GBS – Portail Captif

Chef de projet : RUGGERI Anthony

Equipier : HATCHUEL Jules

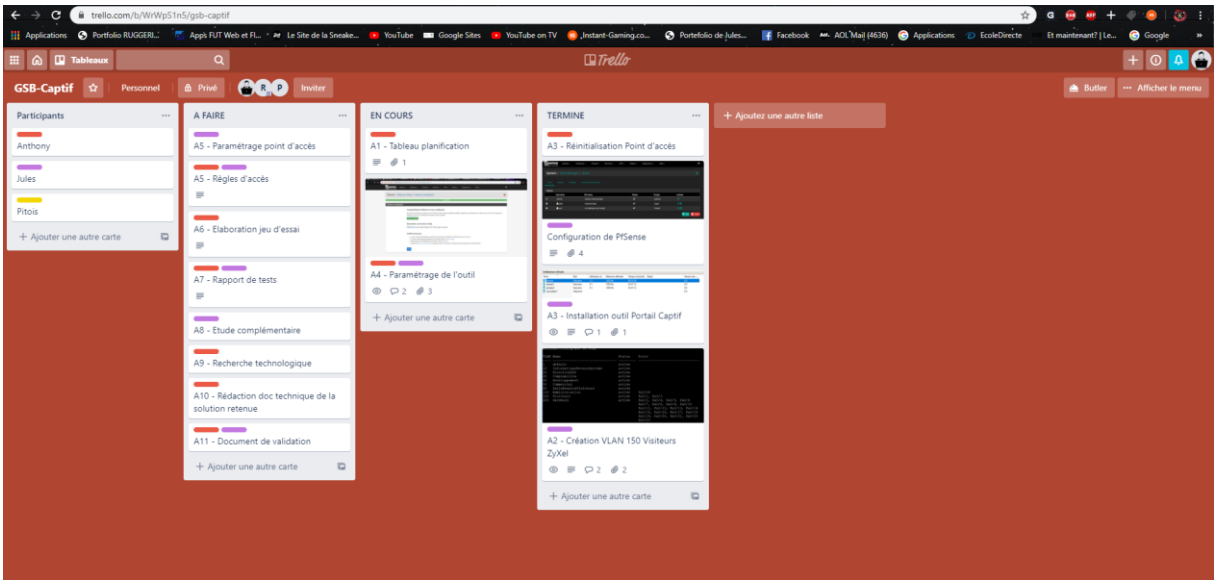
Date de projet : du 22/11/2019 au 20/12/2019

Descriptif : GSB sensibilisée aux problèmes de sécurité de ses accès réseau externes a lancé depuis peu un projet portant sur la mise en place d'un outil permettant la gestion de ses accès Wifi. Le DSI vous propose de mettre en place un accès Wifi réservé aux visiteurs médicaux. Ce SSID nommé « visiteur » redirigera vers un portail captif.

A1.4.1 Participation à un projet

C1.4.1.1 Établir son planning personnel en fonction des exigences et du déroulement du projet

Lors de la répartition des tâches au sein de notre projet, nous avons utilisé l'outil Trello afin de pouvoir obtenir une vision globale sur l'ensemble des missions à réaliser. L'intérêt étant de répartir de manière équitable le temps de travail.



C1.4.1.2 Rendre compte de son activité

Durant chaque fin de séance, nous devions rédiger et actualisé nos missions. Dès lors qu'une mission était prise en charge il fallait rédiger un descriptif de toutes nos actions qui ont permis de remplir la tâche en question. Tous les petits comptes rendus ont été vérifier par notre professeur afin de pouvoir garder un œil sur l'avancement de notre projet.

A1.1.1 Analyse du cahier des charges d'un service à produire

C1.1.1.2 Identifier les fonctionnalités attendues du service à produire

La connexion au SSID devra rediriger les visiteurs médicaux vers un portail captif mis en place par notre groupe au préalable. La fonctionnalité principale de ce portail est de forcer les clients à passer par une page HTML obligatoire pour s'authentifier avant de pouvoir naviguer sur internet. Le but étant de créer un support d'authentification et de pouvoir contrôler chaque connexion au SSID.

