A decorative graphic on the right side of the slide. It features three blue circles of different sizes, each composed of concentric rings of varying shades of blue. Two thin blue lines intersect at a point between the top and middle circles, extending towards the top-left and bottom-right corners of the slide. A third thin blue line extends from the bottom-right corner towards the bottom-right circle.

Mise en place d'un serveur proxy avec authentification AD et serveur RADIUS

BLOC 3 –SIO2

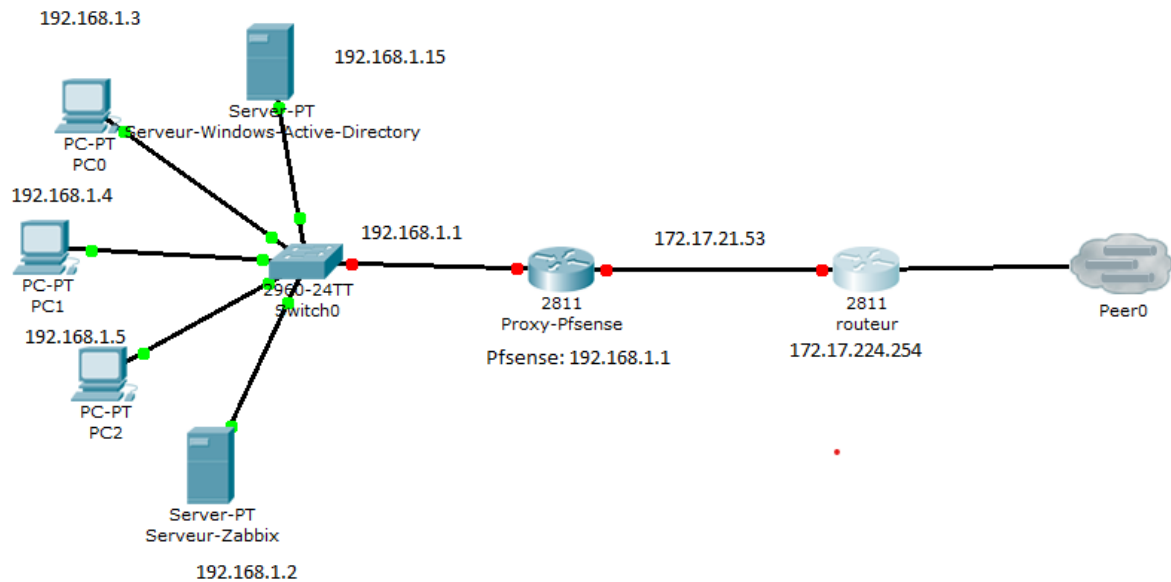
MACLOUD HAUTTECOEUR

07/03/2023

Sommaire

Schéma réseau et plan d'adressage :.....	3
Besoin:.....	3
Objectif :.....	4
Solutions mis en place :.....	4
Configuration :.....	5

Schéma réseau et plan d'adressage :



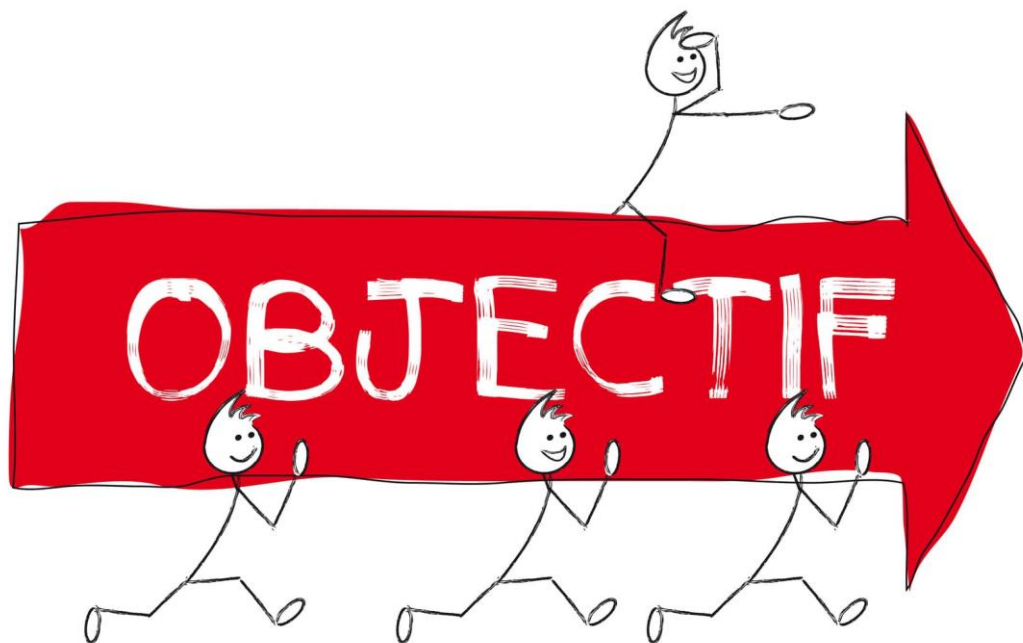
Besoin:

L'entreprise souhaite donc vous confier la mission de filtrer les accès au Web pour 2 raisons principales : savoir quels sont les sites visités et pouvoir fournir les logs aux services de police en cas de réquisition ; empêcher les salariés de consulter des sites dont ils n'ont pas à avoir accès dans le cadre de leur travail. Votre Directeur des Systèmes d'information (DSI) a beaucoup entendu parler du logiciel Squid et souhaite donc que vous utilisiez cette solution. La solution précédente : un serveur proxy transparent ne permet pas l'identification exacte des personnels. On veut donc mettre en place un proxy qui identifie la personne qui utilise la connexion. Cela doit se faire grâce à un serveur Active Directory et au protocole RADIUS.



Objectif :

Répondre à des besoins de filtrage des accès Web des postes clients de l'entreprise BioDicé avec authentification des clients grâce à un serveur Active Directory et à un serveur d'authentification RADIUS.



