

## Projet bornes Wifi Toulouse

### Objectif :

Les salles de réunions du site de Toulouse ne possèdent pas de prises Ethernets, seul un câble a été tiré dans chaque salle afin d'y installer des bornes Wifi. L'objectif est alors d'installer quatre bornes Wifi UniFi UB-U6 PRO alimentées en PoE et connectées en étoile à un switch PoE fournit par la CCAS.

Les ports permettant les accès à internet et aux services courants seront fermés rendant obligatoire la connexion au VPN Check Point à toute personne souhaitant accéder à internet et aux services de la CCAS.

### Filtrage des ports de sortie sur la Livebox :

Tout d'abord il faut accéder à l'interface de configuration de la Livebox en saisissant l'IP du routeur (192.168.1.1) dans un navigateur web tout en étant connecté au réseau de la box.

Puis une fois connecté chercher la section "ma configuration Wifi et Livebox" puis "pare-feu".

Sélectionner le niveau de protection "personnalisé" :

#### **sélection de votre niveau de protection**

☐ **faible**

Le pare-feu ne filtre rien.

Attention : ce niveau est réservé aux utilisateurs avertis pour qui la sécurité n'est pas une priorité ; notez aussi que même dans ce mode, une connexion initiée depuis Internet ne sera pas permise en l'absence de règle NAT/PAT dédiée.

☐ **moyen**

Le pare-feu filtre toutes les connexions entrantes. Le trafic sortant est autorisé à l'exception des services Netbios. Il est recommandé d'utiliser ce mode.

☐ **élevé**

Le pare-feu vous permet d'utiliser les applications standards sur Internet (www, mail, news, ...) et rejette les connexions entrantes non désirées. Ce choix est recommandé pour disposer d'un niveau de sécurité maximum.

☐ **élevé intermédiaire pro**

Le pare-feu vous permet d'utiliser les applications standards sur Internet (www, mail, news, ...) ainsi que l'application de téléphonie "Connect Pro" et rejette les connexions entrantes non désirées.

☒ **personnalisé**

Ce profil vous permet de personnaliser votre pare-feu. Vous pouvez ainsi définir des règles de filtrage spécifiques. (Réservé aux utilisateurs experts)

➤ personnaliser le pare-feu

Puis cliquer sur « personnaliser le pare-feu.

Ensuite, modifier les quatre premières règles (HTTP, HTTPS, FTP et FTP-Data) en les passant d'accepter à rejeter dans le paramètre action.

Pour un meilleur confort visuel il est possible de supprimer toutes les autres règles, mais cela prend un certain temps.

On ajoute une règle afin d'autoriser la connexion au VPN et la place tout en haut de la liste afin de la prioriser.

application / service	Tous
protocole	Tous
IP source	192.168.1.0
masque IP source	255.255.255.0
port source (ou plage)	Tous
IP destination	194.250.178.225
masque IP destination	255.255.255.255
port destination (ou plage)	Tous
action	accepter
activer	<input checked="" type="checkbox"/>

Il faut aussi autoriser les ranges d'IP des services de Microsoft, la liste étant longue je vous laisse vous reporter à la capture d'écran globale un peu plus bas pour prendre connaissance des règles qui leurs sont liés.

Une règle autorisant le Proxy cloud est également mise en place permettant ainsi d'ajouter les restrictions du Proxy à celles du pare-feu.

Création d'une règle qui rejette tout par défaut que l'on vient prioriser après les règles Microsoft :

application / service	Tous
protocole	Tous
IP source	192.168.1.0
masque IP source	255.255.255.0
port source (ou plage)	Tous
IP destination	Tous
masque IP destination	Tous
port destination (ou plage)	Tous
action	rejeter
activer	<input checked="" type="checkbox"/>

Toutes les règles du pare-feu :

