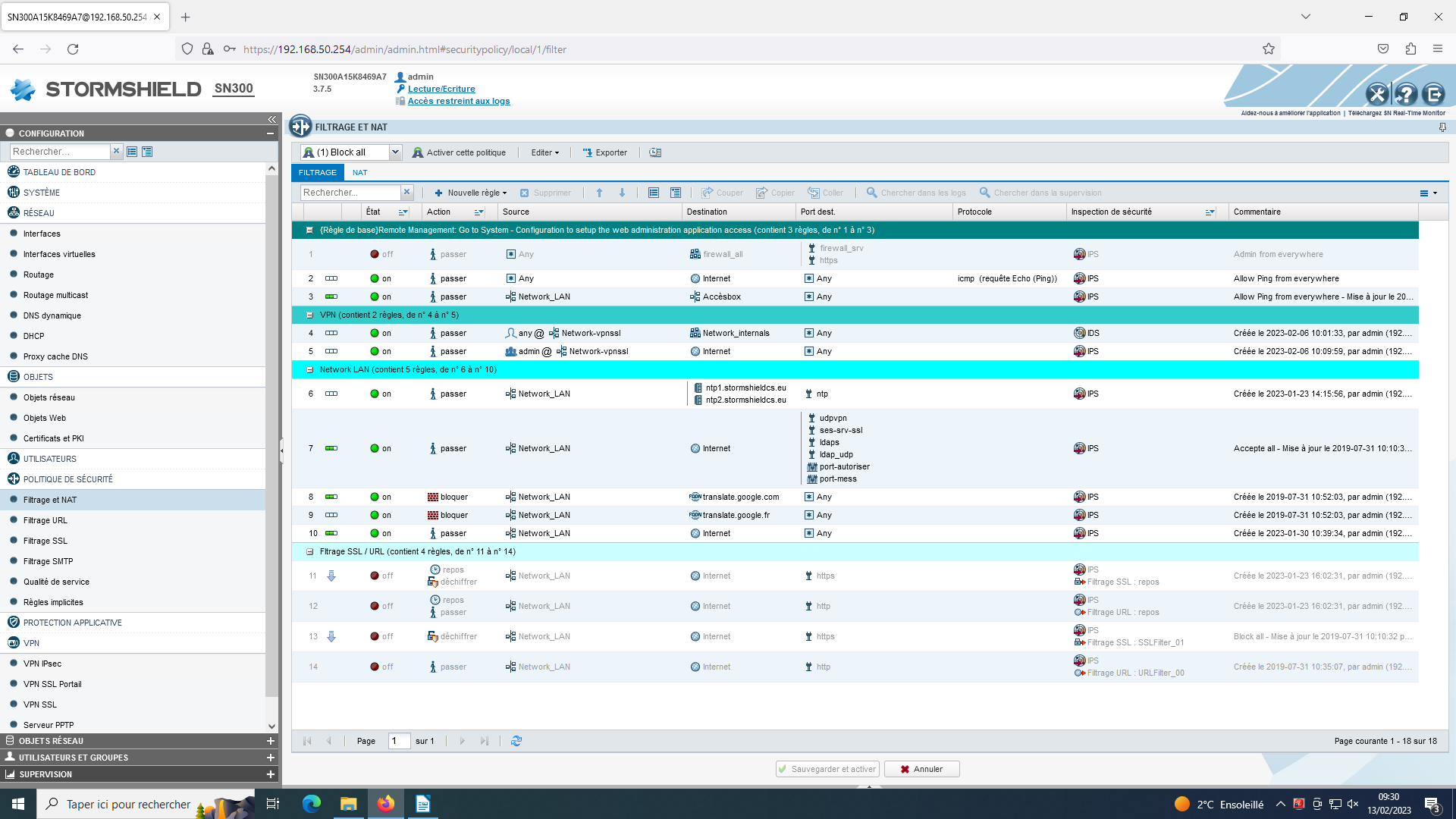
Et redémarer le firewall

Maintenant, il faut que le firewall puisse allez chercher la date et l’heure sur les serveurs ntp1.stormshield.eu et ntp2.stormshield.eu. Pour cela il faut crée des objet machine que l’on intégreras a une regle de filtrage crée pour le ntp.