Solutions mis en place :

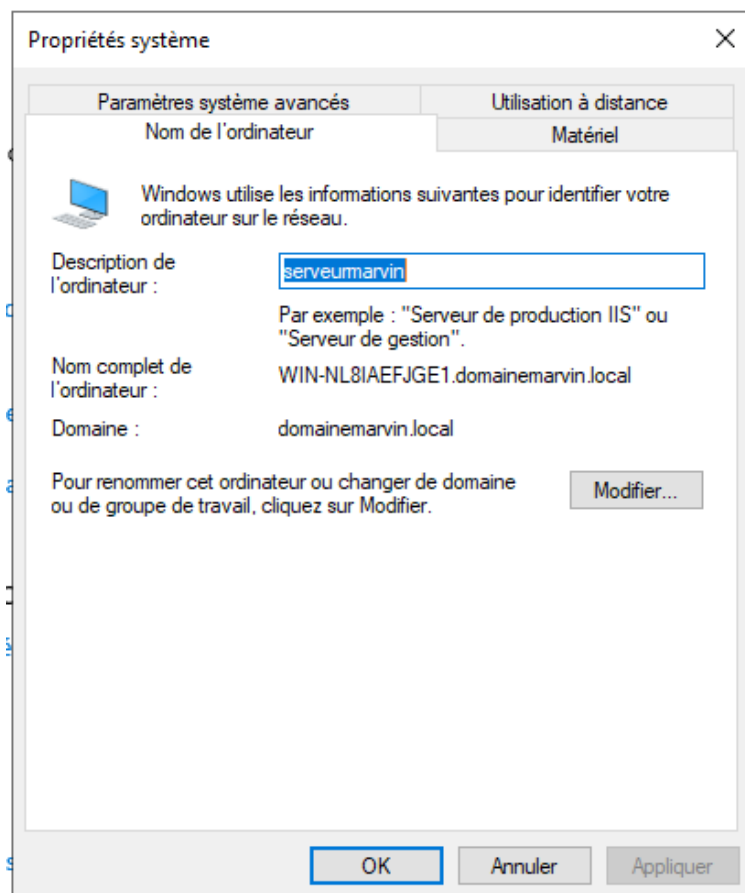
Installation et configuration d'un serveur PROXY avec SQUID sous une distribution PFSense. Les utilisateurs s'authentifient par le biais de leur compte AD à un serveur RADIUS ou le serveur filtre

l'accès à des sites HTTPS. Squid Guard empeche la connexion à certain sites comme les sites adultes par exemple. Et enfin on doit pouvoir consulter les sites visités par chaque client avec SQUIDLIGHT.

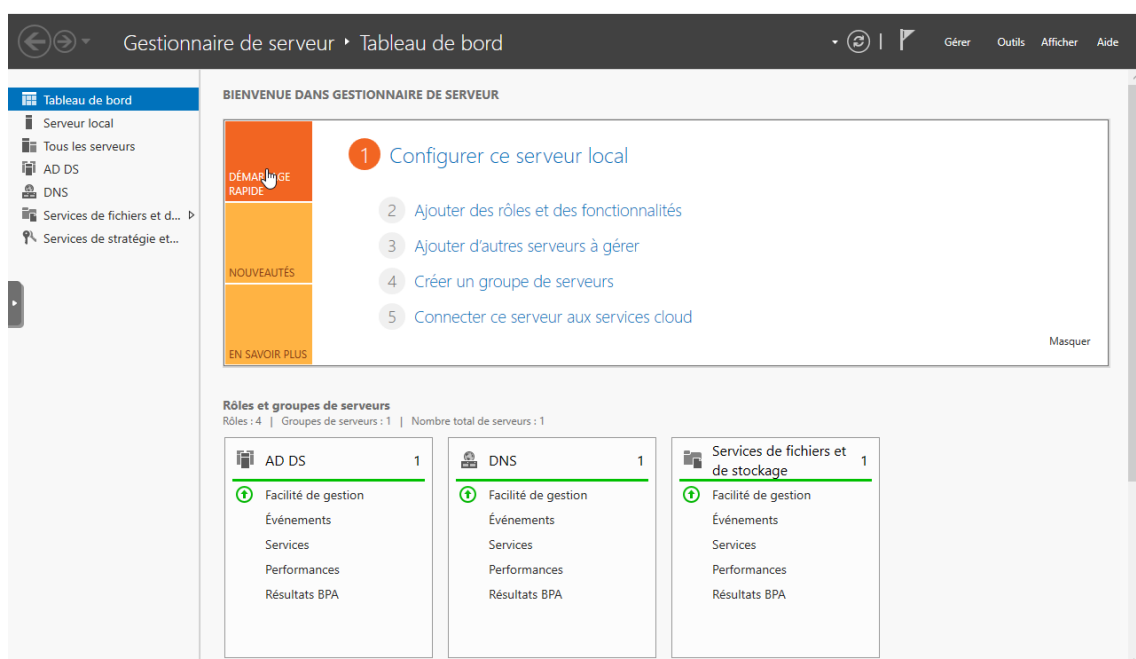


Configuration :

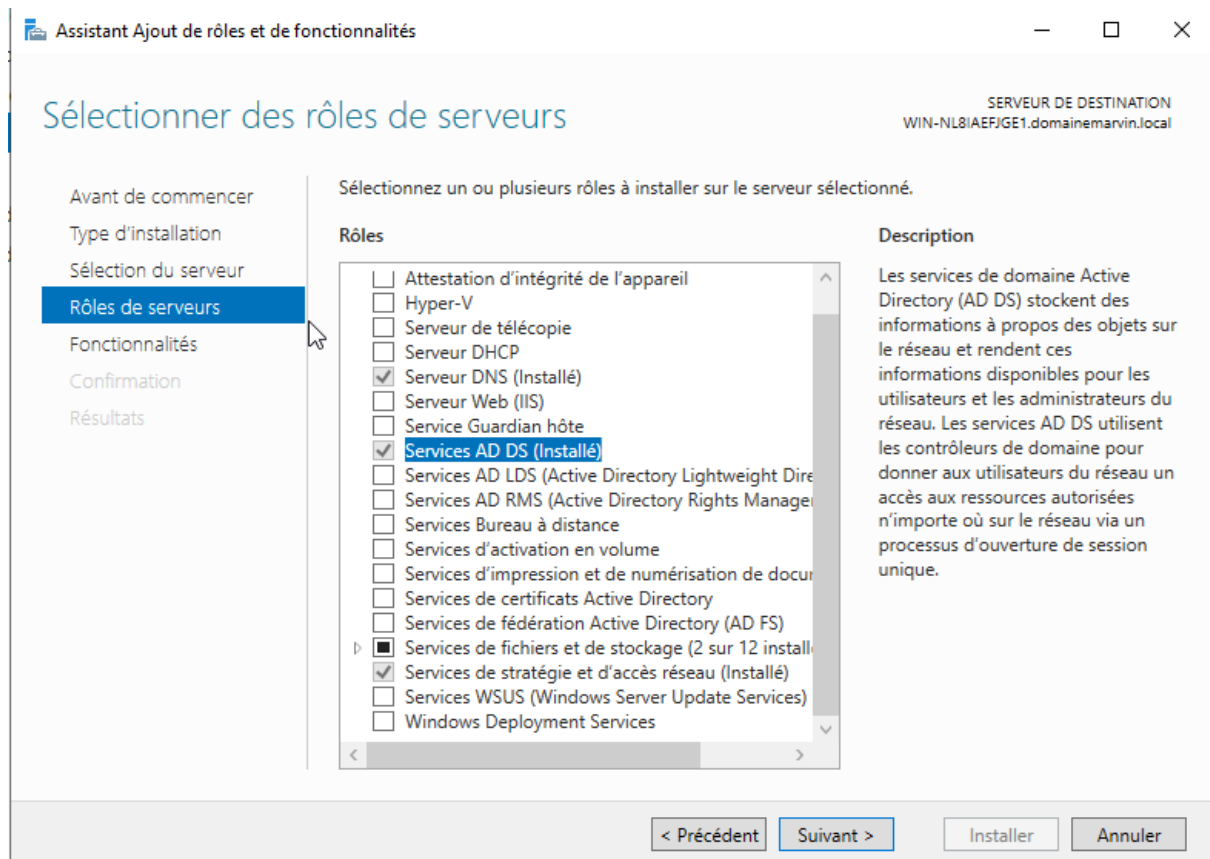
Dans un premier temps je renomme le serveur



