NOLAN MASSOT
T°SN RISC

MÉMOIRE DE STAGE

2022/2023

LOONIX

REMERCIEMENTS

Je tiens à remercier toutes les personnes qui ont contribué au succès de mon stage et qui m'ont aidé lors de la rédaction de ce rapport.

Je tiens à remercier vivement mon maître de stage, Serge FEVRE, gérant de l'entreprise Loonix, pour son accueil, le temps passé ensemble et le partage de son expertise au quotidien. Grâce aussi à sa confiance, j'ai pu m'accomplir totalement dans mes missions. Il fut d'une aide précieuse dans les problèmes auxquels j'ai pu faire face.

Je remercie également Céline et Dominique pour leur accueil et leur esprit d'équipe.

Merci Beaucoup !

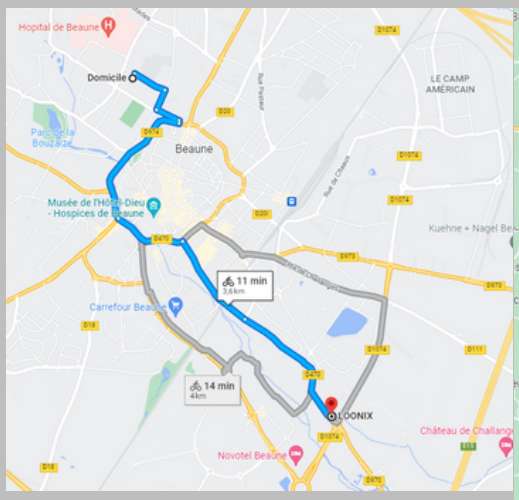
LOONIX®
SERVICES INFORMATIQUES

SOMMAIRE

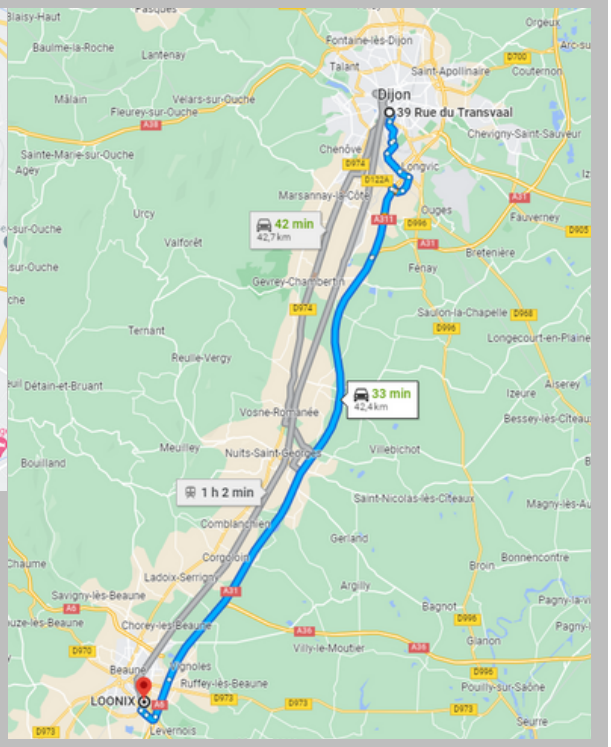
PRÉSENTATION DE L'ENTREPRISE

Situation géographique :

L'entreprise Loonix se situe 45 Routes de Verdun à BEAUNE 21200.



De mon domicile à l'entreprise



De l'entreprise au lycée Saint-Joseph-La-Salle

Historique :

Le 1er octobre 2007 l'entreprise Loonix a vu le jour, elle est toujours active depuis 15 ans.

Le gérant de l'entreprise est Serge FEVRE et son équipe est constituée de 2 autres salariés: Céline et Dominique.

PRÉSENTATION DE L'ENTREPRISE

Type D'activité :

Loonix est une entreprise dont le secteur d'activité est les réseaux informatique et l'installation de périphériques faisant partie du réseau. (Code NAF 9511Z)

Organigramme présentant la hiérarchie du personnel :

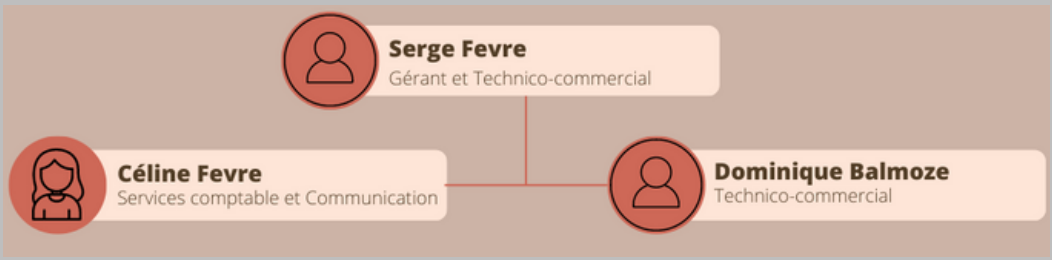
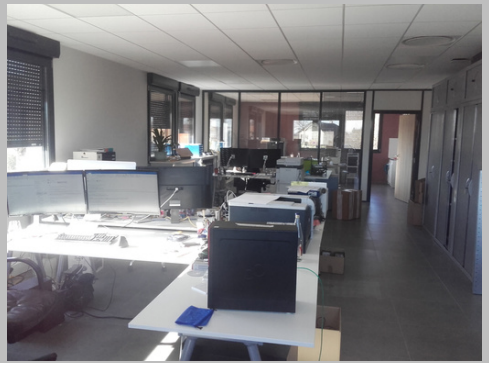


Photo des locaux de l'entreprise :



ACTIVITÉ 1 :

Installation de 6 bornes WIFI dans l'entreprise Dégustation Sélection :

Préalablement, Serge m'a demandé d'accéder au site web Nebula avec le compte de l'entreprise et de créer un site "Dégustation Sélection" ensuite, je peux ajouter des périphériques. (borne wifi)

Borne Wifi ZyXel

Pour faire cela, il faut entrer le numéro de série et l'adresse MAC de chaque borne, ensuite je continue la configuration de chaque borne wifi en changeant leurs noms par VINOPARC-... Et en effectuant toutes les mises à jour.