Allez dans « Objets », « objets réseau », « ajouté », «Nom DNS (FQDN)», mettre «  ntp1.stormshield.eu » dans nom de l’objet, puis appuyer sur la loupe pour que le firewall puisse allez chercher l’adresse ip du serveur ntp. (refaire la même opération pour ntp2.stormshield.eu)



Une fois les 2 objets réseau crée allez dans « Politique de Sécurité », « Filtrage et NAT », «Filtrage», crée une « nouvelle règle », « règle simple », qui a pour action de lasser « passer »les serveur ntp.

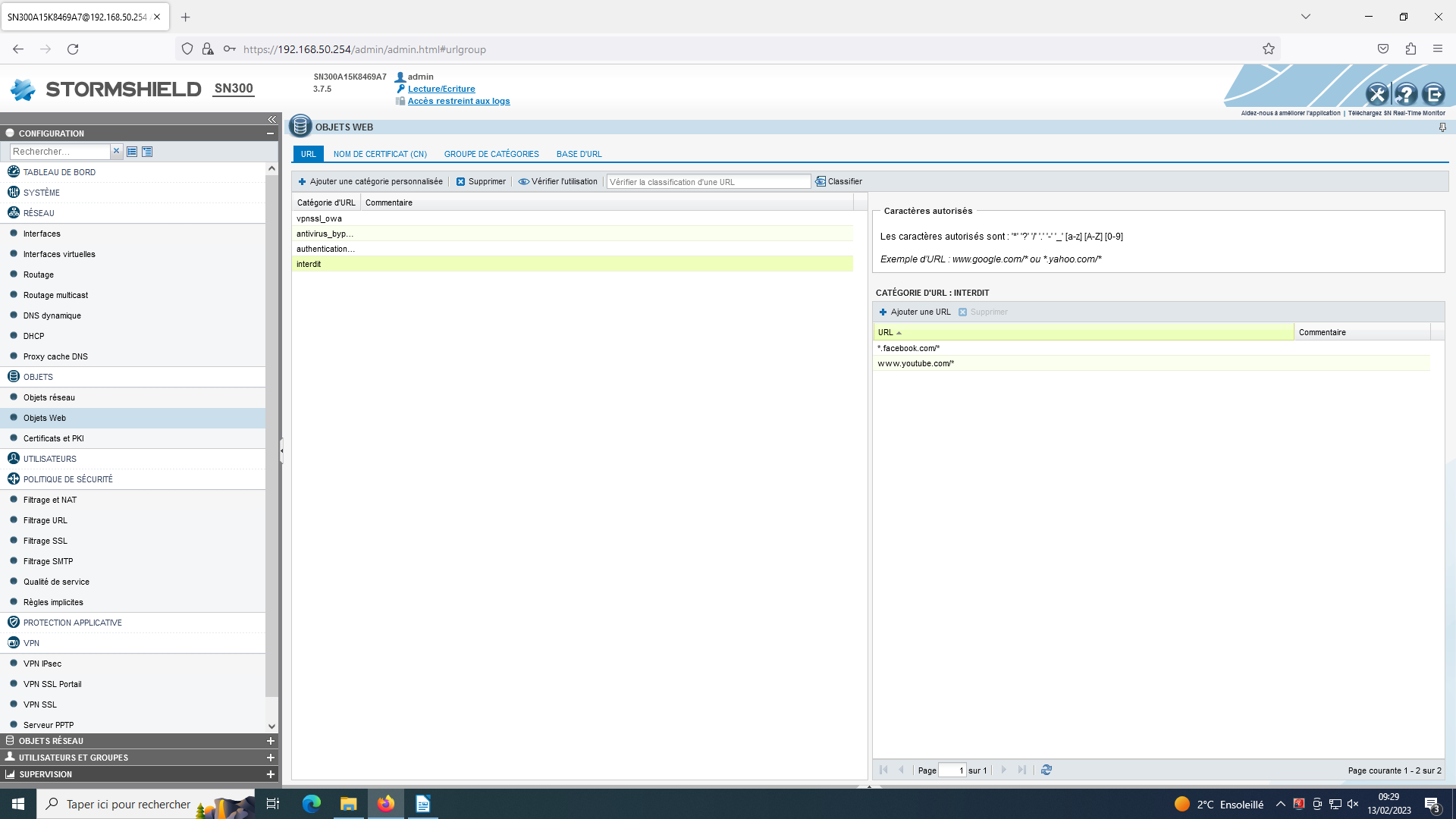


Pour filtrer les site web autoriser ou interdit il faut crée une liste avec les site que vous voulez interdire (attention il y a déjà une liste de site par catégorie crée par l’université de Toulouse ? (à vérif))