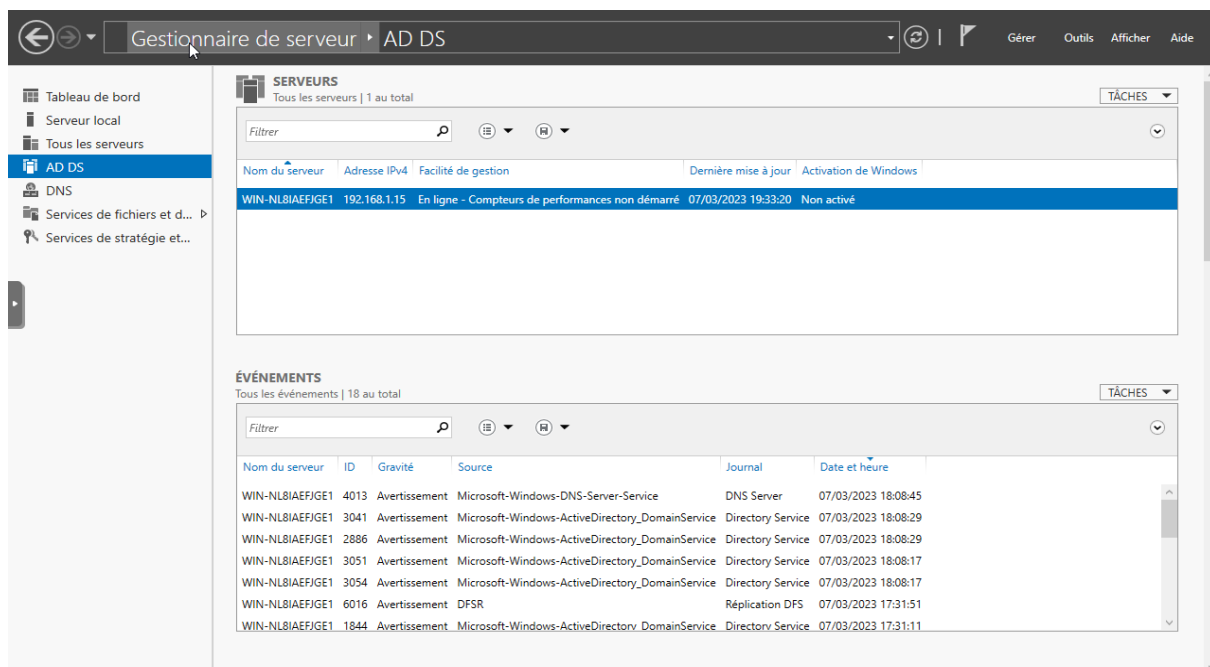
Je vais dans le gestionnaire de serveur puis je clique sur Ajouter des rôles et des fonctionnalités



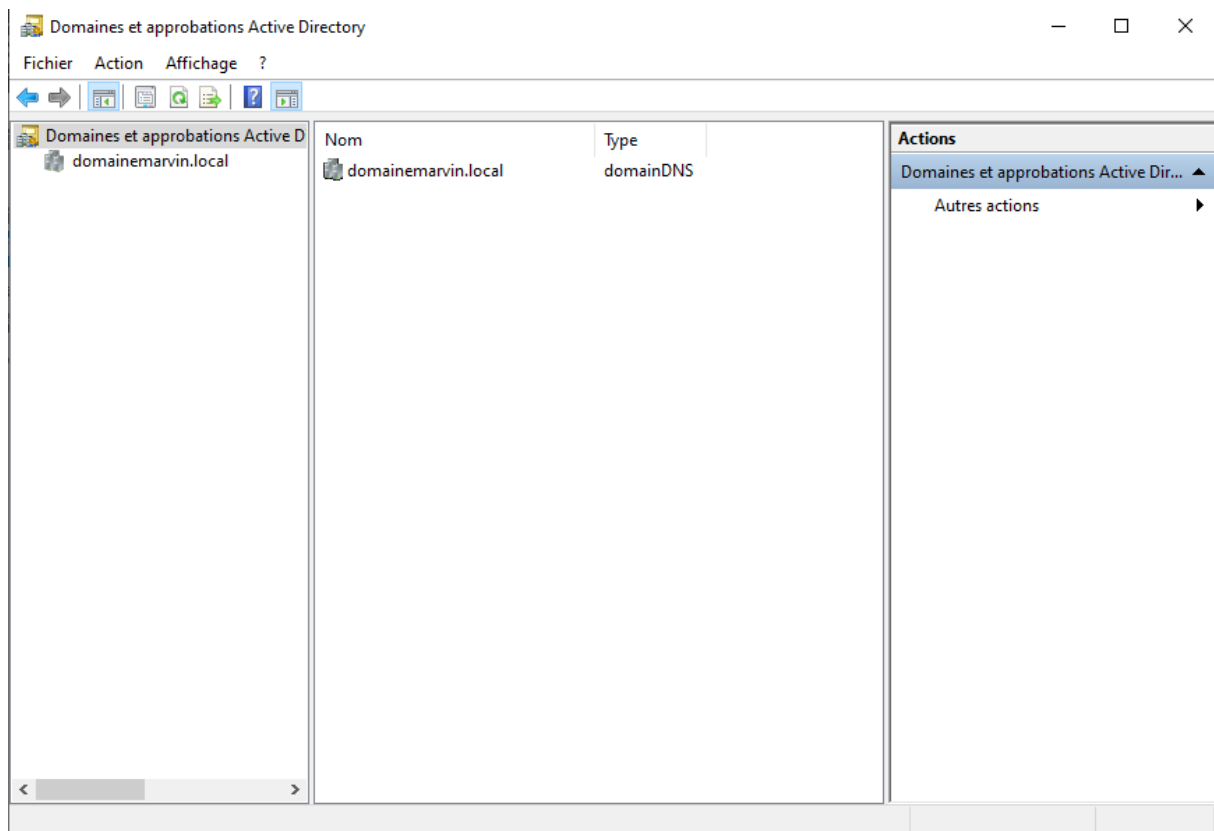
ensuite je vais créer mon Active Directory