Le site Nebula permet de configurer tous les appareils de la marque, de gérer toutes les mises à jour, voir si les appareils sont en ligne ou pas et voir tous les clients qui sont connectés et gérer la consommation...

nebula

ZYXEL

Installation des bornes à 10 mètres de haut dans l'entrepôt de Dégustation Sélection.

ACTIVITÉ 1 :

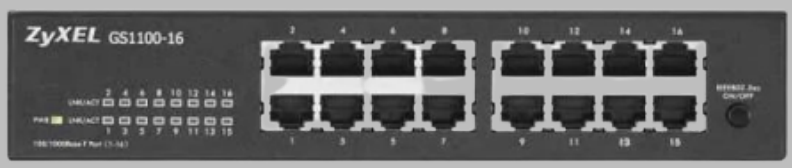
Borne wifi avec système Poe:

Power over Ethernet (PoE) est une technologie de réseaux locaux (LAN) Ethernet filaires qui fait passer le courant électrique nécessaire au fonctionnement de chaque appareil par les câbles de données, au lieu des cordons d'alimentation.

Cette technologie permet de diminuer le nombre de fils nécessaires à l'installation du réseau.

Auparavant, Serge et Dominique ont installé dans la baie de brassage de l'entreprise un switch Poe de la marque Zyxel, avec cela, le câble RJ45 transmet le réseau internet et l'électricité ce qui va nous faciliter la tâche pour installer les bornes, car il n'y a plus qu'un fil qui va être installé.

Le switch a une capacité de 180 Watts et chaque borne WIFI a une consommation 30 Watts parfait pour le nombre de bornes que nous avons dû installer.



Switch ZyXEL GS1100-16 avec système Poe
(Power over Ethernet)

ACTIVITÉ 2 :

Forcer un mot de passe Wifi avec Kali/Linux et un logiciel Brut Force:

Qu'est-ce que le Wi-Fi ?

Le Wi-Fi est une technologie de réseau sans fil qui permet aux périphériques tels que des ordinateurs (portables et fixes), des périphériques mobiles (téléphones intelligents et dispositifs portables), et d'autres équipements (imprimantes et caméras vidéo) d'accéder à Internet. Il permet à ces appareils, et à de nombreux autres, d'échanger des renseignements entre eux, ce qui crée un réseau.

La connectivité Internet est rendue possible grâce à un routeur sans fil. Lorsque vous accédez au Wi-Fi, vous vous connectez à un routeur sans fil, qui permet à vos appareils compatibles avec le Wi-Fi d'accéder à Internet.

Quels sont les types de sécurités d'un WIFI ?

WEP, WPA et WPA 2 (du plus ancien au plus récent) sont tous trois des protocoles de sécurité des réseaux internet sans fil. Il vise à restreindre l'accès à un réseau WiFi grâce à leur technologie de cryptage.

WEP (Wired Equivalent Privacy)

WPA (Wi-Fi Protected Access)

Depuis 2018, un nouveau protocole de sécurité est sorti le WPA3 encore plus fort que le WPA2, mais reste discret.Il n'est pas connu de tous, car la plupart de nos appareils ont toujours le protocole WPA2.

ACTIVITÉ 2 :

Logiciel Brut Force :

Qu’est-ce qu’une attaque par bruteforce ?

Une attaque par bruteforce, ou force brute en français, est une méthode de craquage de mots de passe que les cybercriminels utilisent pour déterminer les informations d'identification des comptes, en particulier les mots de passe.

Dans une attaque par force brute, l'attaquant dispose généralement d'un dictionnaire de termes et de mots de passe courants et les utilise pour “deviner” le mot de passe d'un utilisateur. Après avoir épuisé une liste de termes du dictionnaire, l'attaquant utilise des combinaisons de caractères jusqu'à trouver une correspondance.

Des milliers de tentatives peuvent être nécessaires avant qu'un mot de passe ne soit craqué, c'est pourquoi les attaquants utilisent des outils d'automatisation pour effectuer rapidement des milliers de tentatives.

Le logiciel bruteforce :

L'outil que j'ai utilisé pour mon attaque bruteforce est Aircrack-ng directement installé sur le système d'exploitation de bases Linux, Kali.Un système très protégé est pas mal utilisé par des cybercriminels, il y a énormément d'outils pour plein d'attaques différentes.

ACTIVITÉ 2 :

Explication de l'exercice :

Les équipements utilisés pour l'exercice :

- Un ordinateur portable DELL sous Kali Linux
- Une antenne Wi-Fi NETGEAR
- Un routeur sans fil Cisco
- Un câble RJ45
- Un téléphone connecté au routeur

IInstallation du routeur sur le réseau internet avec le câble Rj45. Sur le PC avec l'antenne branchée, lancer aircrack-ng, un terminal va apparaître tout çe fait par des commandes en mode administrateur (sudo). Dans un premier temps nous allons repérer notre antenne avec la commande iwconfig, puis nous allons mettre notre antenne en mode monitoring (le mode monitoring permet d'écouter tout le trafic d'un réseau sans fil sans avoir besoin d'associer la carte réseau à un routeur).