A1.1.3 Étude des exigences liées à la qualité attendue d'un service

C1.1.3.2 Recenser et caractériser les exigences de sécurité pour le service à produire

A3.1.3 Prise en compte du niveau de sécurité nécessaire à une infrastructure

C3.1.3.2 Proposer une solution de sécurité compatible avec les contraintes techniques, financières, juridiques et organisationnelles

C3.1.3.3 Décrire une solution de sécurité et les risques couverts

Nous avions plusieurs contraintes et exigences en matière de sécurité ainsi que sur un aspect plus juridique.

- Doter l'entreprise d'un portail libre et gratuit de contrôle d'accès à Internet pour la consultation web des visiteurs.

- Pour offrir un maximum de sécurité le point d'accès devra être isolé dans un VLAN, Vlan 150 nommé Visiteurs.

- Le point d’accès se trouvera dans la salle de réunion du 2ème étage.

- Pour l'aspect réglementaire et juridique :

Si dans le cadre d'une enquête judiciaire l'Officier de Police judiciaire sous réquisition du procureur de la république demande les informations de connexion, il faudra fournir les fichiers log des usagers qui correspondent à la date de l'infraction pour répondre aux obligations légales.

A5.2.4 Étude d‘une technologie, d’un composant, d’un outil ou d’une méthode

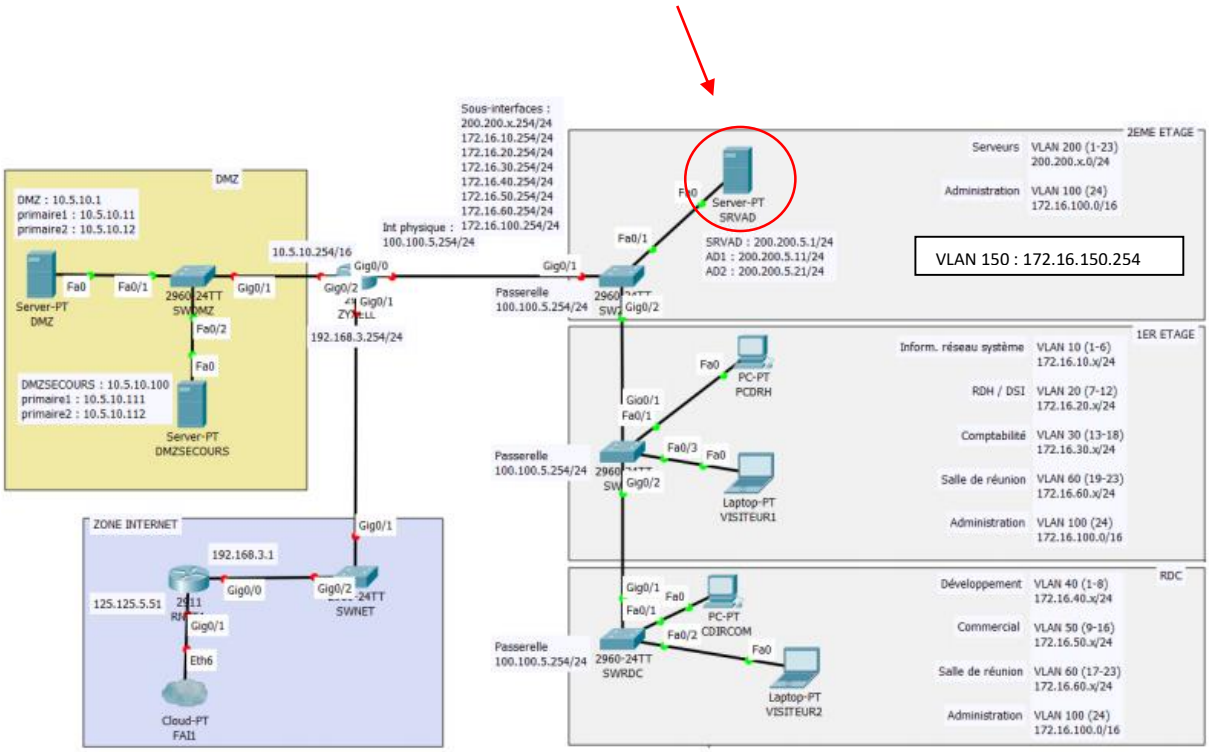
C5.2.4.1 Se documenter à propos d‘une technologie, d’un composant, d’un outil ou d’une méthode

Afin de commencer ce projet dans les meilleures conditions, il a fallu nous renseigner sur internet pour la conception initiale d’un portail captif. De plus les recherches sur la configuration de la borne wifi ou de PfSense nous permettent de ne pas être perdu en arrivant sur les missions concernant ces outils.