A la fin de l'installation de l'Active Directory on a ce serveur



Je crée mon domaine domaineNom.local



Je retourne dans le gestionnaire de serveur de domaine et j'ajoute le rôle « Services et stratégie d'accès réseau »

Sélectionner des rôles de serveurs

SERVEUR DE DESTINATION
WIN-NL8IAEFJGE1.domainemarvin.local

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Confirmation

Résultats

Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.

Rôles

- ☐ Attestation d'intégrité de l'appareil
- ☐ Hyper-V
- ☐ Serveur de télécopie
- ☐ Serveur DHCP
- ☒ Serveur DNS (Installé)
- ☐ Serveur Web (IIS)
- ☐ Service Guardian hôte
- ☒ Services AD DS (Installé)
- ☐ Services AD LDS (Active Directory Lightweight Directory Services)
- ☐ Services AD RMS (Active Directory Rights Management Services)
- ☐ Services Bureau à distance
- ☐ Services d'activation en volume
- ☐ Services d'impression et de numérisation de documents
- ☐ Services de certificats Active Directory
- ☐ Services de fédération Active Directory (AD FS)
- ☒ Services de fichiers et de stockage (2 sur 12 installés)
- ☒ Services de stratégie et d'accès réseau (Installé)
- ☐ Services WSUS (Windows Server Update Services)
- ☐ Windows Deployment Services

Description

Les services de stratégie et d'accès réseau fournissent un serveur NPS (Network Policy Server) qui contribue à garantir la sécurité de votre réseau.

