Documentation technique

****

Utilisation et configuration d'un firewall

Table des matières

Youssouf Hathouti

Introduction :

Objectif :

L'objectif de cette documentation est de voir différentes fonctionnalités que peut faire un firewall au sein d'un réseau, de l'installation du firmware aux règles de filtrage en passant par le VPN.

Matériel :

Nous travaillerons avec un firewall de la marque Fortinet. Le modèle est un Fortigate 200D et la version est la v6.0.18.

Adressage IP :

Nom de l'interface/sous-interface	**Adresse IP (/24)**
LAN (port1)	172.16.10.254
Wifi (employés)	172.16.117.254
WAN	192.168.10.107

1. Firmware

Dans cette partie, nous allons voir comment installer le firmware (micrologiciel) depuis notre PC lorsque l'on a pas accès à l'interface Web d'administration.
Dans notre cas, cela a été utile car le firewall, qui avait déjà été utilisé par d'autres étudiants, était protégé par un mot de passe auquel on n'avait pas accès. L'opération que nous allons voir maintenant nous a donc servie à partir sur une configuration vierge et sans mot de passe.

Dans notre cas, cette opération est utile et même indispensable car sans cela, impossible de travailler sur notre projet. Cependant, dans le cadre d'un équipement installé en milieu professionnel, cela peut représenter un haut risque de sécurité. Raison pour laquelle il est important d'avoir une sauvegarde de sa configuration sur un support externe et surtout de sécuriser l'accès physique aux équipements, puisque cette manipulation se fait via le port console du firewall.

1.1. Serveur TFTP

Pour envoyer le fichier de firmware du PC vers le firewall, on utilisera le protocole TFTP (Trivial File Transfer Protocol), qui est un protocole de transfert de fichier. Le PC joue donc le rôle du serveur TFTP qui envoie le fichier vers son client TFTP, le firewall.
On utilise Tftpd64, un petit serveur TFTP en open source, rapide d'installation et facile d'utilisation (cliquer ici pour l'installer).

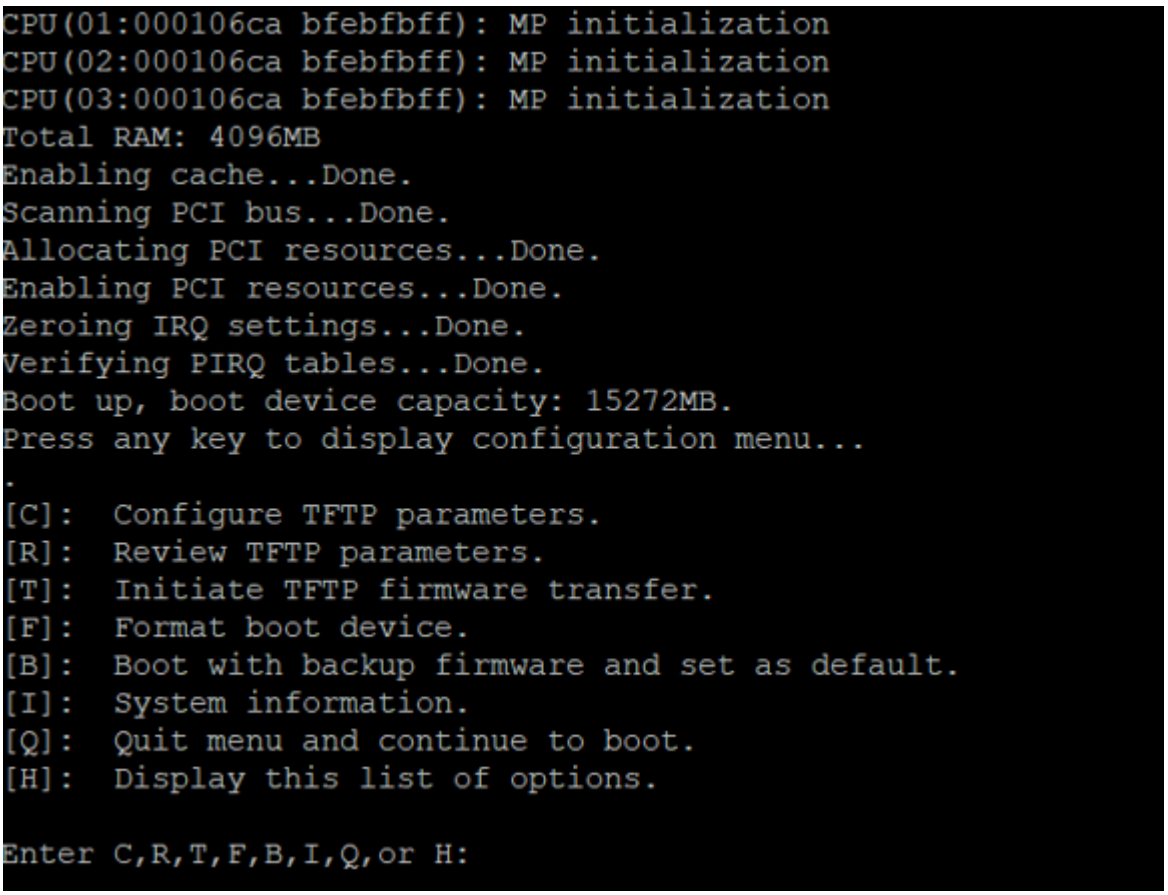
Il faut ensuite configurer les paramètres du serveur TFTP afin d'envoyer le bon fichier vers la bonne destination. Le plus simple est de regarder les paramètres TFTP par défaut du firewall et de les appliquer au serveur TFTP.

Il faut donc brancher, en plus du câble console, un câble RJ45 d'une prise RJ45 du PC vers le port MGMT du firewall et on appliquera à l'interface réseau du PC l'adresse 192.168.1.1 et sélectionner cette interface sur tftpd64.
Il faudra aussi renommer le fichier de firmware en "image.out" et le mettre dans un dossier facilement accessible pour se faciliter la tâche (Bureau ou Téléchargements), et choisir ce dossier sur tftpd64.

1.2. Client TFTP

Nous disposons donc du fichier de firmware sur un PC et nous allons nous brancher au port console de notre Fortigate 200D lorsqu'il est encore éteint.
Une fois le PC branché sur le port console, nous allons lancer un terminal qui permet de configurer des équipements en console (PuTTY ou MobaXterm) et choisir une session console.

À ce moment, nous allons allumer le firewall et appuyer en continu sur n'importe quelle touche jusqu'à arriver dans le menu de configuration qui ressemble à ça :



Une fois les paramètres correctement configurés sur le serveur TFTP, on tape “T” pour lancer le transfert du fichier du serveur TFTP (PC) vers le client TFTP (firewall).

Puis à la question “`Save as Default firmware/Backup firmware/Run image without saving:[D/B/R]?`”, on tape la lettre D et on laisse faire le firewall.

À partir de ce moment, on peut utiliser notre firewall avec une configuration vierge et sans mot de passe que l’on pourra configurer par la suite.