A1.1.2 Étude de l’impact de l’intégration d’un service sur le système informatique

C1.1.2.2 **Recenser les composants de l’architecture technique sur lesquels le service à produire aura un impact**

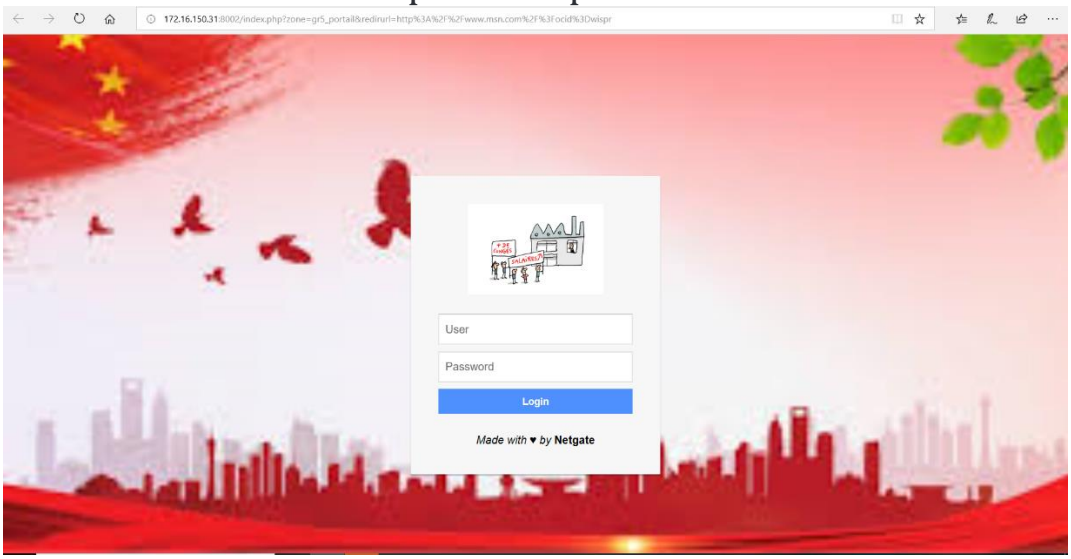
Sur la modification apportée a notre maquette, nous avons dû créer un nouveau VLAN 150 afin d’y mettre notre point d’accès. Ainsi que l’intégration d’une machine virtuelle servant à accueillir PfSense, cette VM sera sur le serveur AD de la partie LAN. De plus nous avons intégrer une borne wifi Cisco à notre maquette.



A1.2.5 Définition des niveaux d'habilitation associés à un service

C1.2.5.1 Recenser les utilisateurs du service, leurs rôles et leur niveau de responsabilité

Les utilisateurs sont les visiteurs médicaux, ce sont les visiteurs qui seront habilités à se connecter au SSID à travers l'authentification sur le portail captif.

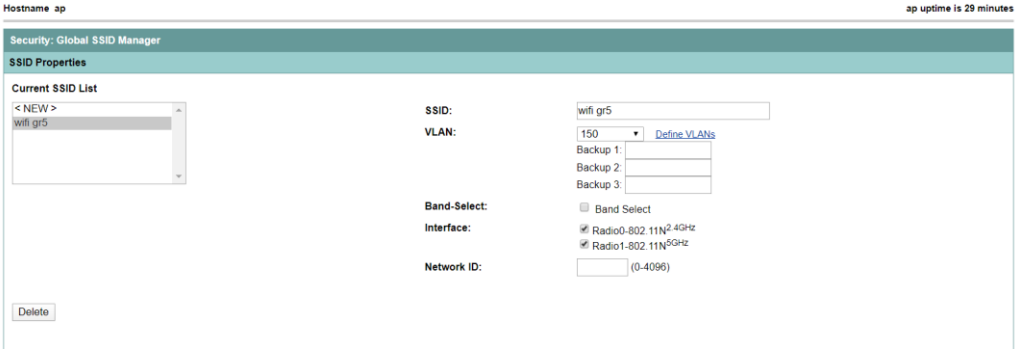


A1.2.2 Rédaction des spécifications techniques de la solution retenue (adaptation d'une solution existante ou réalisation d'une nouvelle solution)

