SPHINX

Tip Technique

Fiches techniques, FAQ, Conseils

tip@sphinxfrance.fr

maj 14/01/2020

ACCESS ENTRANT : PASSERELLES SIERRA AIRLINK

ACCÉDER À L'ÉQUIPEMENT CONNECTÉ À VOTRE PASSERELLE

Pourquoi ?

- Accéder à des équipements distants (caméras, serveurs, capteurs, automates...)
- Remontée ou mises à jour d'informations (panneaux d'affichage, panneaux solaires...)

Comment ?

Votre abonnement opérateur avec carte SIM vous attribue une adresse IP. Elle peut être soit **privée** ou **publique**.

Cette **adresse est dite privée** si elle n'est **pas accessible directement depuis l'Internet**, ceci renforce la sécurité mais rend impossible toute connexion directe.

Inversement, **une IP publique est directement accessible** et l'accès à votre équipement est possible depuis l'internet. En raison du nombre limité d'adresses publiques, par défaut les opérateurs affectent des IP privées. **Demandez à votre opérateur une option "IP PUBLIQUE".**

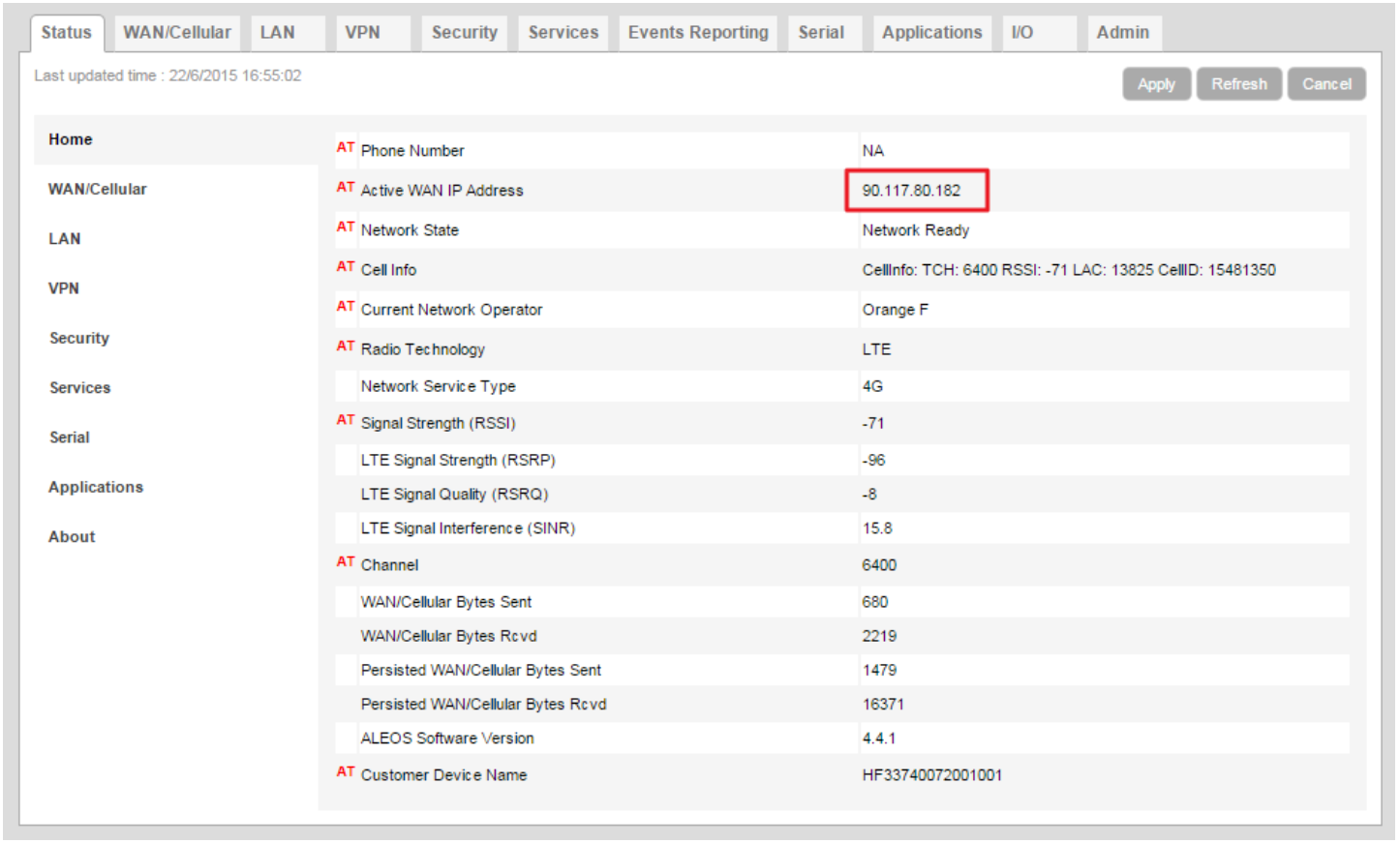
Repérez rapidement si votre IP est privée ? et donc accessible ou non depuis l'Internet...