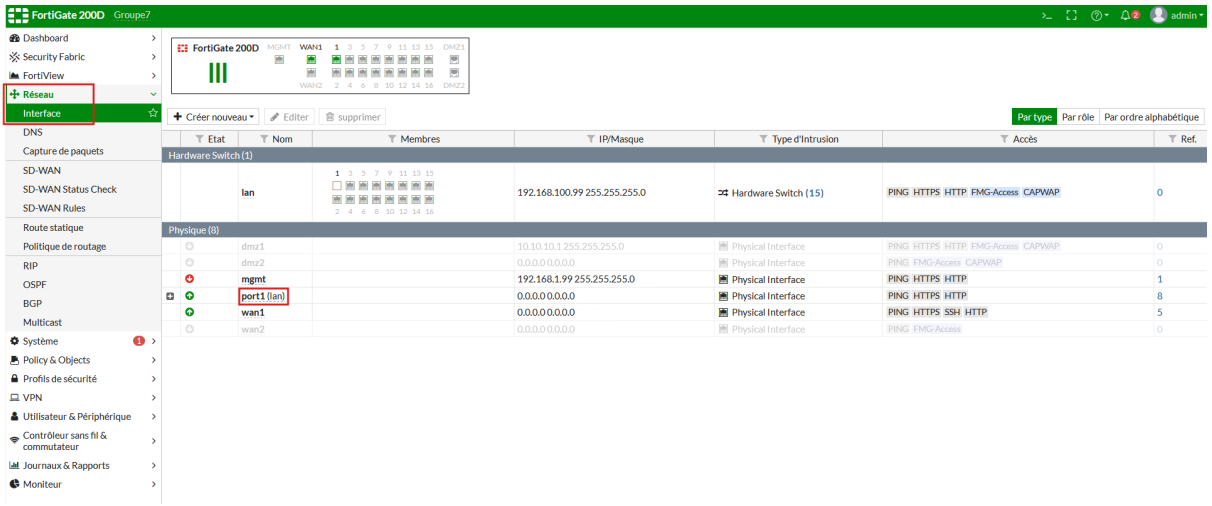
2. Interfaces

Dans cette partie, nous allons voir les interfaces du firewall, leur rôle et comment les configurer.

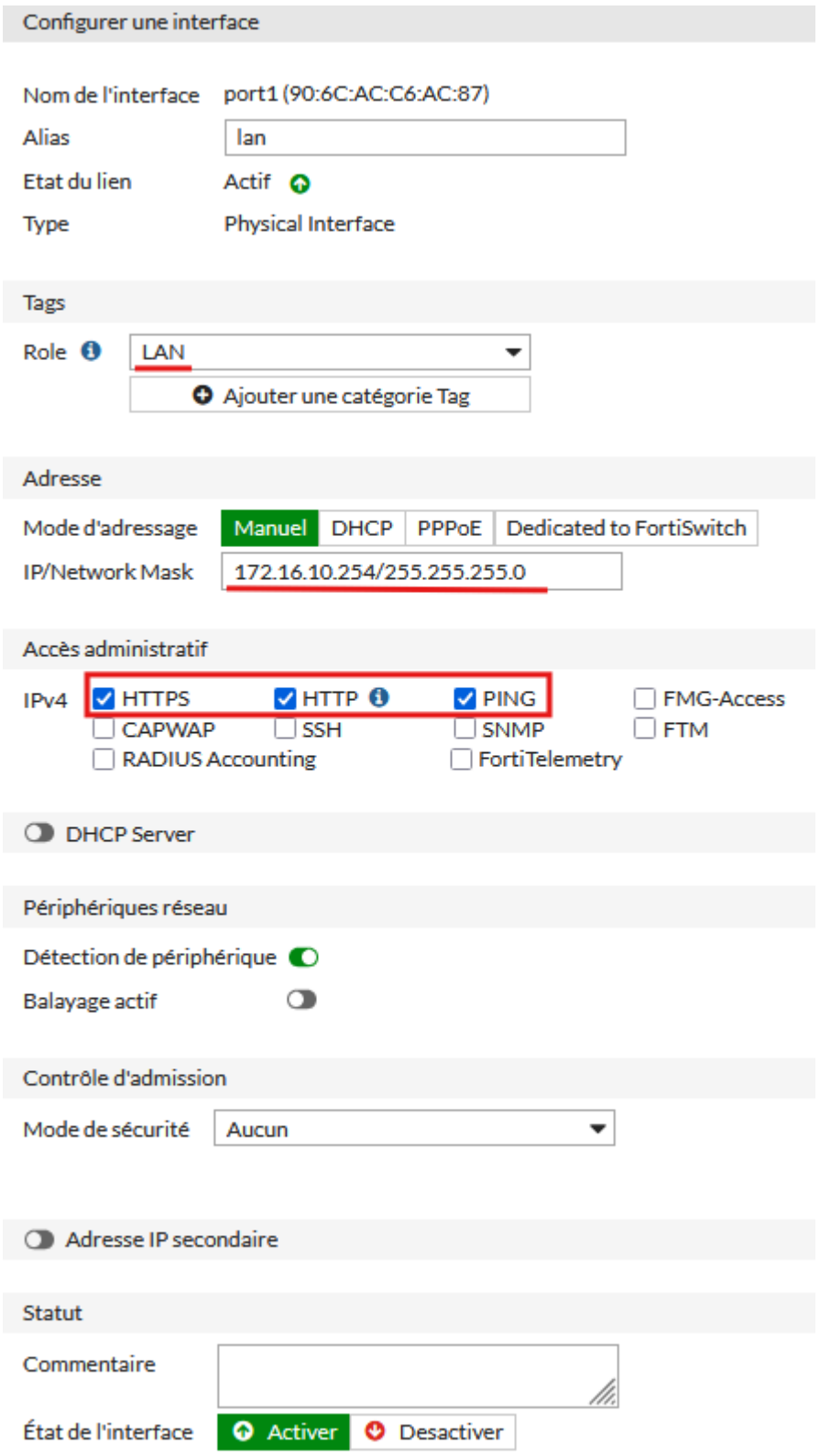
2.1. IN

L'interface IN (ou LAN en fonction des modèles) est l'interface à laquelle est directement connecté le réseau local. En général, c'est un switch (commutateur) qui est relié à cette interface (comme dans notre cas), et sur lequel sont reliés les équipements du réseau local (PCs, imprimantes, borne WiFi, TPE, caméras de surveillance …).
Il faudra donc lui attribuer une adresse IP dans le réseau IP principal, en général la première ou la dernière adresse. Dans notre cas, on choisit la dernière.

Pour lui attribuer une adresse IP, on se rend dans Réseau → Interface :



Puis on double-clique sur l'interface en question, ici elle s'appelle "port1(lan)" :



On vérifie bien que le rôle est “LAN”, puis on renseigne l’adresse IP choisie ainsi que le masque et enfin, les accès que l’on veut autoriser sur cette interface. Ici, on choisit l’accès Web (HTTP/HTTPS) et le PING. L’accès Web permet à l’administrateur du réseau d’accéder à l’interface Web de configuration du firewall en passant par