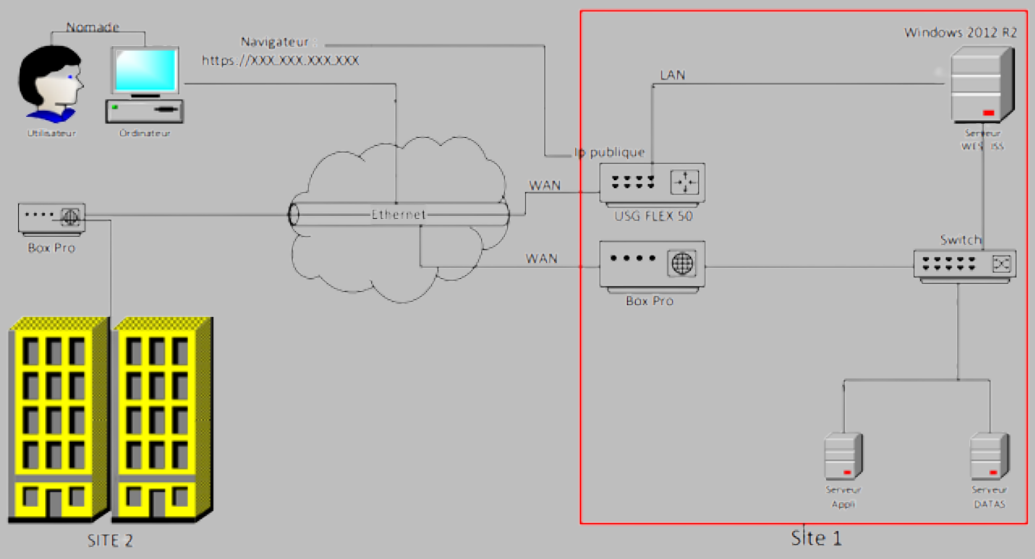
Cela nous permettra de voir le routeur que j'ai installé préalablement et connaître des informations sur celui-ci SSID, adresse MAC et adresse IP.
Ensuite, nous pourrons écouter les trames du routeur au téléphone, car grâce à aircrack-ng, on pourra décrypter pour trouver notre fameux mot de passe Wi-Fi.

Puis plus rien à faire le logiciel a été codé pour automatiser cette tâche.

ACTIVITÉ 3 :

Installation et configuration d'un serveur radius :

Mise en situation :



Je suis un utilisateur (nomade) et j'aimerais pouvoir me connecter au serveur de l'entreprise quand je suis chez moi (site 2) et quand je suis à l'entreprise (site 1) sans utiliser une connexion VPN qui coûte beaucoup trop chère.

C'est pour ça que je vais installer et configurer un serveur radius sous Windows Serveur 2012 et installer un pare-feu (client), cela permettra de protéger la connexion avec un mot de passe.

Avec ce protocole, l'utilisateur aura juste à rentrer l'IP publique du serveur dans son navigateur (https://ip publique) puis rentrer ses informations (nom d'utilisateur et mot de passe), configurés au préalable dans le serveur de l'entreprise.

ACTIVITÉ 3 :

Explication d'un Serveur Radius + avantages et inconvenients :

RADIUS est un protocole initialement conçu pour authentifier les utilisateurs distants d'un serveur avec accès par modem.

Il sert aujourd'hui dans un large éventail de scénarios d'authentification. RADIUS est un protocole client-serveur dont le routeur est le client et le serveur RADIUS le serveur. (Le client RADIUS est parfois appelé le Network Access Server ou NAS.)
Lorsqu'un utilisateur tente de s'authentifier, le périphérique envoie un message au serveur RADIUS. Si celui-ci est correctement configuré avec le périphérique comme client, RADIUS renvoie un message d'autorisation ou de refus au périphérique (le serveur d'accès au réseau).

Avantages :

- Sécurité forte : L’utilisation d’un certificat radius permet de demander à toute personne souhaitant se connecter au réseau de s’authentifier, il consiste à faire présenter un certificat électronique dont la validité sera vérifiée par le serveur. Chaque utilisateur aura son propre certificat. La transaction entre un client radius et le serveur radius est cryptée.

- Fiabilité : La méthode d’authentification par certificat est très fiable.

- Administré : Radius permet de centraliser des données d’authentification.

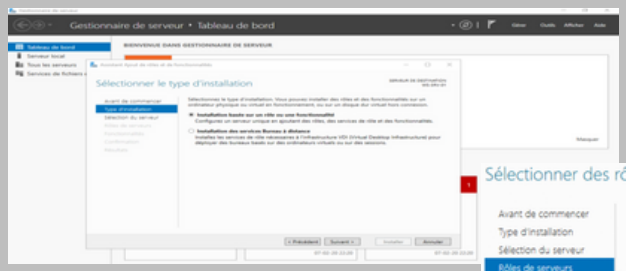
Inconvenients :

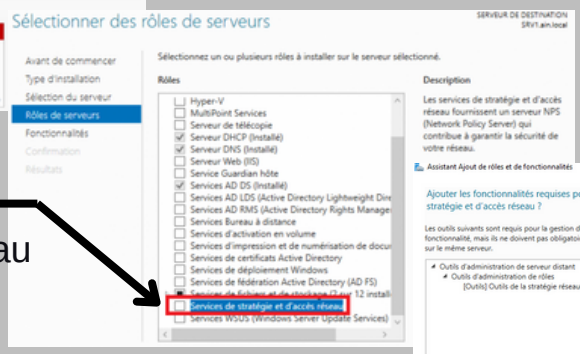
- Complexité de la solution

ACTIVITÉ 3 :

Installation et configuration de radius sur Windows Serveur 2012 R2:

Je commence ma configuration sur un serveur Windows 2012 R2 . Premièrement, je me rends sur le tableau de bord du gestionnaire de serveur pour installer le rôle NPS. (Network Policy Serveur) qui me permettra donc d'utiliser l'authentification RADIUS.





Chercher dans la liste, la fonctionnalité Service de stratégie et d'accès au réseau puis téléchargez la.