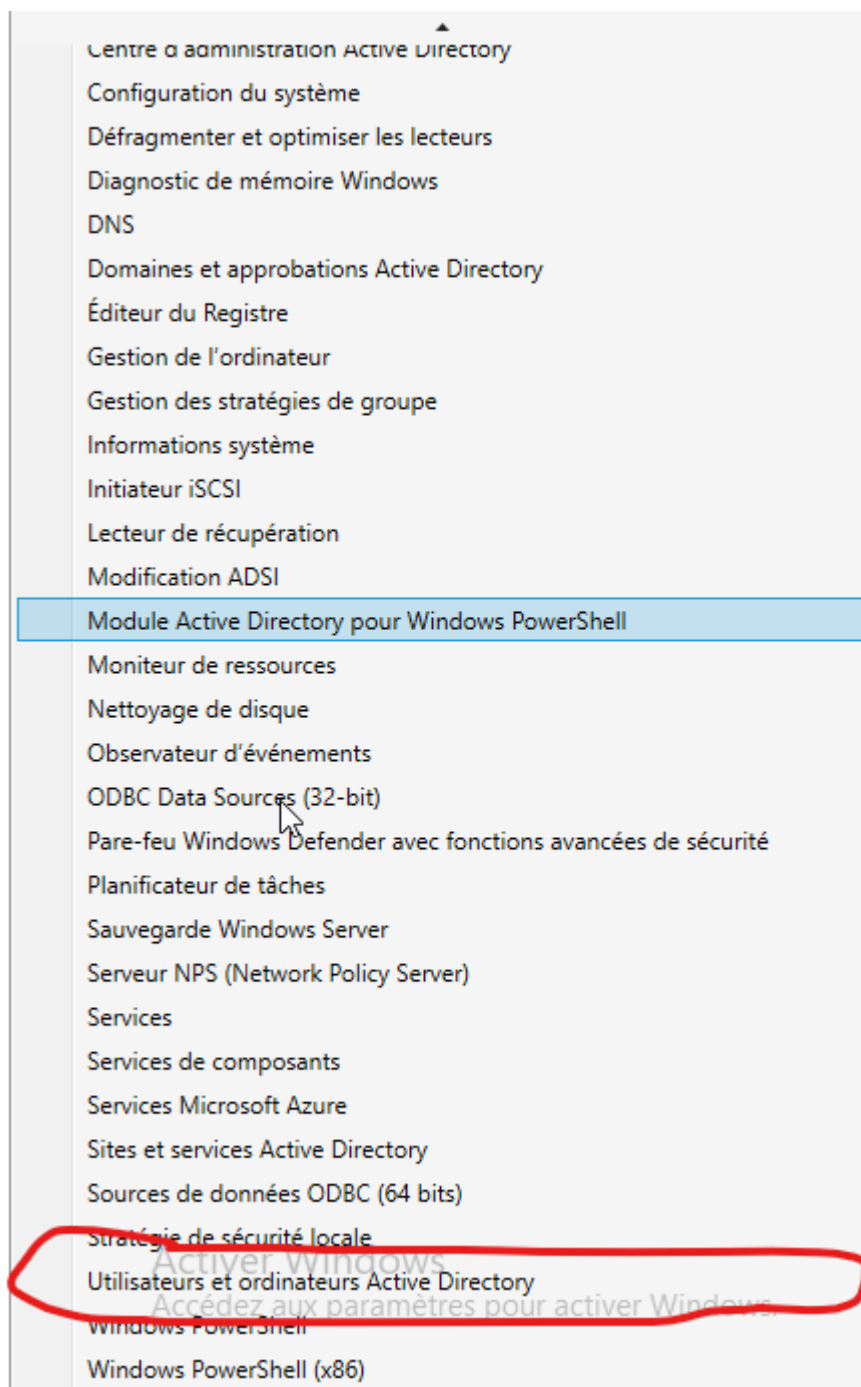
< Précédent

Suivant >

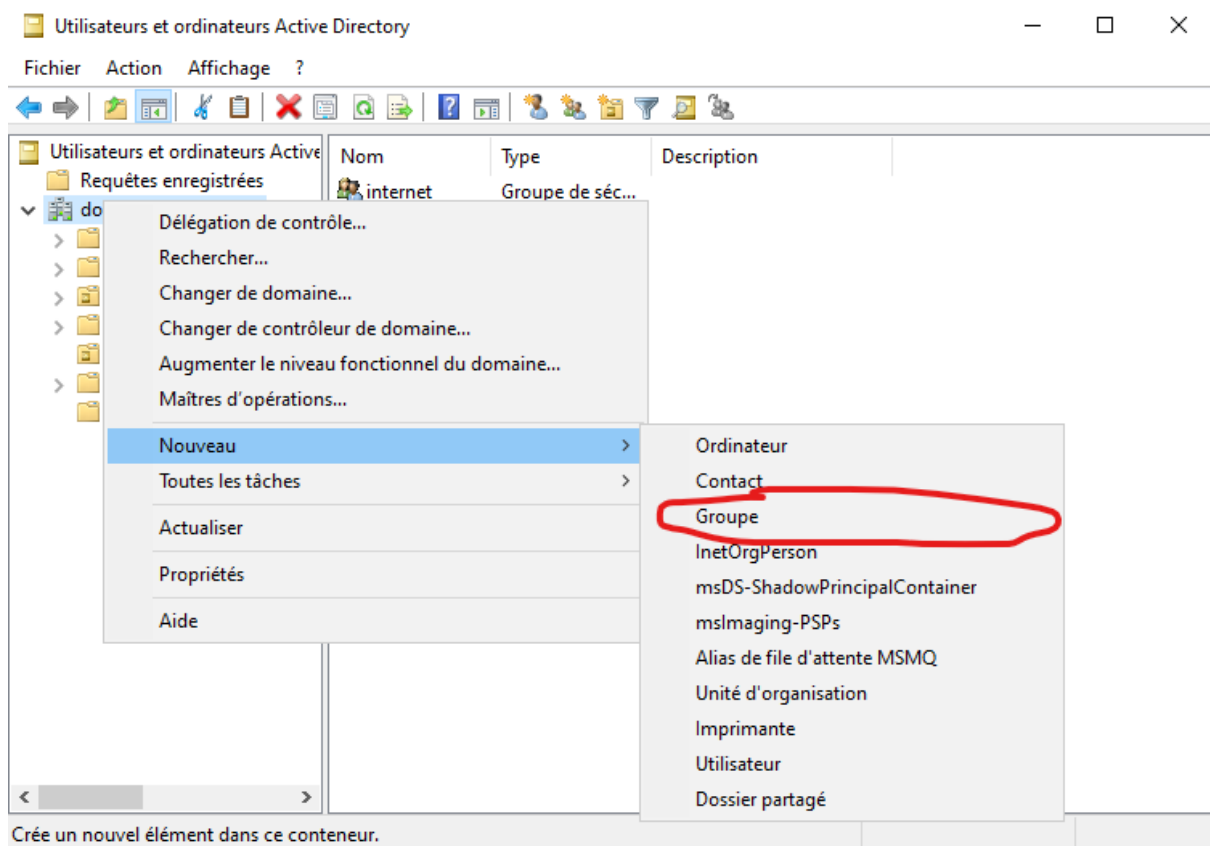
Installer

Annuler

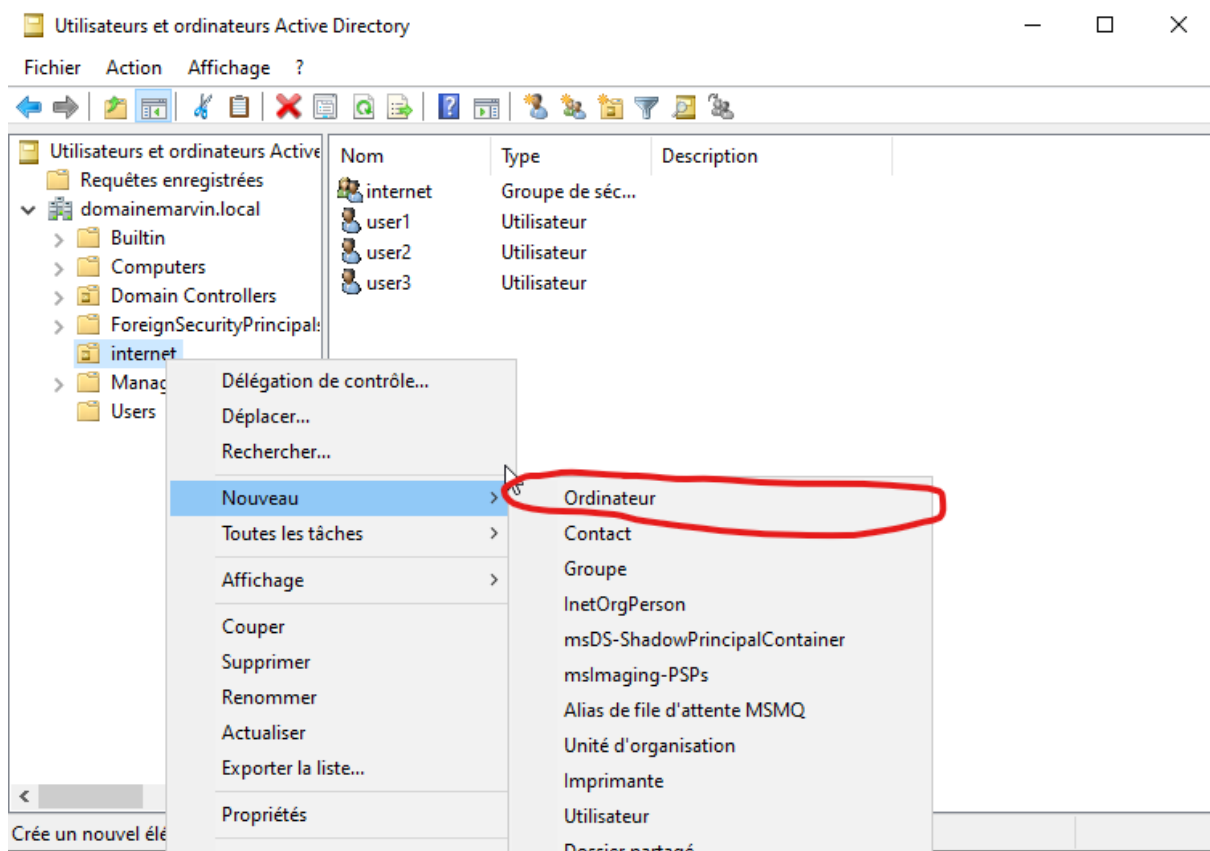
Je retourne dans le gestionnaire de serveur et je clique sur outils en haut à droite et ensuite sur Utilisateurs et Ordinateur Active Directory