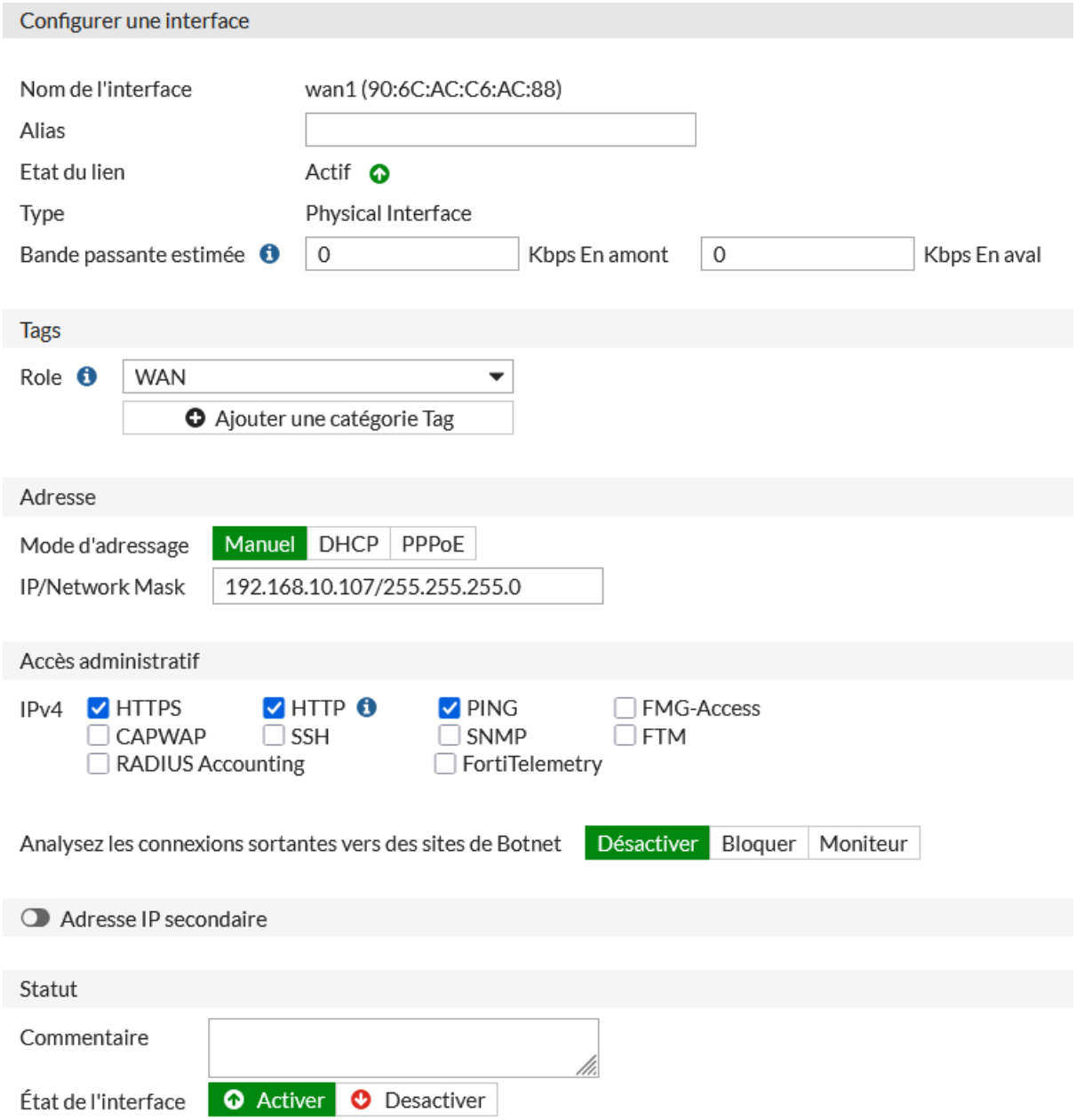
l'adresse IP assignée à cette interface en tapant dans un navigateur "https://172.16.10.254". Le ping quant à lui, sert à tester simplement la connectivité entre une machine et le firewall. Cela peut être très utile en cas de panne afin de détecter la source du problème et de faciliter la résolution de celui-ci. Si la case PING est décochée, toutes les requêtes ICMP vers cette adresse seront bloquées et on ne pourra pas savoir si le firewall est accessible depuis une machine du réseau.

On active pas l'option DHCP Server car dans notre réseau, le service DHCP est géré par un serveur sur une machine virtuelle dédiée. Mais il est tout à fait possible de faire en sorte que le serveur qui distribue les configurations IP pour les machines du réseau soit le firewall.

2.2. OUT

L'interface OUT (ou WAN en fonction des modèles) est l'interface à laquelle est connecté le réseau public, celui qui mène vers Internet. En général, c'est un routeur qui est relié à cette interface, lui-même raccordé à l'accès opérateur qui fournit l'accès à Internet. Dans notre cas, l'interface WAN est reliée à un switch du réseau de notre salle de TP, lui-même relié vers un autre firewall, relié à l'accès opérateur.
De manière générale, c'est donc une adresse IP publique qui est attribuée à cette interface afin qu'elle soit joignable depuis Internet.

Dans notre cas, nous lui attribuons une adresse qui nous a été fournie dans le réseau de la salle de TP. Pour ce faire, on se rend dans le même menu que pour l'interface IN puis on double clique sur l'interface wan1 et on configure les mêmes paramètres que l'interface IN :