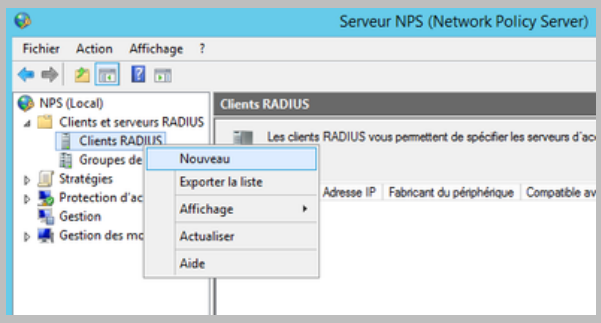
Maintenant, que le rôle est installé, nous allons devoir le configurer. Pour cela dans le gestionnaire de serveur, cliquez sur « Outils » puis sur « Serveur NPS (Network Policy Server) ».

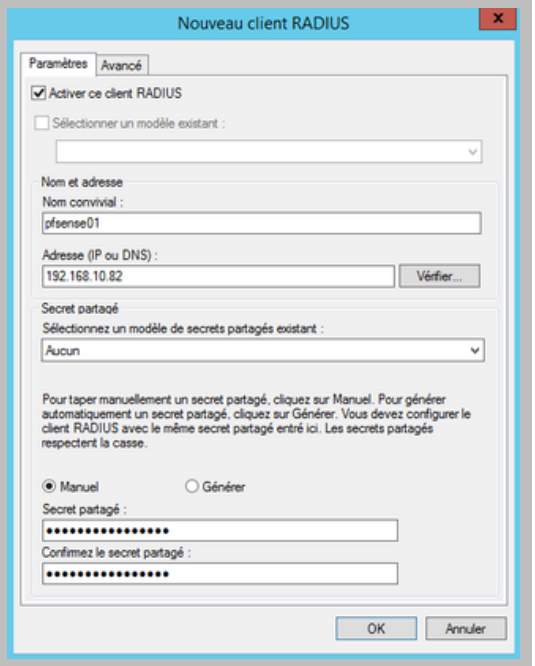
Windows Server 2012 R2

ACTIVITÉ 3 :

Configuration de radius sur Windows Serveur 2012 R2:

Quand le téléchargement prend fin, on se redirige sur Panneau de configuration - Outils d'administration - Serveur NPS (Network Policy Serveur) et nous allons ajouter un nouveau client pour cela. On va sur Clients et serveurs RADIUS - Clients RADIUS - Nouveau.





- Cocher : Activer ce client RADIUS
- Nom convivial : Nom du client (pare-feu)
- Adresse IP : Saisir l'IP du client
- Secret partagé : Indiquer un code qui sera partagé par le client et le serveur RADIUS

Création d'une nouvelle stratégie réseau :

Dans mon exemple, je vais autoriser un groupe de sécurité à s'authentifiez sur le serveur Radius
NPS (local) - Stratégies - Stratégies réseau - Cliquer droit Nouveau

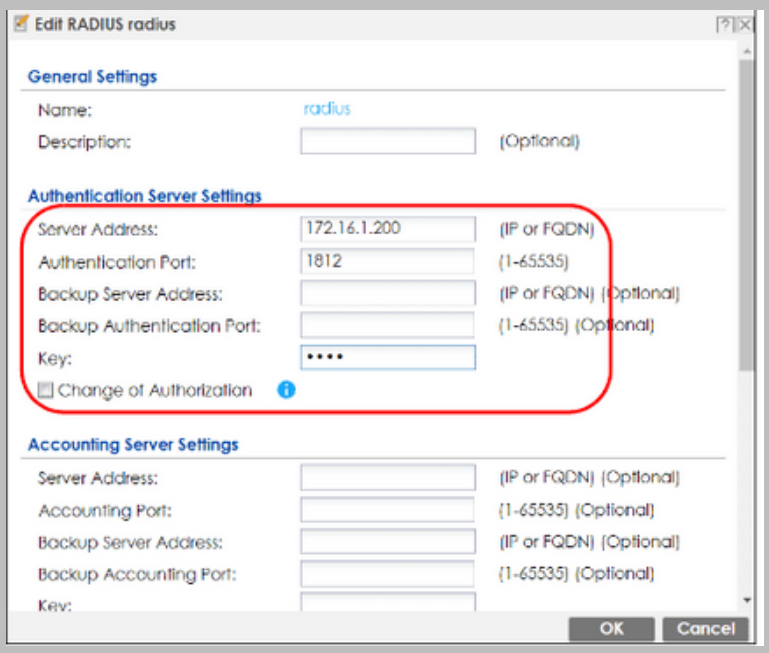
Ensuite, nous allons inscrire le serveur NPS sur active directory cela nous permettra de récupérer tous les utilisateurs que nous avons pu configurer et tous leurs groupes et leurs niveaux de privilèges.

ACTIVITÉ 3 :

Configuration de radius sur le pare-feu:

Nous allons définir l'authentification de l'utilisateur à l'aide du serveur RADIUS. Tout d'abord, configurez les paramètres du serveur RADIUS. Ensuite, configurez la méthode d'authentification et configurez le périphérique Zyxel pour utiliser la méthode d'authentification. Enfin, forcez les utilisateurs à s'authentifier.

Cliquez sur Configuration > Objet > AAA Server > RADIUS. Double-cliquez sur l'entrée du radius. Configurez l'adresse du serveur RADIUS, le port d'authentification (1812) et la clé. Cliquez sur OK.