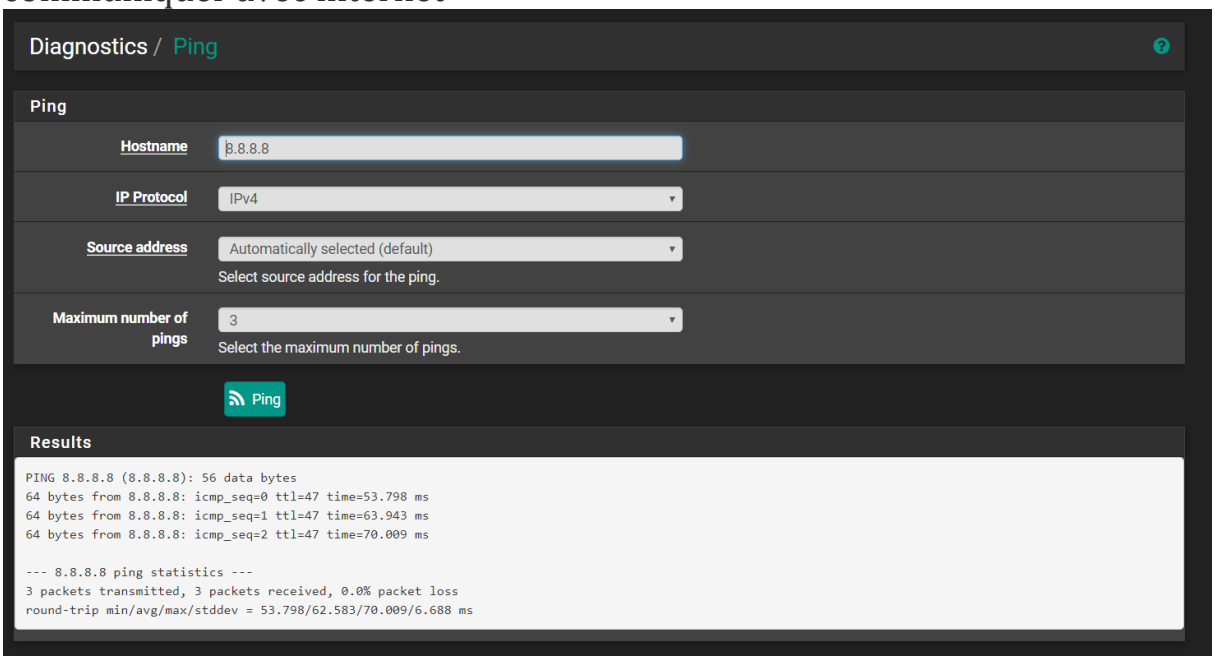
C1.2.2.2 Décrire l'implantation des différents composants de la solution et les échanges entre eux

Nous avions deux nouvelles interfaces :