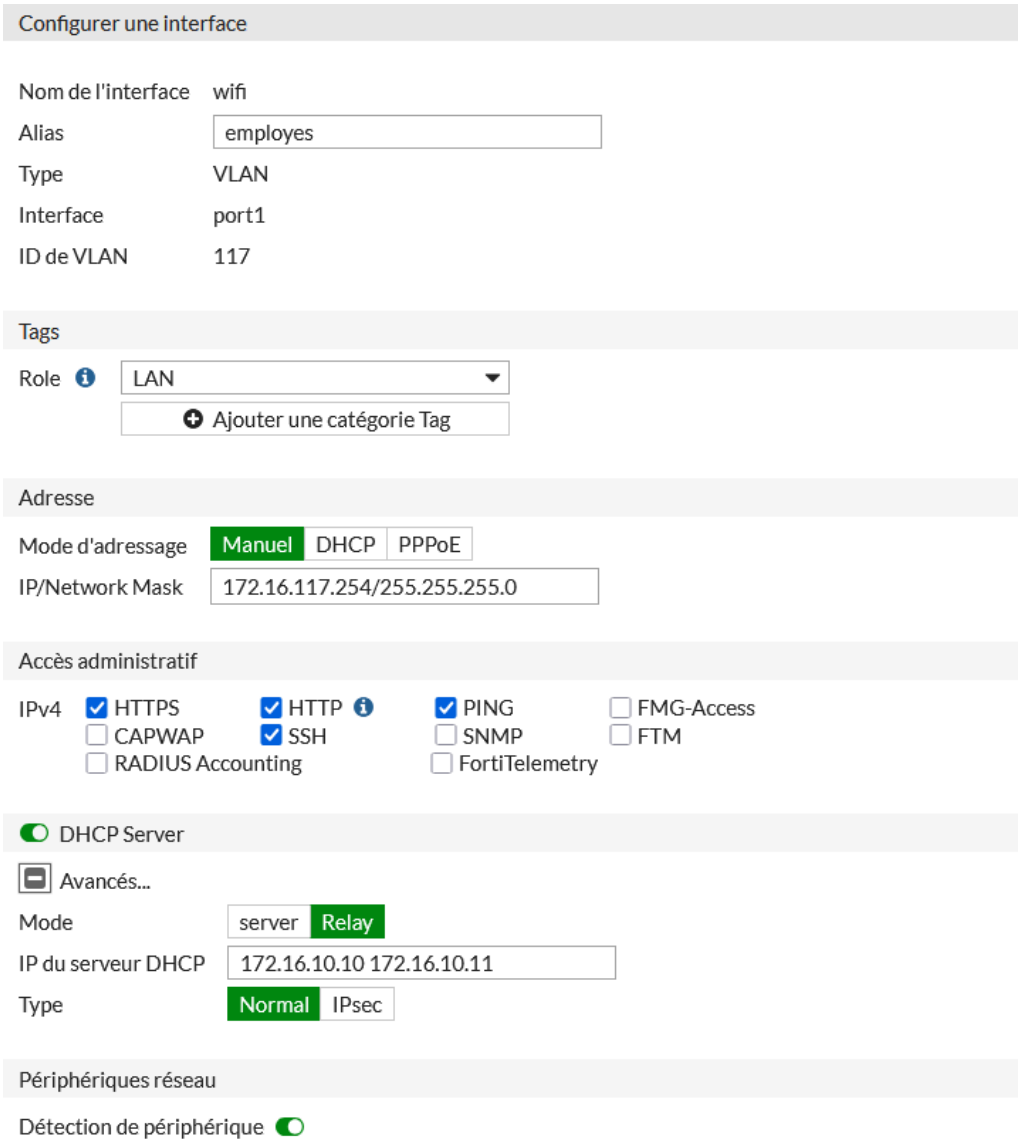


3. VLAN

Dès lors que l'on travaille sur une infrastructure avec plusieurs VLAN, il faut disposer d'un équipement qui fait du routage afin d'assurer l'accès entre les VLAN. Ce peut être un switch de niveau 3 ou un firewall comme dans notre cas.

À chaque VLAN, il faut créer une sous-interface sur l'interface IN du firewall qui sera une interface virtuelle liée à un VLAN en particulier. Ces interfaces virtuelles serviront ensuite à autoriser ou interdire du trafic d'un VLAN à un autre.

Pour créer une sous-interface, on se rend sur notre Fortigate 200D, dans le menu “Interface”, puis on sélectionne l’interface port1 (lan). Ensuite, on clique sur “Créer nouveau” → “Interface” et on se retrouve dans ce menu :



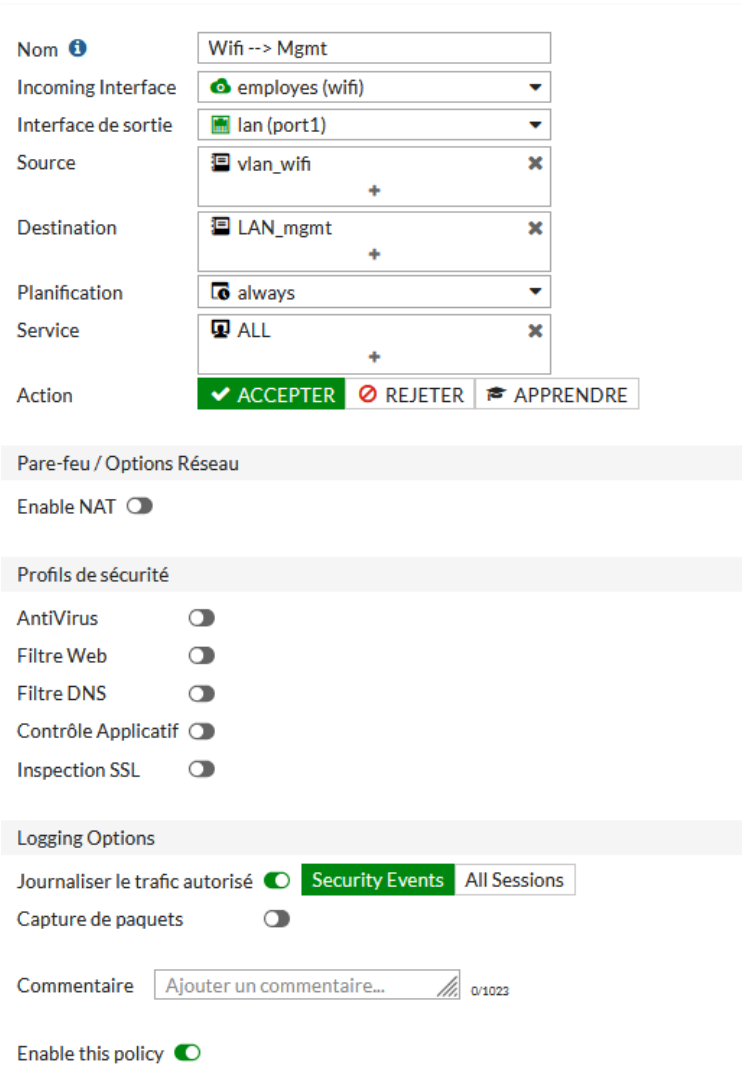
De la même manière que pour les autres interfaces, on remplit les différentes informations en n’oubliant pas de déclarer le type d’interface en tant que VLAN, de mettre le numéro du VLAN et d’activer le DHCP relai. Il sert à relayer les requêtes DHCP venant du réseau de ce VLAN vers le bon serveur DHCP (ce que l’on renseigne sur le firewall). À savoir que l’on peut renseigner deux serveurs DHCP, il suffit de mettre les 2 adresses IP à la suite, séparées par un espace ou une virgule.

4. Règles de filtrage

Les règles de filtrages sont importantes, car elles vont nous permettre de gérer les accès à la fois entre les différents réseaux locaux mais aussi de ces réseaux vers l'extérieur (donc vers Internet).

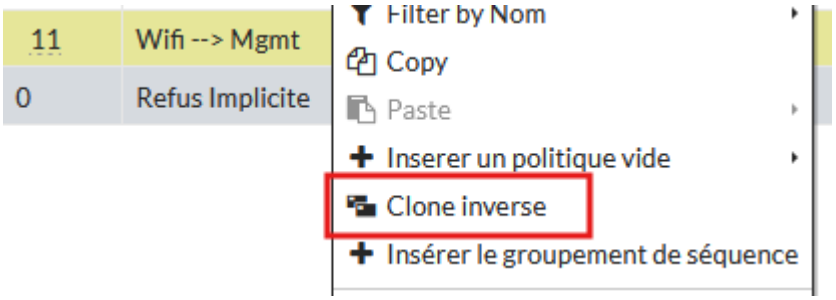
4.1. Inter-VLAN

Par exemple, pour autoriser les utilisateurs connectés au réseau WiFi employés à accéder aux machines du réseau local câblé, il faut faire une règle de filtrage dans un sens puis dans l'autre. Pour ce faire, on se rend dans l'onglet "Policy & Objects" → "Règle IPv4" → "Créer nouveau" :



Tout d'abord, on nomme notre règle de manière claire et concise, afin que l'on puisse l'identifier très facilement et qu'on ne la confonde pas avec une autre par la suite. Ici, "Mgmt" correspond au réseau câblé sur lequel se trouvent les serveurs

auxquels doivent accéder les employés. Ensuite, on complète les différents champs et on pense à désactiver le NAT (qui est activé par défaut).
Le NAT n'est pas utile ici car il s'agit d'accès entre les VLAN de notre infrastructure locale. Il sera utile dans le cas où l'on fera une règle qui autorise le trafic vers Internet. Une fois la règle créée et validée, il faut faire une règle retour. Pour éviter de refaire une nouvelle règle en sens inverse à la main (ce qui prend du temps et qui peut contenir un risque d'erreur), il existe une fonctionnalité qui permet de créer une règle inverse en deux clics.
Pour cela, on effectue un clic droit sur la règle, puis sur "Clone inverse" :