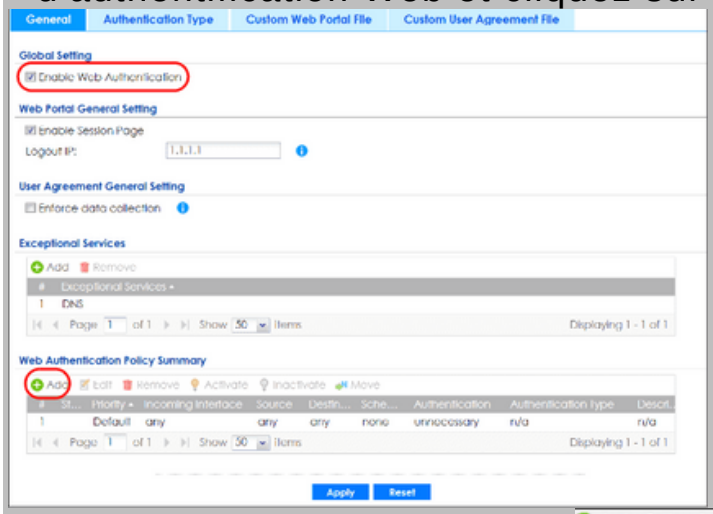
Nous venons de configurer le chemin que doit faire le pare-feu pour demander au serveur NPS si l'utilisateur et le mot de passe sont bons par rapport à ce qui est configuré dans l'active directory.

ACTIVITÉ 3 :

Configuration de radius sur le pare-feu:

Nous allons maintenant configurer le pare-feu pour que l'authentification soit forcée lors de la demande du nomade pour accéder au serveur. Et nous allons activer l'authentification web que propose Zyxel pour avoir un WEB Portail ce qui fera plus propre lors de l'enregistrement du compte.

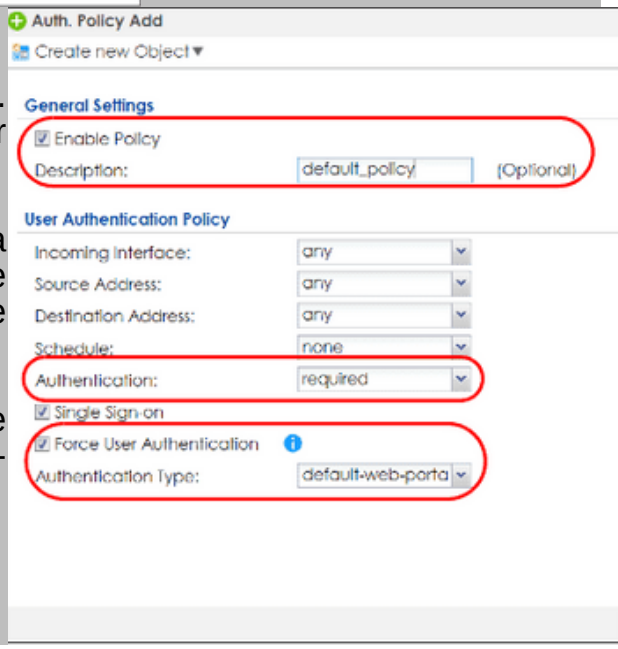
Cliquez sur Configuration > Authentification Web. Dans l'écran Authentification Web > Général, sélectionnez Activer l'authentification Web pour activer la fonction d'authentification Web et cliquez sur Appliquer.



Sélectionnez Activer, la politique. Saisissez un nom descriptif, par exemple « default_policy ».

Réglez le champ Authentication à required, et assurez-vous que Forcer l'authentification de l'utilisateur est sélectionné.

Sélectionnez un profil de type d'authentification (« default-web-portal »).



ACTIVITÉ 3 :

Conclusion de l'installation:

Les équipements utilisés pour l'exercice :

- Un ordinateur fixe Lenovo (nomade)
- Un serveur ThinkSystem ST550 (Windows serveur 2012 r2)
- Un pare-feu USG flex 50 Zyxel (client)

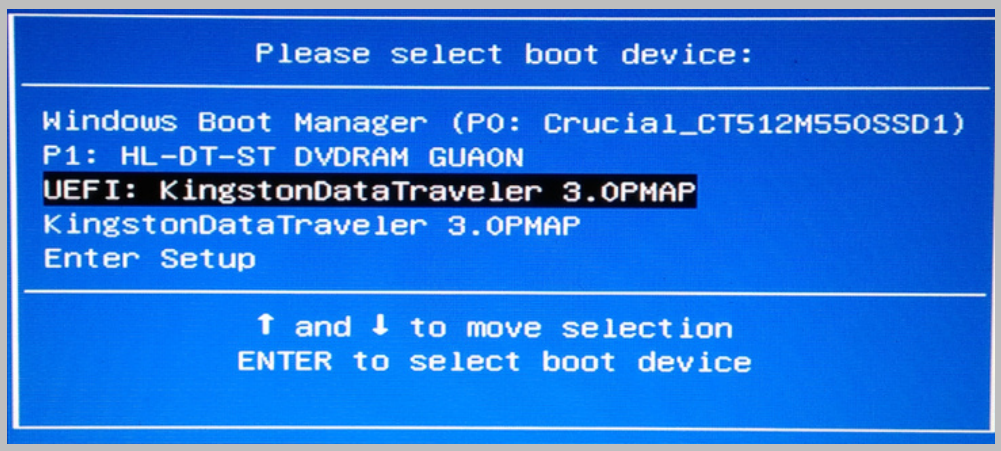
La configuration terminée sur le serveur Windows 2012 R2 et sur le pare-feu. Dès que l'on veut accéder à l'interface WEB du serveur IIS et que l'on tape dans la barre de recherche de notre navigateur l'adresse IP du serveur, on est bloqué par le client (pare-feu). Celui-ci va nous demander de nous authentifier pour y accéder. (on utilise le mot de passe et le nom d'utilisateur configurés préalablement dans l'active directory).

ACTIVITÉ 4 :

Installation du système d'exploitation IPfire sous Linux :

Premièrement, Serge, mon maître de stage, m'a prêté un ordinateur que je devais vérifier s'il fonctionnait et puis le réinitialiser. Après tout cela sur un autre PC, j'ai dû télécharger le fichier ISO du système d'exploitation et créer une clé bootable avec le logiciel Rufus.