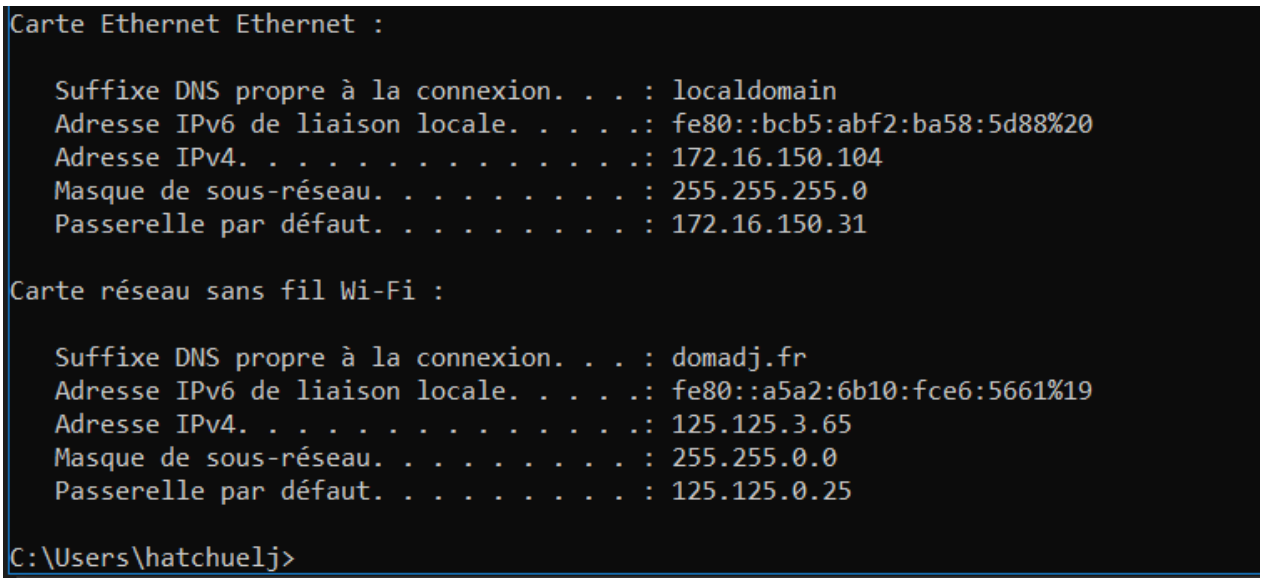
- Celui de notre borne wifi



- Celui de notre portail captif, PfSense qui doit évidemment communiquer avec internet



L’intérêt est d’avoir une plage d’adresse DHCP qui sera délivrer pour les visiteurs médicaux situé dans le VLAN 150.



A1.3.4 Déploiement d’un service

C1.3.4.3 Mettre en exploitation le service

A3.1.1 Proposition d’une solution d’infrastructure

C3.1.1.2 Caractériser les éléments d’interconnexion, les services, les serveurs et les équipements terminaux nécessaires

C3.1.1.5 Caractériser les solutions d’interconnexion utilisées entre un réseau et d’autres réseaux internes ou externes à l’organisation

A3.2.1 Installation et configuration d’éléments d’infrastructure

C3.2.1.1 Installer et configurer un élément d’interconnexion, un service, un serveur, un équipement terminal utilisateur

C3.2.1.3 Installer et configurer des éléments de sécurité permettant d’assurer la protection du système informatique

Au préalable il a fallu créer le VLAN 150 Visiteurs, d'un coté sur notre switch situé au deuxième étage mais aussi sur notre routeur ZyXEL au centre de notre maquette.

```
SW2ESERV(config)#do sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
10   InformatiqueReseauSysteme        active
20   DirectionDSI                     active
30   Comptabilite                     active
40   Developpement                    active
50   Commercial                       active
60   SalleReunionVisiteurs            active
100  Administration                   active    Fa0/24
150  Visiteurs                        active    Fa0/1, Fa0/3
200  Serveurs                         active    Fa0/2, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23
1002 fddi-default                     act/unsup
```

Add | Edit | Remove | Activate | Inactivate | Create Virtual Interface | Object Reference

#	Status	Name	Port/VID	IP Address	Mask
1		vlan10	lan2/10	static --172.16.10.254	255.255.255.0
2		vlan100	lan2/100	static --172.16.100.254	255.255.255.0
3		vlan150	lan2/150	static --172.16.150.254	255.255.255.0
4		vlan20	lan2/20	static --172.16.20.254	255.255.255.0
5		vlan200	lan2/200	static --200.200.5.254	255.255.255.0
6		vlan30	lan2/30	static --172.16.30.254	255.255.255.0
7		vlan40	lan2/40	static --172.16.40.254	255.255.255.0
8		vlan50	lan2/50	static --172.16.50.254	255.255.255.0
9		vlan60	lan2/60	static --172.16.60.254	255.255.255.0

Page 1 of 1 Show 50 items

J'ai créé les groupes sur le PfSense afin de pouvoir préparer les futures connexions des visiteurs médicaux.