La règle retour est créée juste en dessous :

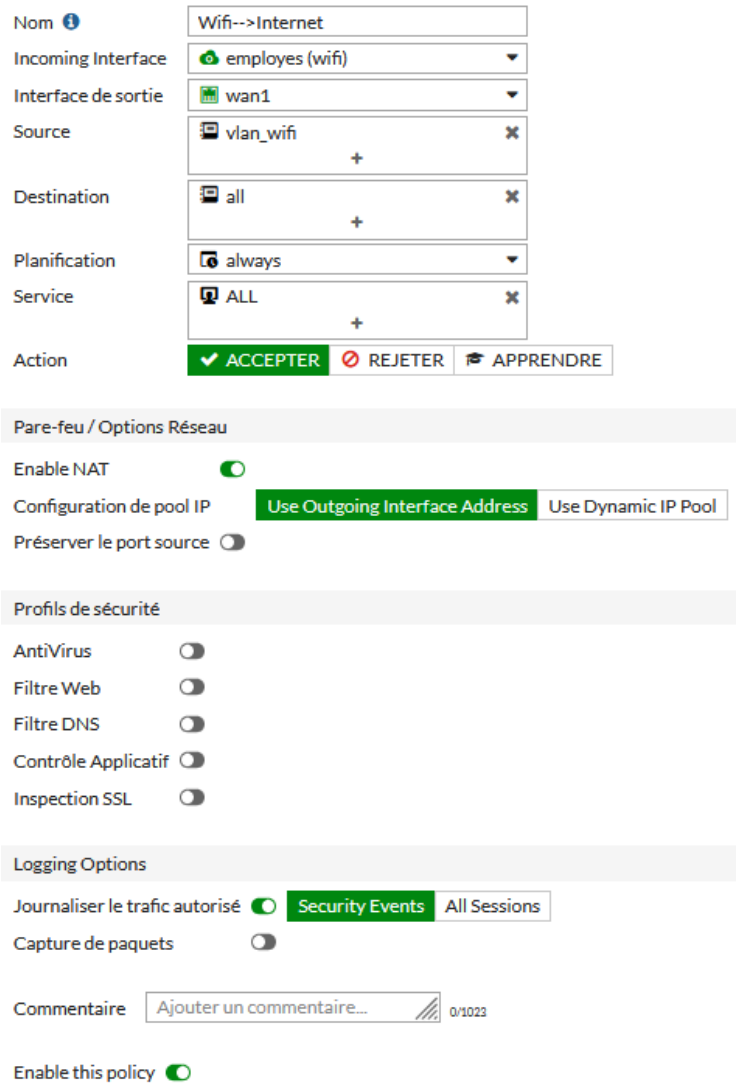
Il ne manque plus qu'à double-cliquer sur cette règle afin de la nommer et de l'activer.

4.2. Vers Internet

Si l'on veut autoriser les utilisateurs d'un réseau à accéder à Internet, il faudra créer une règle en procédant de la même manière que vu précédemment, mais en faisant attention à quelques points :

- l'interface de sortie sera l'interface WAN et la destination sera "all"
- il faudra activer le NAT car l'adresse IP privée de l'utilisateur n'est pas routable sur Internet
- on ne fera pas de règle retour pour les règles "réseau interne vers Internet"

Voici un exemple de configuration d'une règle qui autorise les utilisateurs du WiFi employés à accéder à Internet :



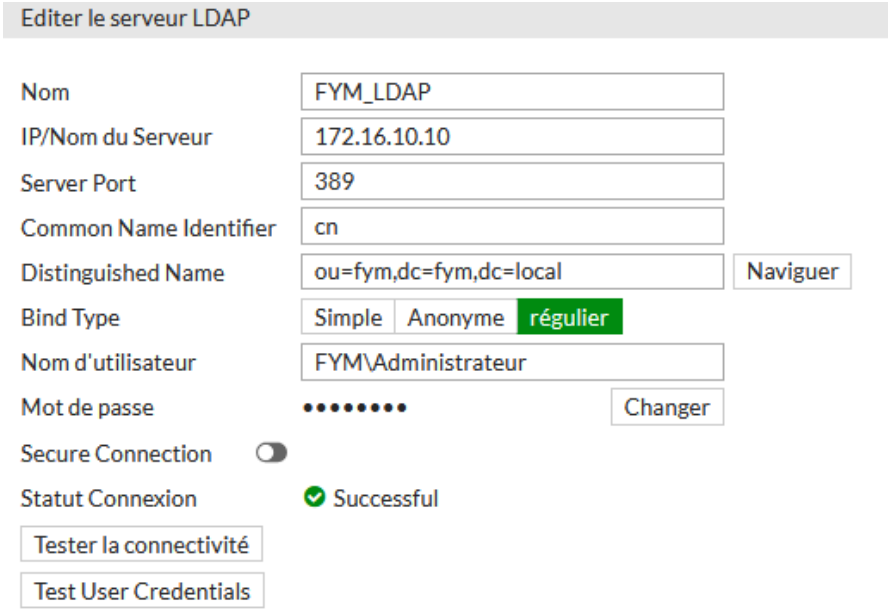
5. VPN SSL

Dans un réseau d'entreprise, il peut être utile de mettre en place un accès VPN afin que les employés puissent travailler et accéder aux ressources internes de l'entreprise (serveurs, applications métiers) depuis l'extérieur (comme en télétravail par exemple).

Sur la plupart des firewalls de la marque Fortinet, il est possible de mettre en place un accès VPN. Pour la connexion VPN, on a 2 options : créer manuellement un compte local (propre au firewall) pour chaque utilisateur, ce qui prend du temps et qui ne facilite pas la connexion pour les utilisateurs, qui se retrouvent avec un compte différent pour la connexion VPN.
La deuxième option est de lier l'AD au firewall via le protocole LDAP. Ainsi, les utilisateurs peuvent se connecter en VPN avec leur comptes AD, ce qui fait un seul compte à gérer par personne et cela facilite aussi bien à l'utilisateur qu'à l'administrateur.

5.1. Créer un serveur LDAP

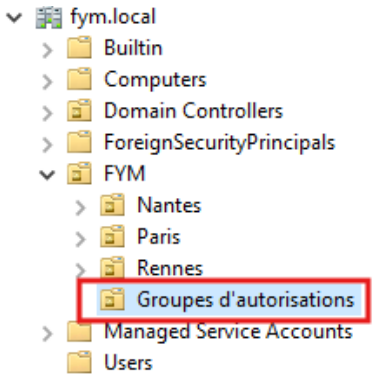
Dans un premier temps, on se rend dans le menu “Utilisateur & périphérique” → LDAP Server. On clique sur “Créer nouveau” et on remplit les différents champs comme ci-dessous :