Ensuite, sur le premier PC que j'ai préparé, j'ai branché la clé USB bootable. Tout en démarrant le PC, j'appuie plusieurs fois sur la touche F 12 pour accéder au boot menu. Sur la page du menu démarrage, apparaît toute la liste des périphériques sur lesquels je peux démarrer et je vois ma clé USB que je sélectionne pour commencer l'installation du système d'exploitation IPfire.



ACTIVITÉ 4 :

Configuration D'IPfire :

Après le démarrage de l'installation, je peux commencer la configuration, je sélectionne la langue, je formate le disque dur, je choisis la disposition du clavier, le fuseau horaire et je rentre un nom d'hôte (pour ma part, c'est Nolan-FW), un nom de domaine (Nolan.local) et je crée un mot de passe pour les utilisateurs root et admin.

Pour utiliser IPfire et crée un pare-feu, il faut installer deux cartes réseau au minimum dans un PC, car pour cet exercice, pour j'utilise la zone verte et rouge. (LAN et WAN)

Zone Rouge (WAN): la zone rouge est une zone sur laquelle nous n'avons aucun contrôle, et c'est là que viennent la plupart des menaces. Cette zone doit être séparée du reste du réseau interne par un pare-feu.

Zone Verte (LAN) : la zone verte est le cœur du réseau interne. C'est la zone avec le plus d'accès, principalement à Internet. Souvent, des proxy web de filtrage de pages et de détection de virus sont avantageusement installés pour réduire les risques de danger provenant d'Internet.

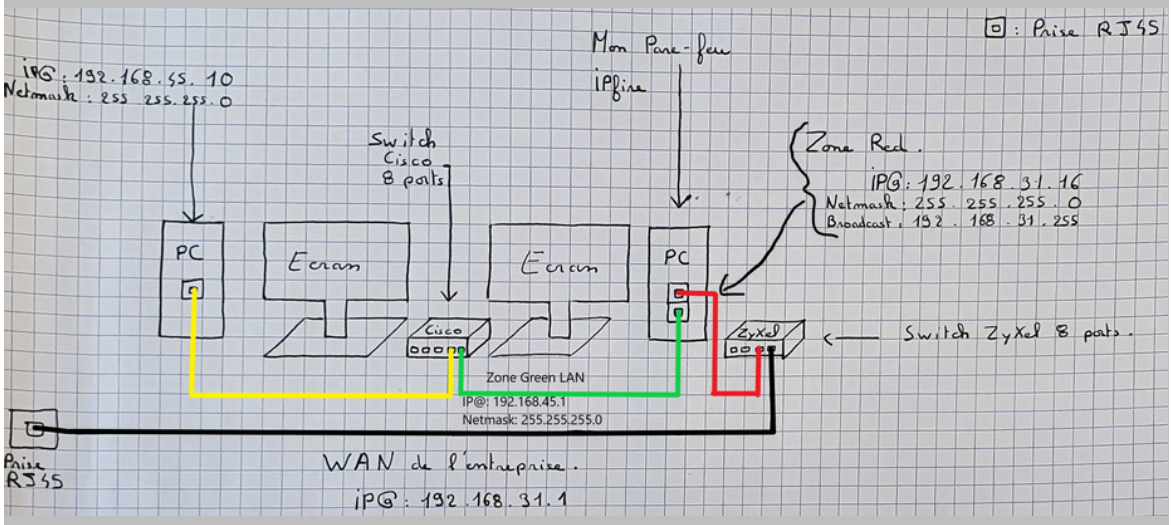
Zone Rouge (WAN): IP@= 192.168.31.1
Masque : 255.255.255.0

Zone Verte (LAN) :IP@=192.168.45.1
Masque : 255.255.255.0

ACTIVITÉ 4 :

Câblage :

Voici le câblage que j'ai effectué pour la création de réseau et mon pare-feu.



Après toutes les affectations des cartes réseau et adresse IP, le pare-feu démarre. Nous pouvons à présent accéder à l'interface Web D'IPfire.

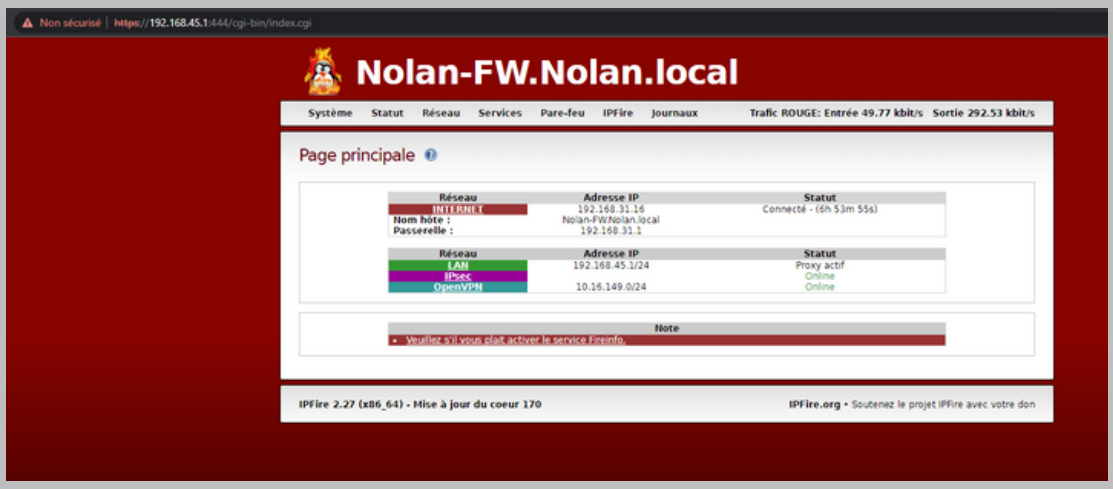
Pour y accéder, il faut taper dans la barre de recherche d'un navigateur https:// puis l'adresse IP que l'on a affecté à la zone verte et après :444.