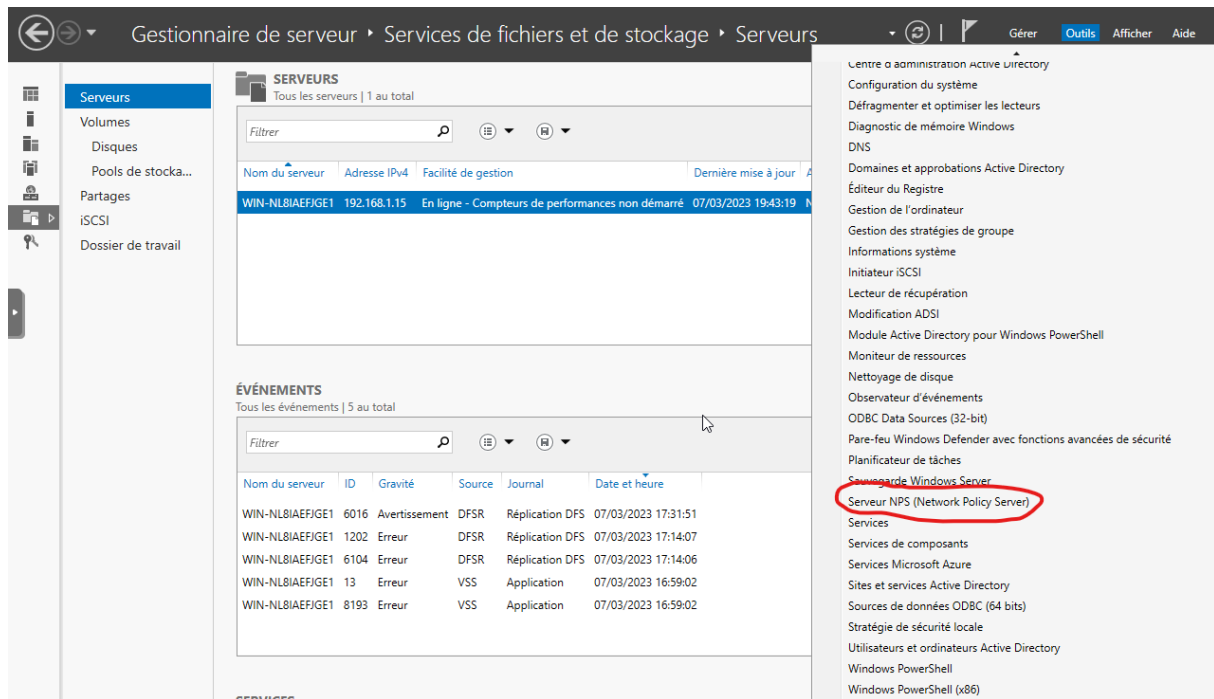
Je vais un groupe avec 3 utilisateurs qui seront soumis aux règles du proxy



Une fois le groupe créé je clique droit dessus et je crée mes 3 utilisateurs



Après avoir créé mon groupe avec mes utilisateurs je retourne dans le gestionnaire de serveur > Outils, et je clique sur serveur NPS



Je clique droit sur Client RADIUS et j'ajoute toutes les informations du Pfsense

Nouveau client RADIUS



Paramètres Avancé

☒ Activer ce client RADIUS

☐ Sélectionner un modèle existant :

Nom et adresse

Nom convivial :

Adresse (IP ou DNS) :

Vérifier...

Secret partagé

Sélectionnez un modèle de secrets partagés existant :

Pour taper manuellement un secret partagé, cliquez sur Manuel. Pour générer automatiquement un secret partagé, cliquez sur Générer. Vous devez configurer le client RADIUS avec le même secret partagé entré ici. Les secrets partagés respectent la casse.

☒ Manuel

☐ Générer

Secret partagé :

Confirmez le secret partagé :


OK

Annuler

Puis ensuite je crée une nouvelle stratégie réseaux

Nouvelle stratégie réseau

X



Spécifier le nom de la stratégie réseau et le type de connexion

Vous pouvez spécifier le nom de votre stratégie réseau ainsi que le type des connexions auxquelles la stratégie s'applique.

Nom de la stratégie :

Méthode de connexion réseau

Sélectionnez le type de serveur d'accès réseau qui envoie la demande de connexion au serveur NPS. Vous pouvez sélectionner une valeur dans Type de serveur d'accès réseau ou bien Spécifique au fournisseur, mais ces paramètres ne sont pas obligatoires. Si votre serveur d'accès réseau est un commutateur d'authentification ou un point d'accès sans fil 802.1X, sélectionnez Non spécifié.

☒ Type de serveur d'accès réseau :

▼

☐ Spécifique au fournisseur :

▲▼

Précédent

Suivant

Terminer

Annuler



Spécifier les conditions

Spécifiez les conditions qui déterminent si cette stratégie réseau est évaluée pour une demande de connexion. Au minimum, une condition est nécessaire.

Sélectionner une condition



Sélectionnez une condition, puis cliquez sur Ajouter.

Groupes



Groupes Windows

La condition Groupes Windows spécifie que l'utilisateur ou l'ordinateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.



Groupes d'ordinateurs

La condition Groupes d'ordinateurs spécifie que l'ordinateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.



Groupes d'utilisateurs

La condition Groupes d'utilisateurs spécifie que l'utilisateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.

Restrictions relatives aux jours et aux heures



Restrictions relatives aux jours et aux heures

Les restrictions relatives aux jours et aux heures indiquent les jours et les heures auxquels les tentatives de connexion sont autorisées ou non. Ces restrictions sont basées sur le fuseau horaire du serveur NPS (Network Policy Server).

Ajouter...

Annuler

Ajouter...

Modifier...

Supprimer

Précédent

Suivant

Terminer

Annuler



Spécifier les conditions

Spécifiez les conditions qui déterminent si cette stratégie réseau est évaluée pour une demande de connexion. Au minimum, une condition est nécessaire.

Sélectionner une condition

✕

Sélectionnez une condition

Groupes

Groupes Windows
La condition Groupes Windows doit appartenir à l'un des groupes sélectionnés.

Groupes d'ordinateur
La condition Groupes d'ordinateur doit appartenir à l'un des groupes sélectionnés.

Groupes d'utilisateurs
La condition Groupes d'utilisateurs doit appartenir à l'un des groupes sélectionnés.

Restrictions relatives aux connexions
Les restrictions relatives aux connexions sont au minimum une condition (Policy Server).

Groupes d'utilisateurs

Spécifiez l'appartenance aux groupes nécessaire pour correspondre à cette stratégie.