application / service	protocole	IP source	masque IP source	port source (ou plage)	IP destination	masque IP destination	port destination (ou plage)	action	ordre	activer <input checked="" type="checkbox"/>	modifier	supprimer
VPN	Tous	192.168.1.0	255.255.255.0	Tous	194.250.178.225	255.255.255.255	Tous	accepter	↑ ↓	<input checked="" type="checkbox"/>		
Teams	Tous	192.168.1.0	255.255.255.0	Tous	13.107.64.0	255.255.192.0	Tous	accepter	↑ ↓	<input checked="" type="checkbox"/>		
Teams	Tous	192.168.1.0	255.255.255.0	Tous	52.112.0.0	255.252.0.0	Tous	accepter	↑ ↓	<input checked="" type="checkbox"/>		
Teams	Tous	192.168.1.0	255.255.255.0	Tous	52.122.0.0	255.254.0.0	Tous	accepter	↑ ↓	<input checked="" type="checkbox"/>		
Exchange Online	Tous	192.168.1.0	255.255.255.0	Tous	13.107.6.152	255.255.255.254	Tous	accepter	↑ ↓	<input checked="" type="checkbox"/>		
Exchange Online	Tous	192.168.1.0	255.255.255.0	Tous	13.107.18.10	255.255.255.254	Tous	accepter	↑ ↓	<input checked="" type="checkbox"/>		
Exchange Online	Tous	192.168.1.0	255.255.255.0	Tous	13.107.128.0	255.255.252.0	Tous	accepter	↑ ↓	<input checked="" type="checkbox"/>		
Exchange Online	Tous	192.168.1.0	255.255.255.0	Tous	23.103.160.0	255.255.240.0	Tous	accepter	↑ ↓	<input checked="" type="checkbox"/>		
Exchange Online	Tous	192.168.1.0	255.255.255.0	Tous	40.96.0.0	255.248.0.0	Tous	accepter	↑ ↓	<input checked="" type="checkbox"/>		
Exchange Online	Tous	192.168.1.0	255.255.255.0	Tous	40.104.0.0	255.254.0.0	Tous	accepter	↑ ↓	<input checked="" type="checkbox"/>		
Exchange Online	Tous	192.168.1.0	255.255.255.0	Tous	52.96.0.0	255.252.0.0	Tous	accepter	↑ ↓	<input checked="" type="checkbox"/>		
Exchange Online	Tous	192.168.1.0	255.255.255.0	Tous	131.253.33.215	255.255.255.255	Tous	accepter	↑ ↓	<input checked="" type="checkbox"/>		
Exchange Online	Tous	192.168.1.0	255.255.255.0	Tous	132.245.0.0	255.255.0.0	Tous	accepter	↑ ↓	<input checked="" type="checkbox"/>		
Exchange Online	Tous	192.168.1.0	255.255.255.0	Tous	150.171.32.0	255.255.252.0	Tous	accepter	↑ ↓	<input checked="" type="checkbox"/>		
Exchange Online	Tous	192.168.1.0	255.255.255.0	Tous	204.79.197.215	255.255.255.255	Tous	accepter	↑ ↓	<input checked="" type="checkbox"/>		
Sharepoint/OneDrive	Tous	192.168.1.0	255.255.255.0	Tous	13.107.136.0	255.255.252.0	Tous	accepter	↑ ↓	<input checked="" type="checkbox"/>		
Sharepoint/OneDrive	Tous	192.168.1.0	255.255.255.0	Tous	40.108.128.0	255.255.128.0	Tous	accepter	↑ ↓	<input checked="" type="checkbox"/>		
Sharepoint/OneDrive	Tous	192.168.1.0	255.255.255.0	Tous	52.104.0.0	255.252.0.0	Tous	accepter	↑ ↓	<input checked="" type="checkbox"/>		
Sharepoint/OneDrive	Tous	192.168.1.0	255.255.255.0	Tous	104.146.128.0	255.255.128.0	Tous	accepter	↑ ↓	<input checked="" type="checkbox"/>		
Sharepoint/OneDrive	Tous	192.168.1.0	255.255.255.0	Tous	150.171.40.0	255.255.252.0	Tous	accepter	↑ ↓	<input checked="" type="checkbox"/>		
Proxy cloud	Tous	192.168.1.0	255.255.255.0	Tous	85.115.60.150	255.255.255.255	Tous	accepter	↑ ↓	<input checked="" type="checkbox"/>		
HTTP	TCP	192.168.1.0	255.255.255.0	Tous	Tous	Tous	80	rejeter	↑ ↓	<input checked="" type="checkbox"/>		
HTTPS	TCP	192.168.1.0	255.255.255.0	Tous	Tous	Tous	443	rejeter	↑ ↓	<input checked="" type="checkbox"/>		
FTP	TCP	192.168.1.0	255.255.255.0	Tous	Tous	Tous	21	rejeter	↑ ↓	<input checked="" type="checkbox"/>		
FTP-Data	TCP	192.168.1.0	255.255.255.0	Tous	Tous	Tous	20	rejeter	↑ ↓	<input checked="" type="checkbox"/>		
Tous	Tous	192.168.1.0	255.255.255.0	Tous	Tous	Tous	Tous	rejeter	↑ ↓	<input checked="" type="checkbox"/>		

Et pour finir ne pas oublier de sauvegarder.

## Configuration bornes Wifi UniFi :

Tout d'abord, il faut installer le serveur Unifi (<https://ui.com/download/releases/network-server>) et créer un compte afin de pouvoir configurer et manager les bornes.

A chaque fois qu'une borne est connectée pour la première fois, parmi les onglets à gauche on recherche UniFi Devices où il faut "adopter" la borne.

Une fois les bornes bien allumées et connectées au serveur, il faut créer un nouveau réseau Wifi qui permettra de se connecter aux bornes :

Pour cela, dans les settings et WiFi on fait "Create New" puis on donne un SSID et un mot de passe qui permettra de se connecter aux bornes.

Toute les AP seront sur le même Wifi, en mèche.