Pour ma part c'est https://192.168.45.1:444

ACTIVITÉ 4 :

Interface Web D'IPfire :

Bien sûr, pour pouvoir entrer dans l'interface, il faut taper le code administrateur que nous avons préalablement choisi dans l'installation.



IPfire propose beaucoup de services:

_Open VPN.

_Proxy web.

_Serveur CRON.

_Serveur DHCP.

_Serveur NTP.

_Serveur Shell Sécurisé.

_Serveur de connexion.

_Serveur de journaux du noyau.

_Serveur proxy DNS.

_Serveur web.

_Système de détection d'intrusion.

_VPN.

Sur ces services, je vais choisir le proxy web pour filtrer le contenu URL.

ACTIVITÉ 4 :

Proxy Web :

Un serveur proxy est utile pour des raisons de cybersécurité et de performance, notamment pour anonymiser les adresses IP internes et mettre en cache le contenu afin d'améliorer la vitesse de transfert des données et de réduire l'utilisation de la bande passante.

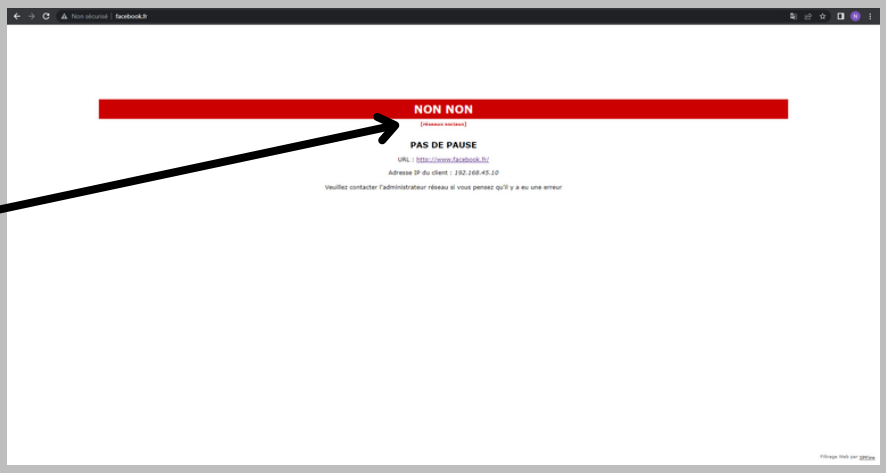
Exemple:

Les entreprises qui utilisent un serveur web proxy peuvent également l'utiliser pour filtrer le contenu qui ne doit pas être téléchargé sur le réseau de l'entreprise. Ces serveurs fonctionnent comme un intermédiaire entre le web et les appareils clients.

L'exercice que j'ai dû faire, était de configurer le proxy Web et le filtre URL pour que la zone LAN sortant que j'ai créé (192.168.45.1) n'accède pas aux sites comme "www.facebook.fr" et "www.lequipe.fr" et affiche un message d'erreur si quelqu'un veut entrer sur ces sites.

Vous pouviez voir dans l'annexe page 18
la configuration que j'ai effectuée.

Voici le résultat quand j'ai voulu me rendre sur le site de "Facebook":



Il détecte le type de contenu ici les réseaux sociaux. Pour l'équipe ce sera presse.

CONCLUSION

Conclusion :

Pour cette dernière année de stage auprès de l'entreprise Loonix et surtout Serge fût un exellent "mentor" pour moi car grâce à lui, j'ai pu acquérir beaucoup de connaissances techniques sur la profession.

Depuis la 3ème où j'ai effectué mon stage découverte dans son entreprise, il m'a permis de trouver ma voie et d'avoir plus confiance en moi.

Tous les exercices que j'ai pu effectuer ont tous été constructifs et cela m'a permis de choisir le métierque j'aimis exercer plus tard.

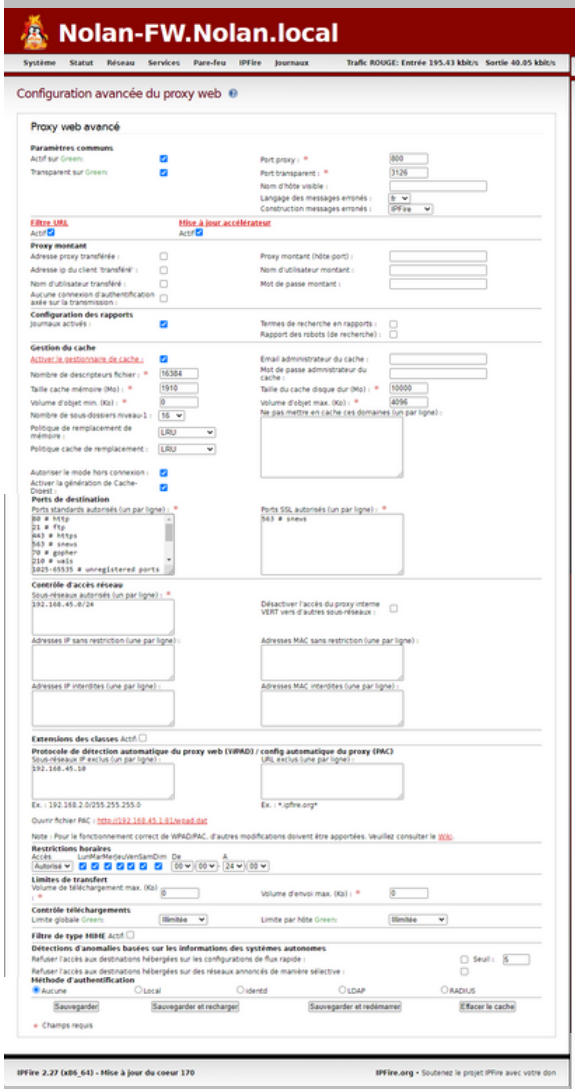
Je remercie encore et toujours Serge, Céline et Dominique pour leur accueil et les moments partagés tout le long du stage.