System / User Manager / Groups

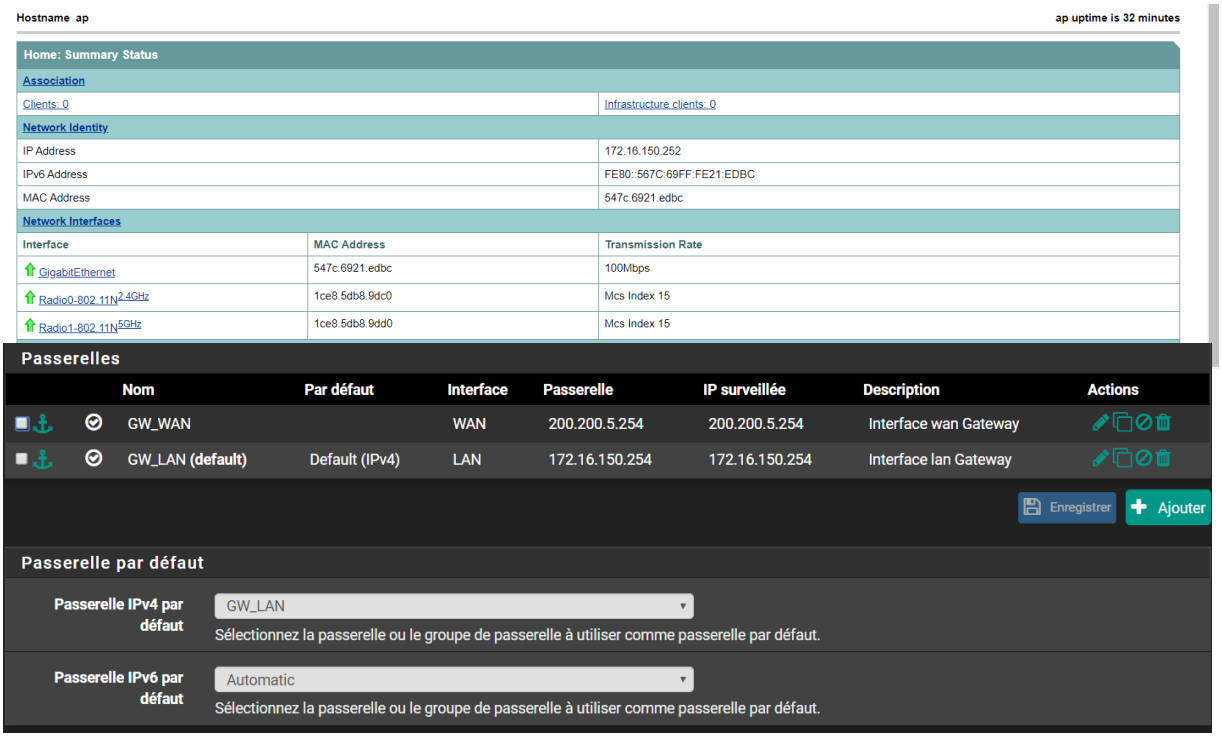
Users | Groups | Settings | Authentication Servers

Groups

Group name	Description	Member Count	Actions
Agent	Deletation Creation Utilisateurs Portail	1	
Portail	utilisateurs du Portail	1	
admins	System Administrators	1	
all	All Users	4	

Add

Par la suite nous avons configurer notre borne ainsi que le portail depuis les menus de configurations. (Renommage + IP) En ce qui concerne le portail captif il doit avoir deux cartes réseaux : une pour la partie WAN et une autre pour la partie LAN, la borne wifi en l'occurrence.



Hostname ap — ap uptime is 32 minutes

Home: Summary Status

Association	
Clients: 0	Infrastructure clients: 0
Network Identity	
IP Address	172.16.150.252
IPv6 Address	FE80::567C:69FF:FE21:EDBC
MAC Address	547c.6921.edbc

Network Interfaces

Interface	MAC Address	Transmission Rate
GigabitEthernet	547c.6921.edbc	100Mbps
Radio0-802.11N^2.4GHz	1ce8.5db8.9dc0	Mcs Index 15
Radio1-802.11N^5GHz	1ce8.5db8.9dd0	Mcs Index 15