Le tableau ci dessous indique les adresses IP privées ou réservées, si votre IP est dans cette catégorie, vous devez contacter votre opérateur pour qu'il active l'option IP publique ou qu'il vous indique le bon nom d'APN.

Bloc	Usage	Référence
0.0.0.0/8	*Adresse réseau par défaut*	RFC 1700
10.0.0.0/8	Adresses privées	RFC 1918
100.64.0.0/10	Espace partagé pour Carrier Grade NAT	RFC 6598
127.0.0.0/8	adresse de bouclage (localhost)	RFC 1122
169.254.0.0/16	adresses locales autoconfigurées (APIPA)	RFC 3927
172.16.0.0/12	Adresses privées	RFC 1918
192.0.0.0/24	Réservé par l'IETF	RFC 5736
192.0.2.0/24	Réseau de test TEST-NET-1	RFC 5737
192.88.99.0/24	6to4 anycast	RFC 3068
192.168.0.0/16	Adresses privées	RFC 1918
198.18.0.0/15	Tests de performance	RFC 2544
198.51.100.0/24	Réseau de test TEST-NET-2	RFC 5737
203.0.113.0/24	Réseau de test TEST-NET-3	RFC 5737
224.0.0.0/4	Multicast	RFC 5771
240.0.0.0/4	Réservé à un usage ultérieur non précisé	RFC 1112
255.255.255.255/32	broadcast limité	RFC 919

CONNEXION

La page “status” permet de visualiser l’adresse IP. Dans notre exemple, l’APN “orange.m2m” nous donne une IP publique.



Vérifiez que l'adresse IP Publique est joignable depuis un PC avec connexion internet.

```
>ping 90.117.80.182

Envoi d'une requête 'Ping'  90.117.80.182 avec 32 octets de données :
Réponse de 90.117.80.182 : octets=32 temps=1343 ms TTL=49
Réponse de 90.117.80.182 : octets=32 temps=59 ms TTL=49
Réponse de 90.117.80.182 : octets=32 temps=66 ms TTL=49
Réponse de 90.117.80.182 : octets=32 temps=66 ms TTL=49

Statistiques Ping pour 90.117.80.182:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 59ms, Maximum = 1343ms, Moyenne = 383ms

C:\Users\sergeb>
```

Bien qu'ayant une IP publique, **celle ci reste dynamique sur les réseaux cellulaire** donc attribuée pour une période de temps limitée.

DNS DYNAMIQUE SIERRA : IP MANAGER

RAPPEL

Une adresse peut changer à tout moment. Et ceci dépend de votre fournisseur d'accès. Elle peut changer toutes les 24 heures, toutes les heures, à chaque redémarrage, etc. Dans ce cas, joindre l'IP devient pratiquement impossible. Il faut donc que votre produit soit identifié par un nom. Ce nom (domaine) sera alors géré par un serveur capable de mettre à jour l'IP en face du nom choisi. **C'est le serveur dns dynamique**.