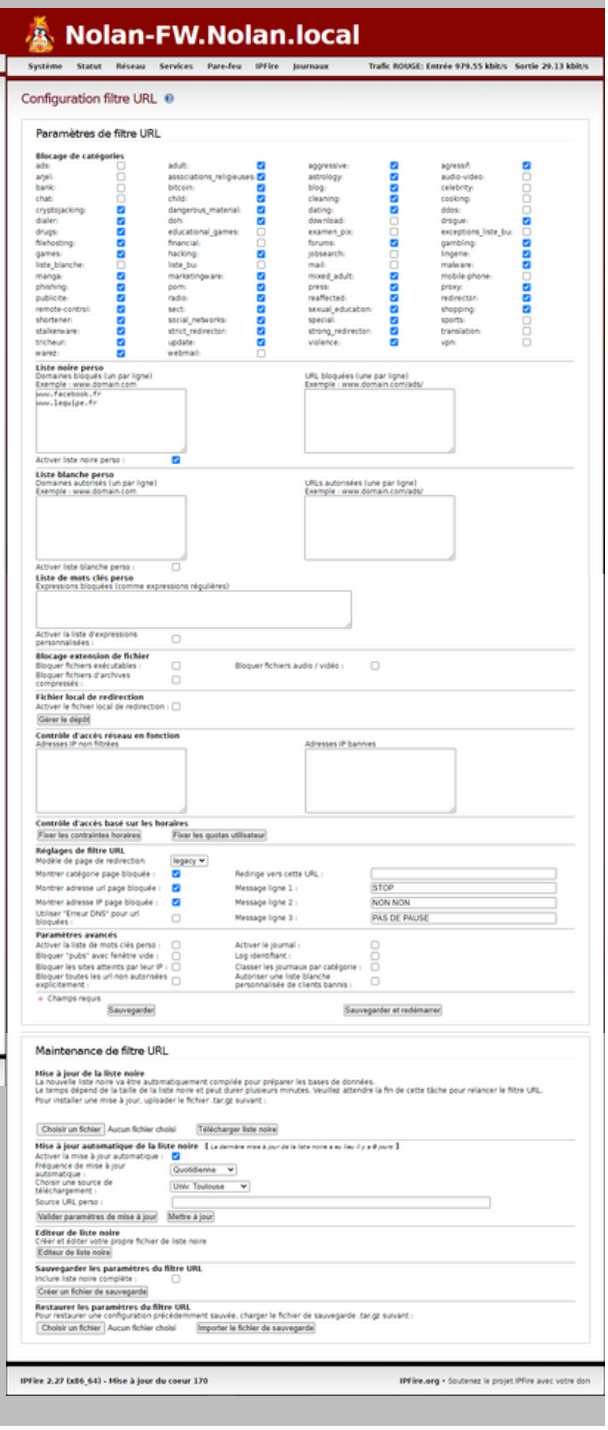
LOONIX®
SERVICES INFORMATIQUES

Saint Joseph-La Salle
DIJON
Frères des Écoles Chrétiennes

ANNEXES

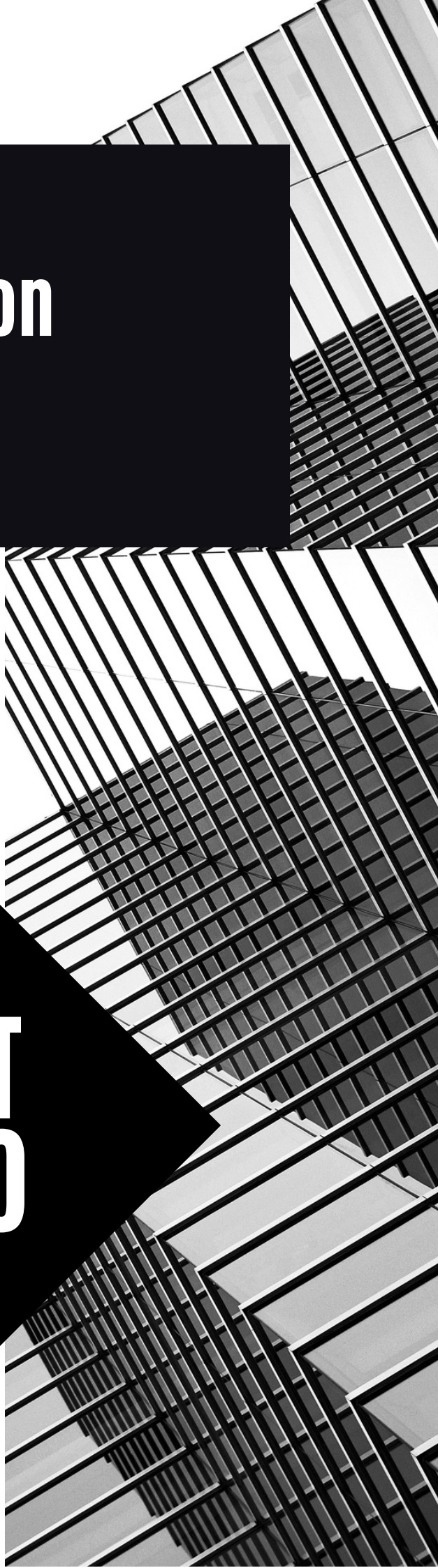
Configuration ProxyWeb et Filtre URL





Merci d'avoir lu mon mémoire

26/09/2022 au 21/10/2022
09/01/2023 au 03/02/2023



ST JO

PROPOSÉ PAR

Nolan MASSOT

PROPOSÉ À

L'équipe Saint Joseph et l'entreprise Loonix