Passerelles

	Nom	Par défaut	Interface	Passerelle	IP surveillée	Description	Actions
	GW_WAN		WAN	200.200.5.254	200.200.5.254	Interface wan Gateway	
	GW_LAN **(default)**	Default (IPv4)	LAN	172.16.150.254	172.16.150.254	Interface lan Gateway	

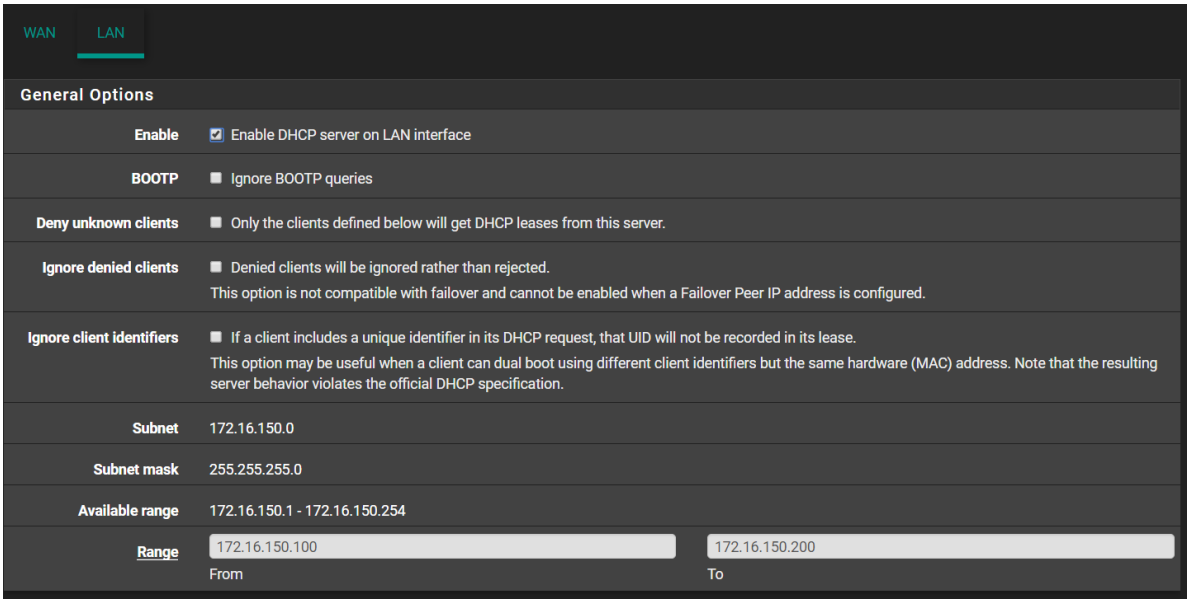
Enregistrer — Ajouter

Passerelle par défaut

Passerelle IPv4 par défaut: GW_LAN
Sélectionnez la passerelle ou le groupe de passerelle à utiliser comme passerelle par défaut.

Passerelle IPv6 par défaut: Automatic
Sélectionnez la passerelle ou le groupe de passerelle à utiliser comme passerelle par défaut.

En ce qui concerne le relais DHCP, nous avions déterminer une plage d'adresse d'environs 100 IP différentes. La création du DHCP se fait assez rapidement il ne nous restera plus qu'à vérifier si notre SSID nous délivre bien une adresse correspondante à la plage préalablement définit.



WAN | LAN

General Options

Enable	☑ Enable DHCP server on LAN interface
BOOTP	☐ Ignore BOOTP queries
Deny unknown clients	☐ Only the clients defined below will get DHCP leases from this server.
Ignore denied clients	☐ Denied clients will be ignored rather than rejected. This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore client identifiers	☐ If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease. This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.
Subnet	172.16.150.0
Subnet mask	255.255.255.0
Available range	172.16.150.1 - 172.16.150.254
Range	172.16.150.100 (From) — 172.16.150.200 (To)

A1.2.4 Détermination des tests nécessaires à la validation d'un service

C1.2.4.1 Recenser les tests d'acceptation nécessaires à la validation du service et les résultats attendus

C1.2.4.2 Préparer les jeux d'essai et les procédures pour la réalisation des tests