Groupes
DOMAINEMARVIN\internet

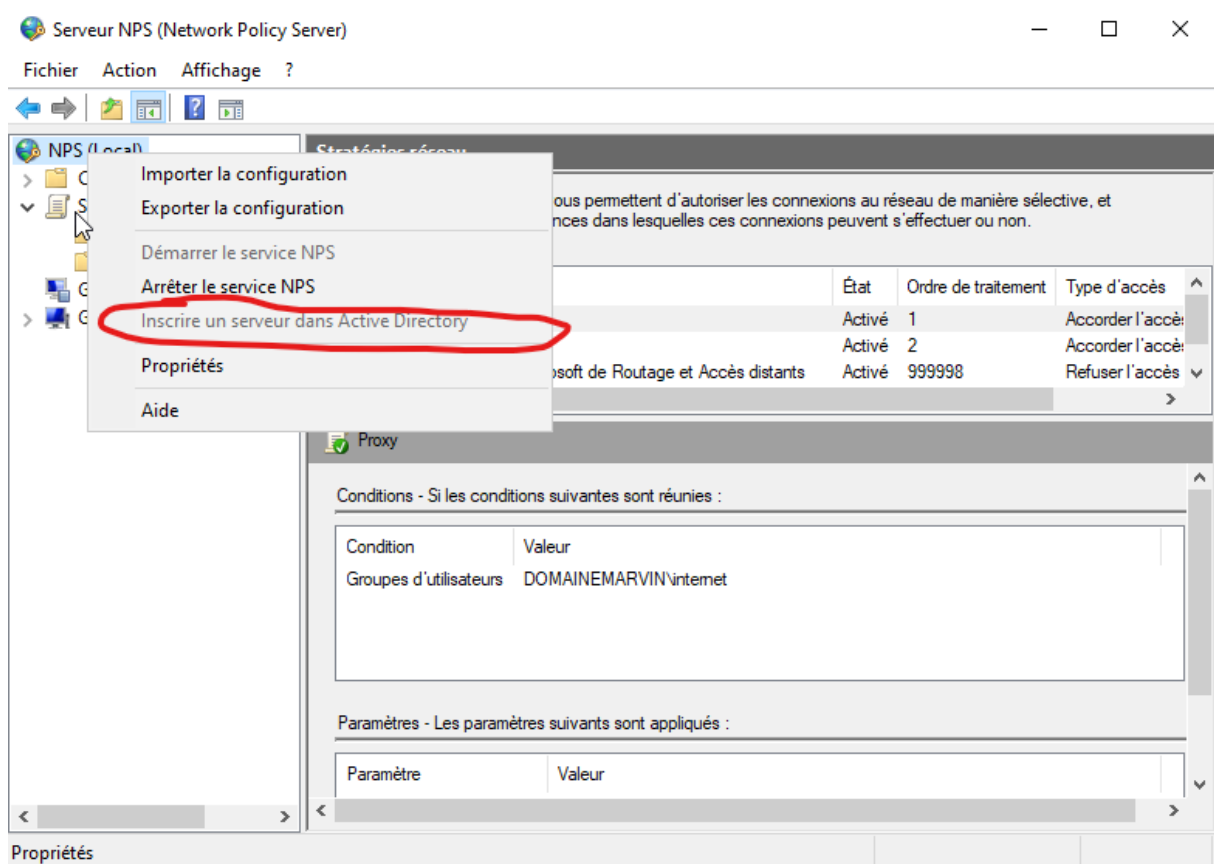
Ajouter des groupes... Supprimer OK Annuler

Ajouter... Modifier... Supprimer

Précédent Suivant Terminer Annuler

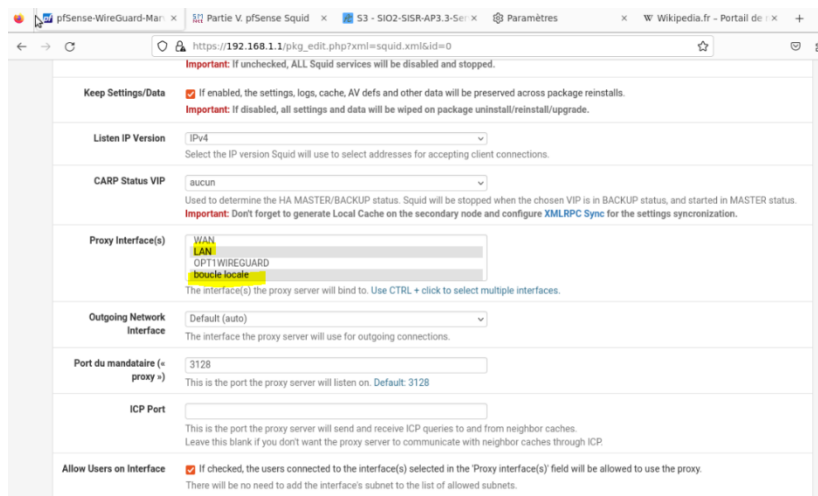
Ensuite suivant, suivant , suivant et terminer

Une fois la création je clique droit sur serveur NPS > Inscrire un serveur dans Active Directory

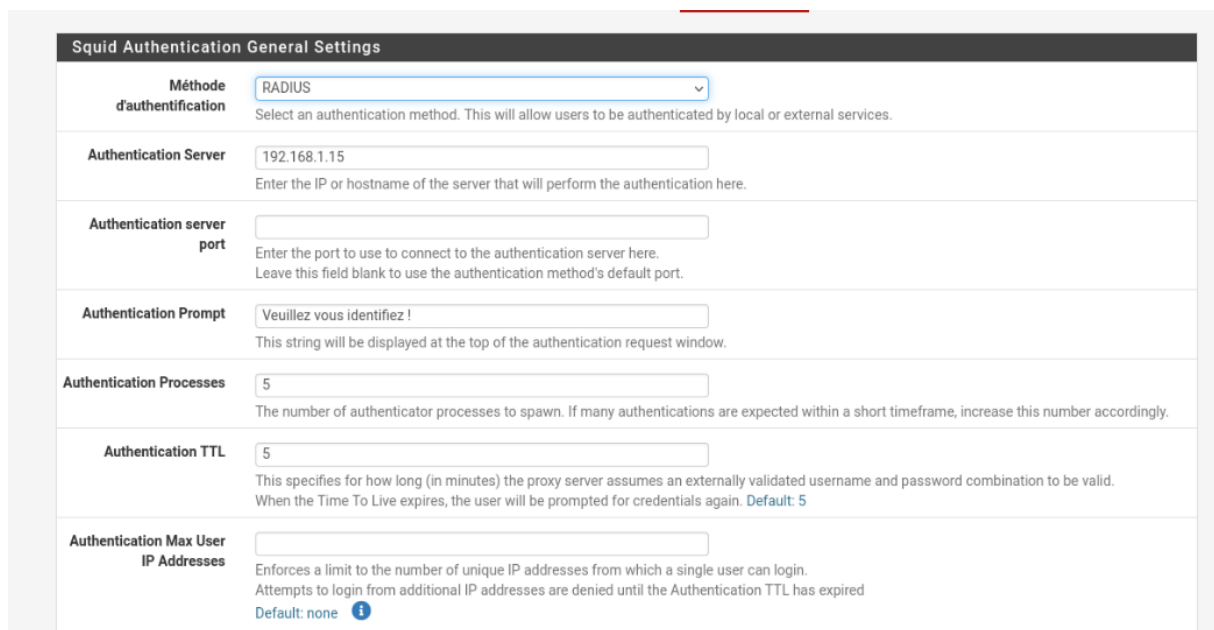


Proxy authentifié RADIUS sous pfsense

Je dois paramétrer l'authentification radius sous pfsense. Je vais modifier la configuration proxy de squid proxy server en rajoutant boucle local :