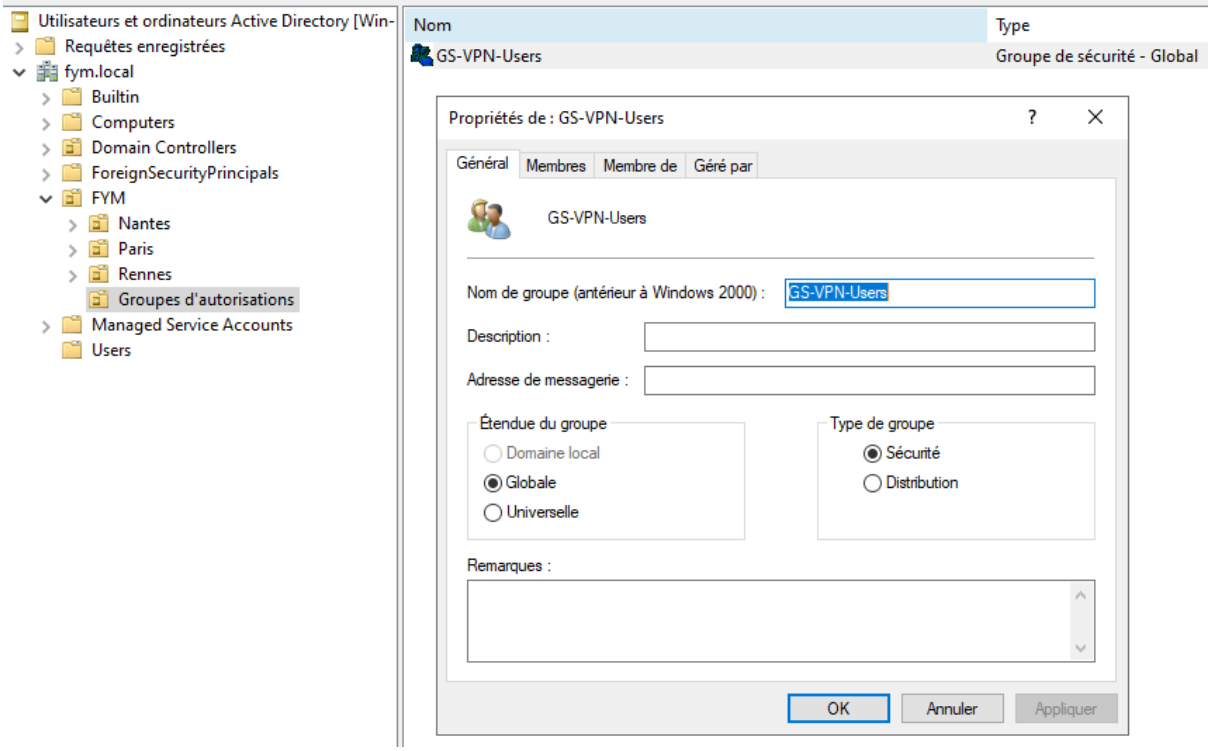
On nomme le serveur LDAP avec un nom clair et facilement identifiable (pour la suite), on renseigne l’adresse IP du serveur AD et on met le port 389 qui est le port utilisé par le protocole LDAP. Dans le champ “Distinguished Name”, on renseigne l'emplacement de l’AD dans lequel on placera notre groupe d’utilisateurs VPN.
Enfin, on renseigne un utilisateur du domaine qui permettra de tester la connexion à l’AD. Ici, on a mis l’administrateur du domaine. Pour tester la connexion, on clique sur “Tester la connectivité” et on observe qu’il est écrit “Successful”.
On termine par valider en cliquant sur OK.

5.2. Groupes AD et Firewall

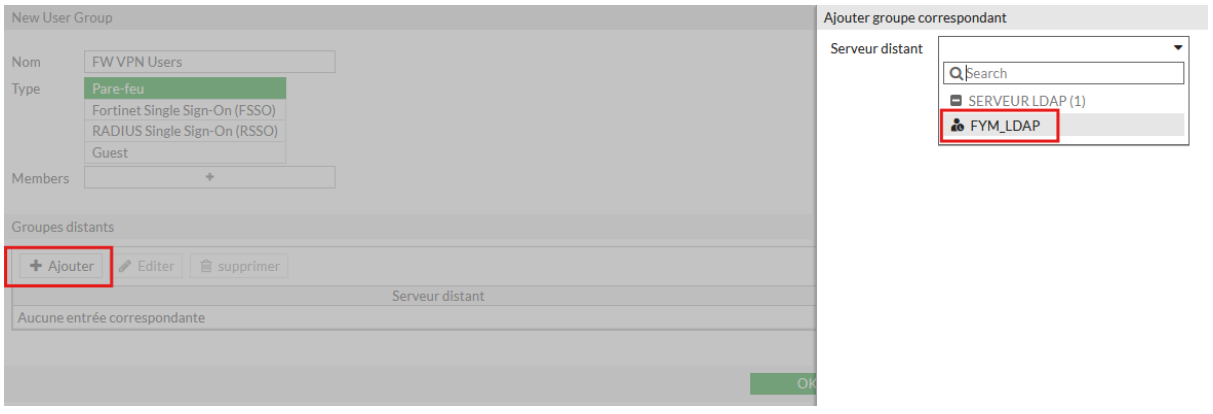
Une fois le serveur LDAP créé sur le firewall, on se rend sur le contrôleur de domaine et on va créer une OU dans l’emplacement que l’on a renseigné à l’étape précédente :



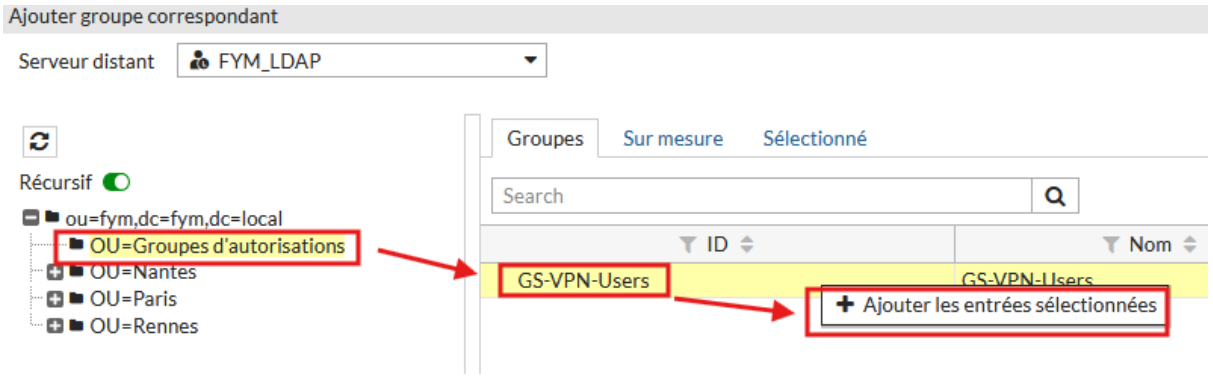
Dans cette OU, on crée un groupe de sécurité globale dans lequel on définit comme membres de ce groupes tous les utilisateurs auxquels on souhaite donner un accès VPN.