Communication internet - PfSense	Le ping passe
Borne Wifi – PfSense	La borne doit connaitre l'IP de PfSense pour nous rediriger vers le portail
PfSense – internet	Attribution d'une IP comprise entre :172.16.150.100– 172.16.150.200

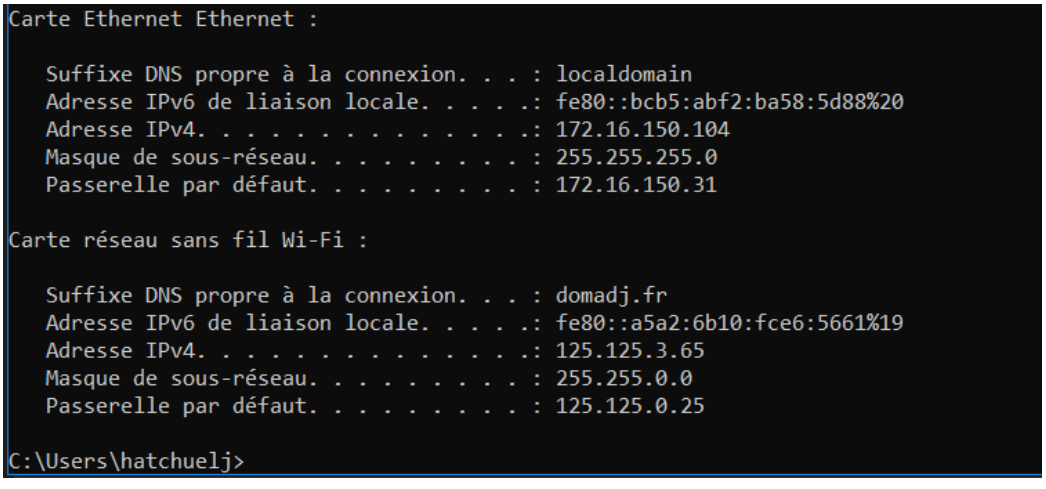
A1.3.1 Test d'intégration et d'acceptation d'un service

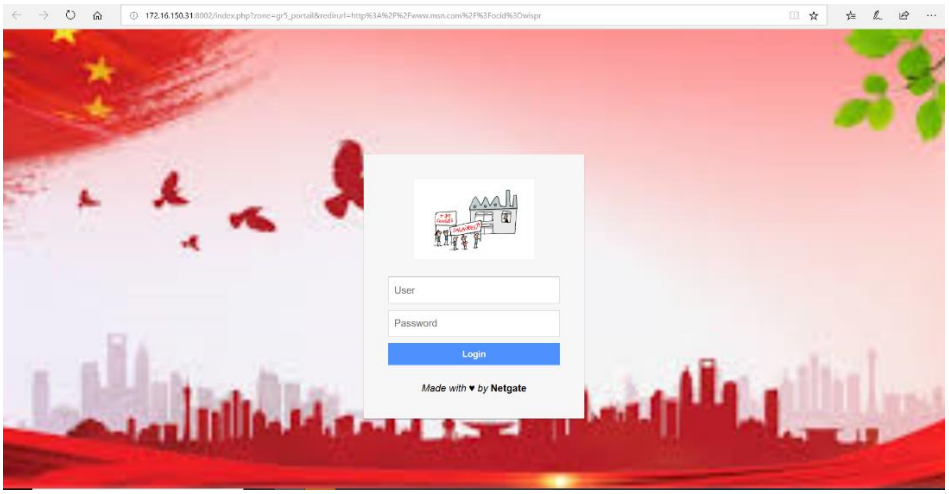
C1.3.1.1 Mettre en place l'environnement de test du service

C1.3.1.2 Tester le service

Nous avons bien le wifi « visiteurs GR5 » qui apparait sur nos smartphones, nous allons tenter de nous connecter aux wifi afin de voir si nous obtenons la bonne adresse IP ainsi que la bonne redirection vers le portail captif.

Nous avions également testé le DHCP avec un pc test que nous relier par câble au port correspondant au Vlan 150. Notre pc obtient l'IP 172.16.150.104, cette adresse IP correspond bien à notre plage définit préalablement.





Une fois arrivé sur la page HTML il ne nous reste qu'a rentrer le mot de passe par notre groupe. (« visiteurs »)