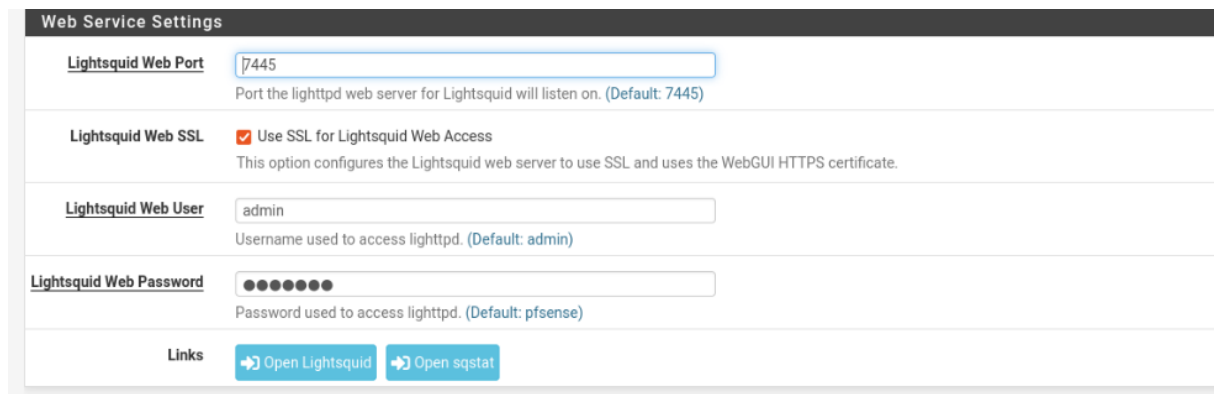
Ensuite je paramètre l'authentification RADIUS en y ajoutant l'adresse ip de windows server :



Squid Authentication General Settings

Méthode d'authentification	<input type="text" value="RADIUS"/>	Select an authentication method. This will allow users to be authenticated by local or external services.
Authentication Server	<input type="text" value="192.168.1.15"/>	Enter the IP or hostname of the server that will perform the authentication here.
Authentication server port	<input type="text"/>	Enter the port to use to connect to the authentication server here. Leave this field blank to use the authentication method's default port.
Authentication Prompt	<input type="text" value="Veuillez vous identifier !"/>	This string will be displayed at the top of the authentication request window.
Authentication Processes	<input type="text" value="5"/>	The number of authenticator processes to spawn. If many authentications are expected within a short timeframe, increase this number accordingly.
Authentication TTL	<input type="text" value="5"/>	This specifies for how long (in minutes) the proxy server assumes an externally validated username and password combination to be valid. When the Time To Live expires, the user will be prompted for credentials again. Default: 5
Authentication Max User IP Addresses	<input type="text"/>	Enforces a limit to the number of unique IP addresses from which a single user can login. Attempts to login from additional IP addresses are denied until the Authentication TTL has expired. Default: none

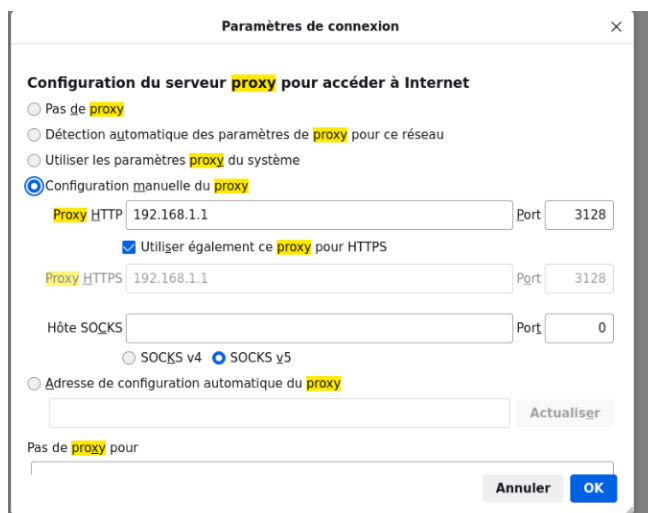
Puis on modifie le paramétrage dans squid proxy report en y ajoutant le port et le mot de passe :



Web Service Settings

Lightsquid Web Port	<input type="text" value="7445"/>	Port the lighttpd web server for Lightsquid will listen on. (Default: 7445)
Lightsquid Web SSL	<input checked="" type="checkbox"/> Use SSL for Lightsquid Web Access	This option configures the Lightsquid web server to use SSL and uses the WebGUI HTTPS certificate.
Lightsquid Web User	<input type="text" value="admin"/>	Username used to access lighttpd. (Default: admin)
Lightsquid Web Password	<input type="password" value="••••••"/>	Password used to access lighttpd. (Default: pfsense)
Links	➔ Open Lightsquid ➔ Open sqstat	

Enfin on modifie le parametre proxy de notre navigateur internet comme ceci :



Paramètres de connexion

Configuration du serveur proxy pour accéder à Internet

- ☐ Pas de proxy
- ☐ Détection automatique des paramètres de proxy pour ce réseau
- ☐ Utiliser les paramètres proxy du système
- ☒ Configuration manuelle du proxy

Proxy HTTP **Port**

☒ Utiliser également ce proxy pour HTTPS

Proxy HTTPS **Port**

Hôte SOCKS **Port**

☐ SOCKS v4 ☒ SOCKS v5

☐ Adresse de configuration automatique du proxy

Actualiser

Pas de proxy pour

Annuler **OK**

Enfin on essaie de se connecter à un site internet par exemple wikipedia et là il nous demander les logs des utilisateurs qu'on à paramétrer avant :



Authentification requise - Mozilla Firefox

Le proxy moz-proxy://192.168.1.1:3128 demande un nom d'utilisateur et un mot de passe. Le site indique : « Veuillez vous identifier ! »

Nom d'utilisateur

Mot de passe

Annuler Connexion

Puis sa nous affiche notre page :