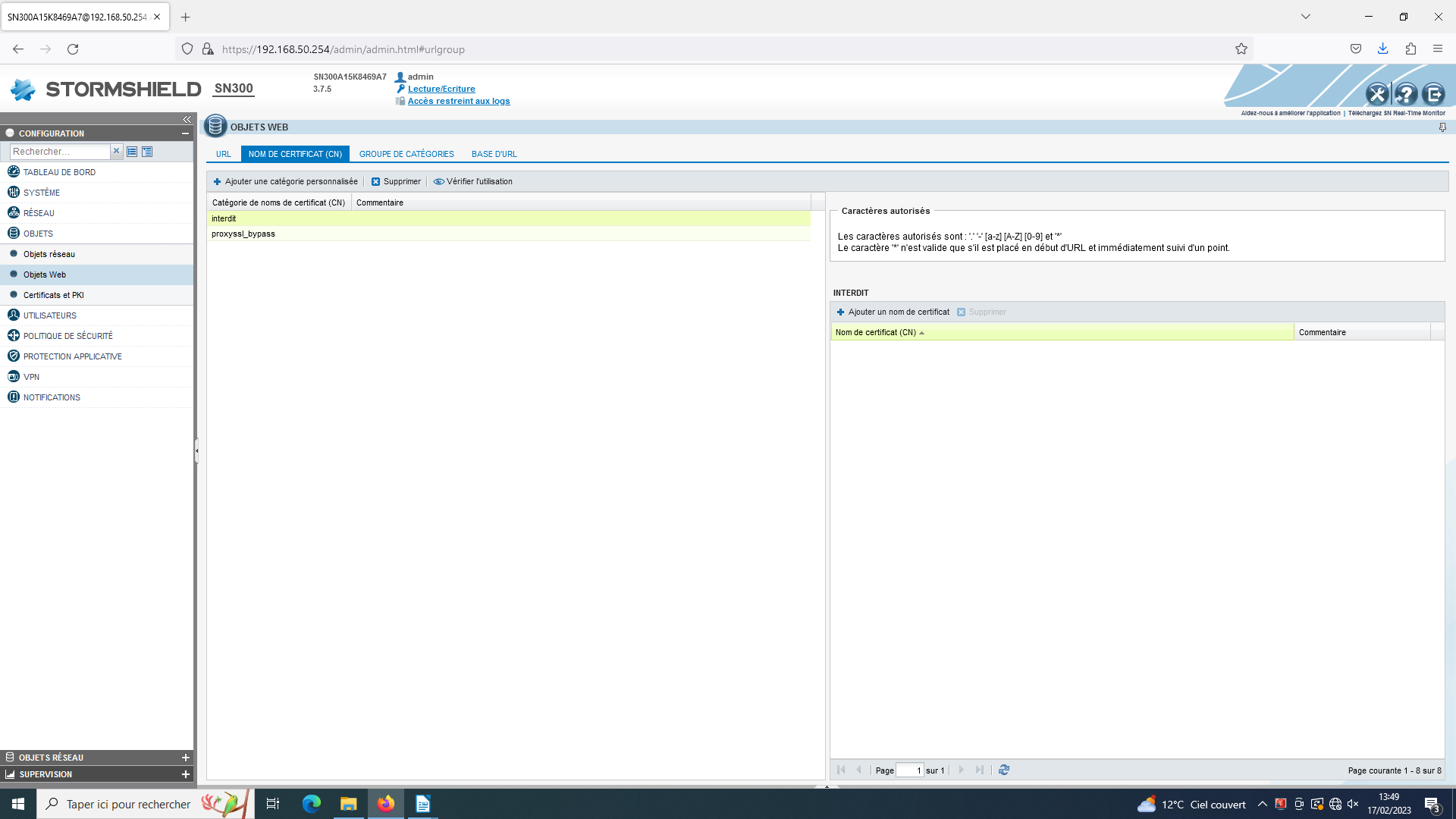
pour crée une nouvelle liste de site web a interdire (dans l’ex), il faut allez dans « objet s web » et cliquez sur « ajouter une catégorie personnalisée »