Une fois ce groupe créé sur l'AD, on revient sur le firewall et on se rend dans "Groupe utilisateur". On clique sur "Créer nouveau", on nomme notre groupe avec un nom clair et facilement identifiable, puis dans la partie "Groupes distants", on clique sur "Ajouter" et on sélectionne notre serveur LDAP :



Ensuite, on cherche dans l'arborescence de l'AD, le groupe d'utilisateurs VPN que l'on vient de créer et on clique droit dessus, puis "Ajouter les entrées sélectionnées" :

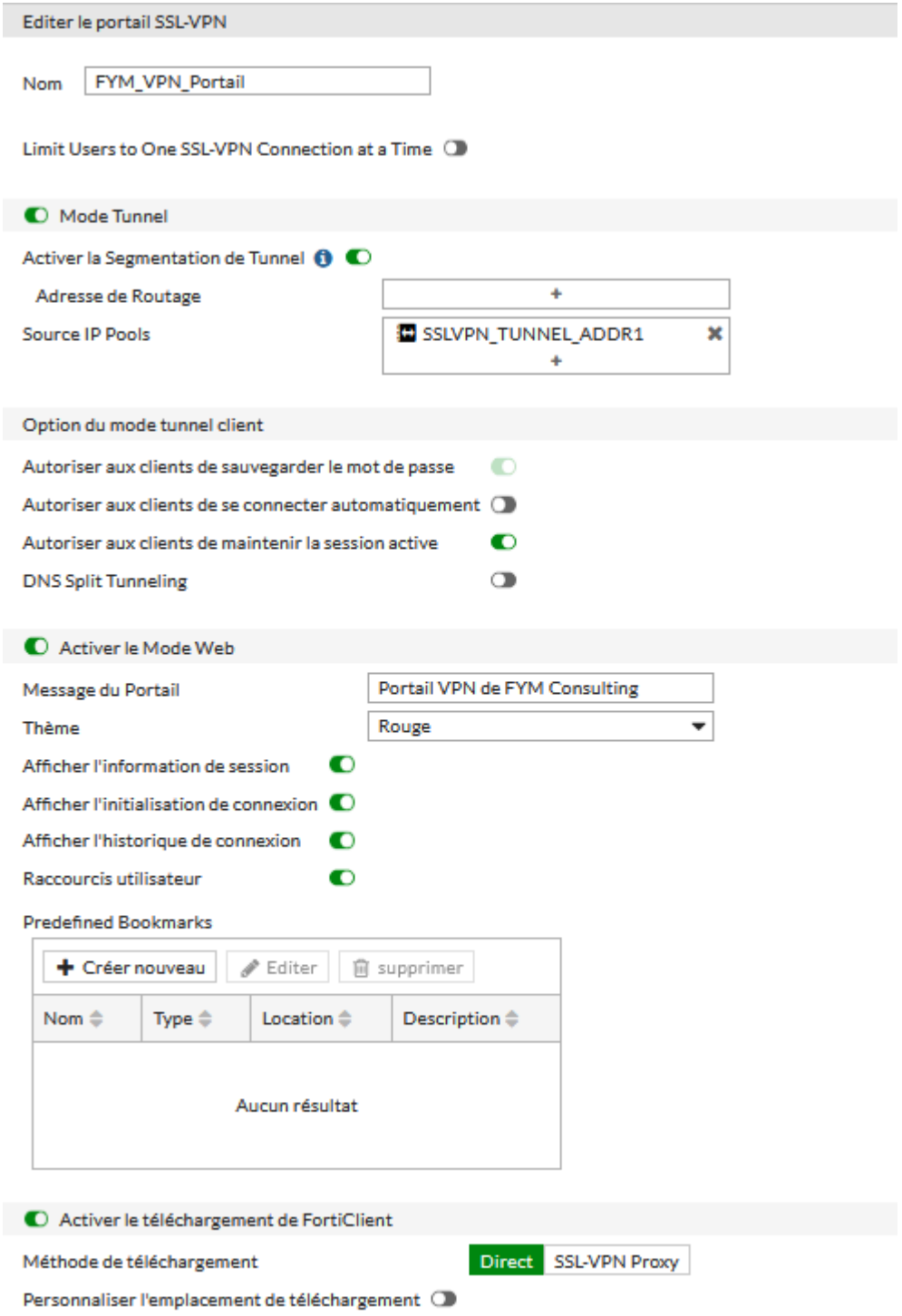


On termine par valider en cliquant sur OK.

5.3. Portail et paramètres VPN

Pour terminer, il faut configurer un portail web de connexion (on peut prendre un portail déjà existant par défaut mais je préfère personnaliser le mien) ainsi que les paramètres de la connexion VPN.

Pour cela, on se rend dans le menu VPN → Portails SSL-VPN → Créer nouveau :



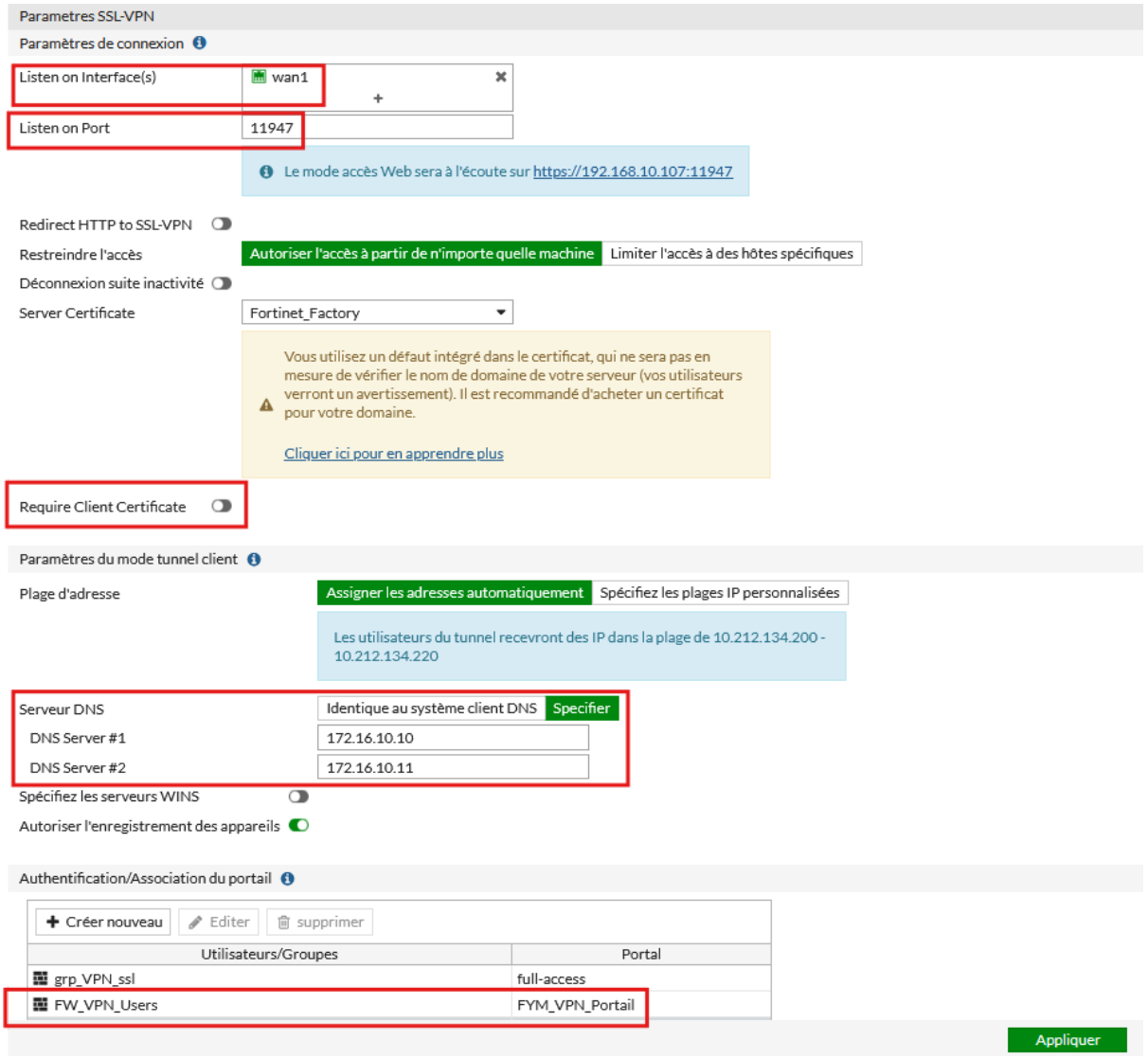
Points importants :