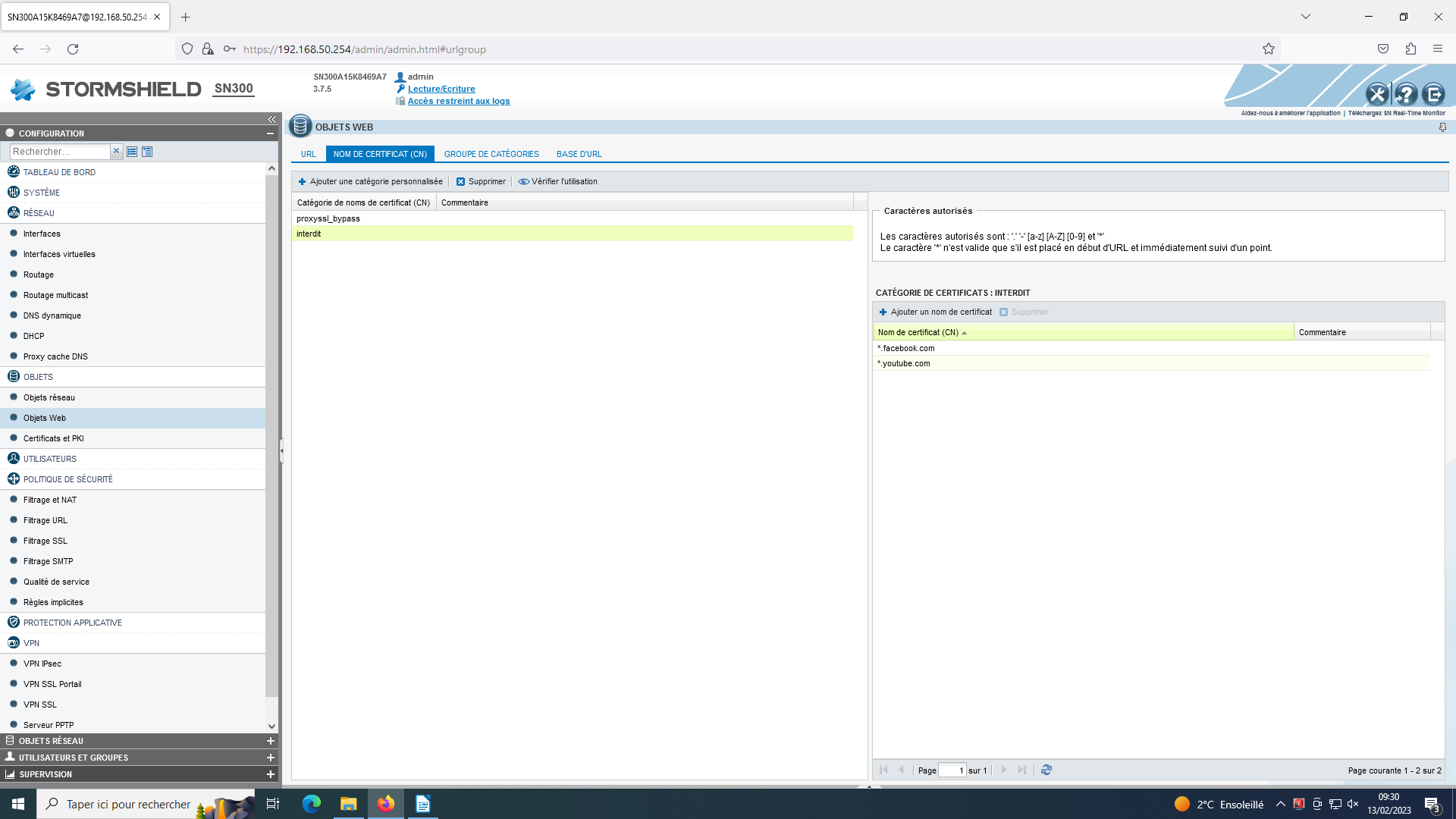


(Dans l’ex interdit est la catégorie)Pour ajouter un site web, cliquez sur «  ajouter une URL », ex bloquez youtube et fb il faut notez : www.youtube.com/\*



Puis refaire la même chose, crée une catégorie le même nom de préférence dans « Nom de certification »





Allez dans « Politique de sécurité », « Filtrage URL »