- Bien renseigner dans “Source IP Pools” la plage d’adresse attribuée au clients VPN (ici on utilise celle configurée par défaut qui s’appelle “SSLVPN_TUNNEL_ADDR1”)
- Mettre un message du portail qui soit clair, avec le nom de l’organisation ou du groupe

- Vérifier que “Activer le téléchargement de FortiClient” est bien cochée afin que les utilisateurs puissent télécharger le client Fortinet depuis leur espace Web VPN

On termine par valider en cliquant sur OK.

Ensuite, on se rend sur “SSL-VPN Settings” :

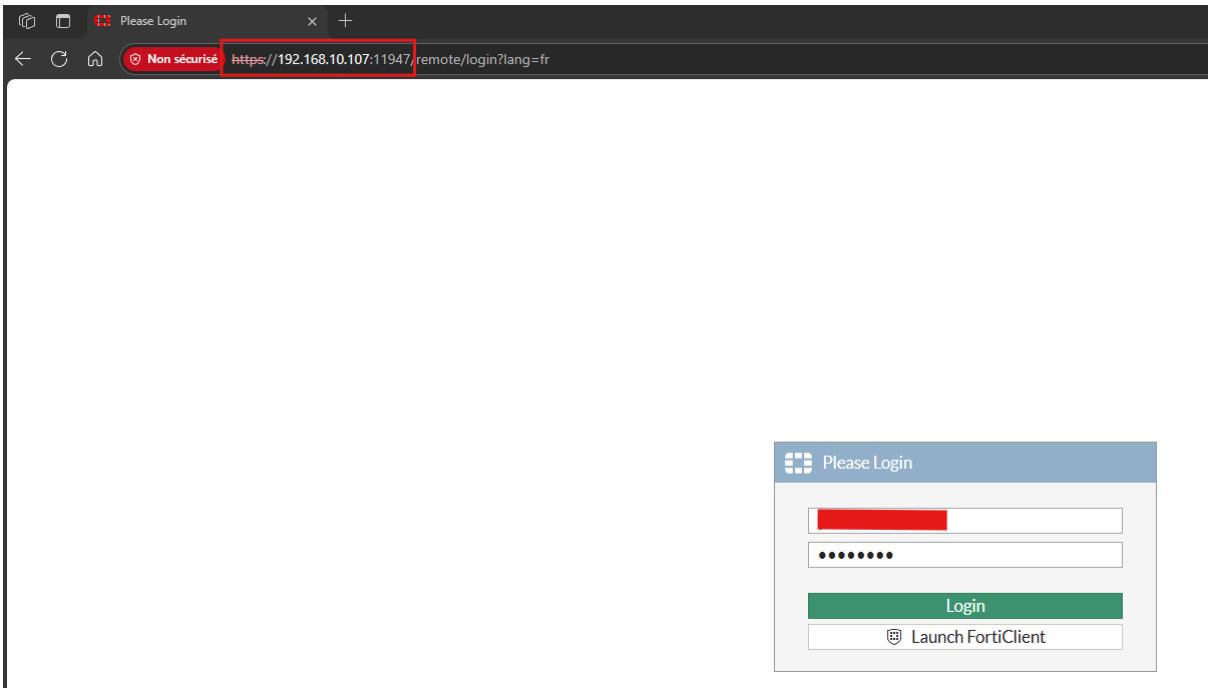


Points importants :

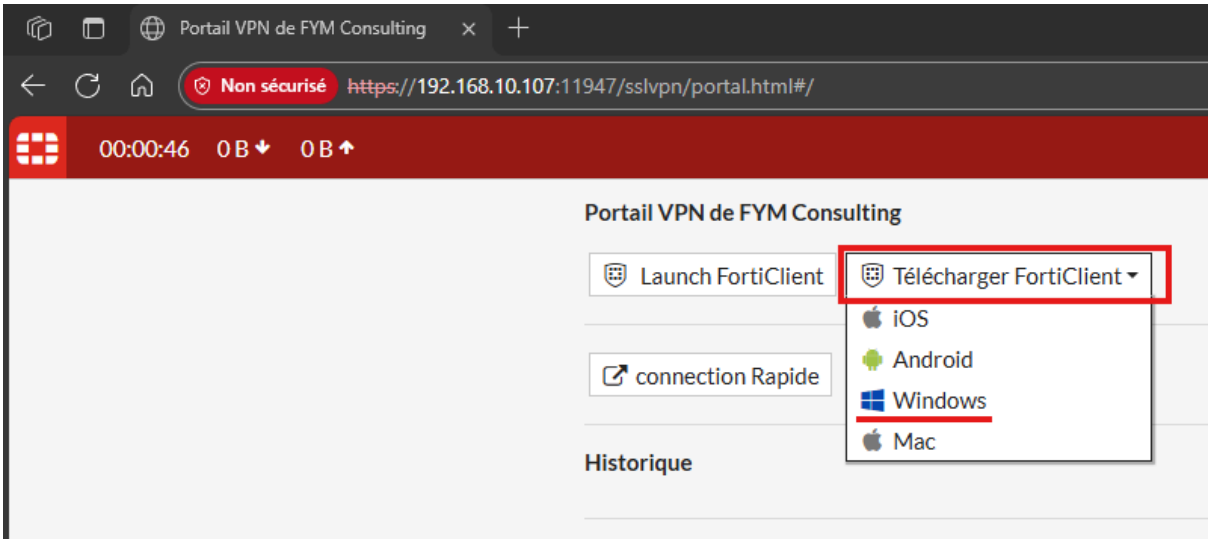
- Interface d’écoute : interface WAN
- Port d’écoute : ici, on a mis le port qui nous a été communiqué par le professeur. Sinon, on peut mettre le port de notre choix tant que celui-ci n’est pas déjà utilisé pour un autre service
- Veiller à ce que la case “Require Client Certificate” soit bien décochée
- Renseigner les serveurs DNS qui seront communiqués aux clients VPN (ici on a mis les deux serveurs DNS de notre réseau)

- Sélectionner le groupe firewall lié au groupe AD d'utilisateurs VPN que l'on a créé à l'étape précédente en cliquant sur "Créer nouveau" et en choisissant le bon groupe et le portail que l'on vient de configurer.

On termine par valider en cliquant sur Appliquer.
Il ne manque plus qu'à tester la connexion VPN, tout d'abord en tapant dans un navigateur (depuis une connexion externe au réseau local) : https://(adresseIP_publique_du_FW):(port) :



On obtient cette page :



A partir de là, on peut télécharger le FortiClient et configurer une connexion que l'on pourra enregistrer pour les fois suivantes.