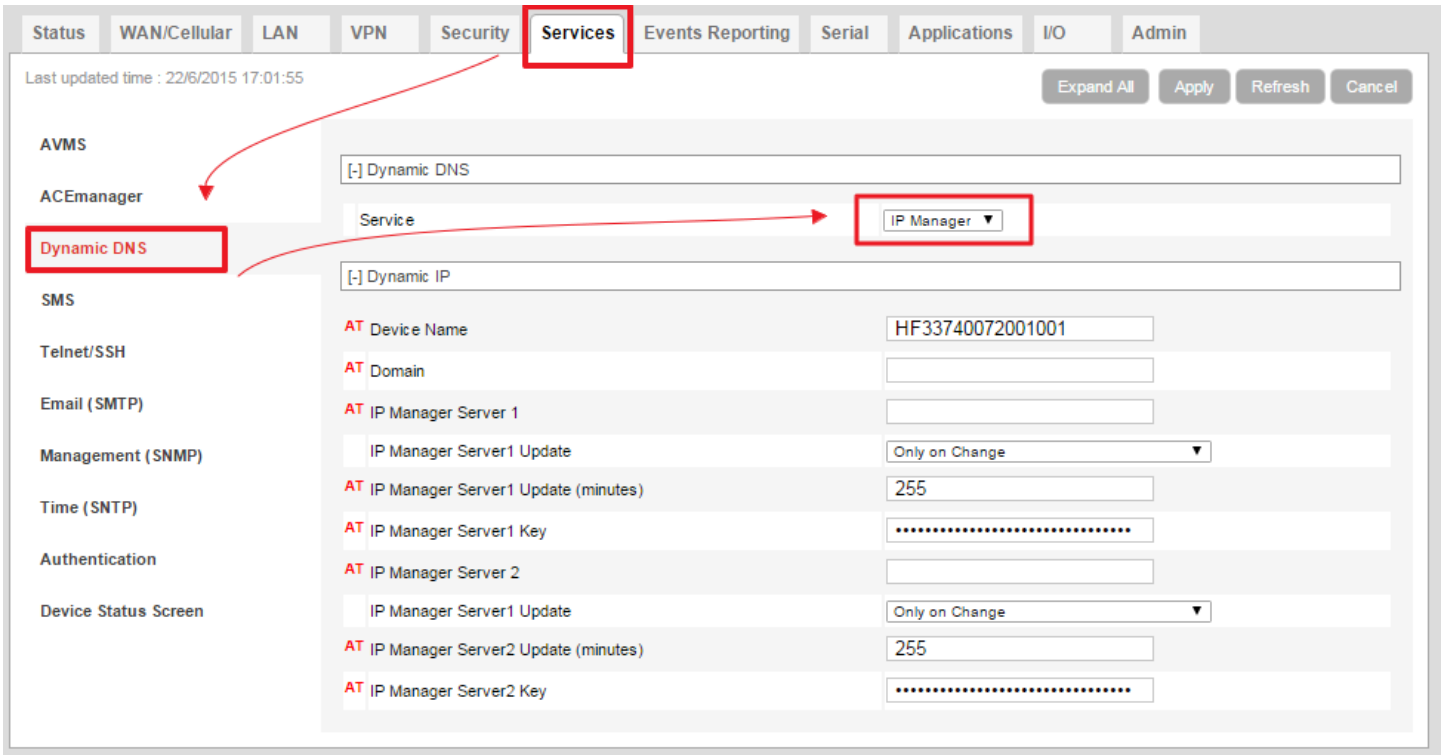
Votre passerelle intègre :

- Un client dns dynamique propriétaire sans incription préalable qui fonctionne avec les serveurs de sierra (ip manager)
- Des clients dynamique DNS de tierce partie >> dyndns, no-ip, ods.org, regfish.com, tzo.com

Nous allons ici décrire le paramétrage du client SIERRA IP manager.

Accédez à l'interface web (http://192.168.13.31:9191)
User Name: user
Password: 12345 **(Paramétres usine)**

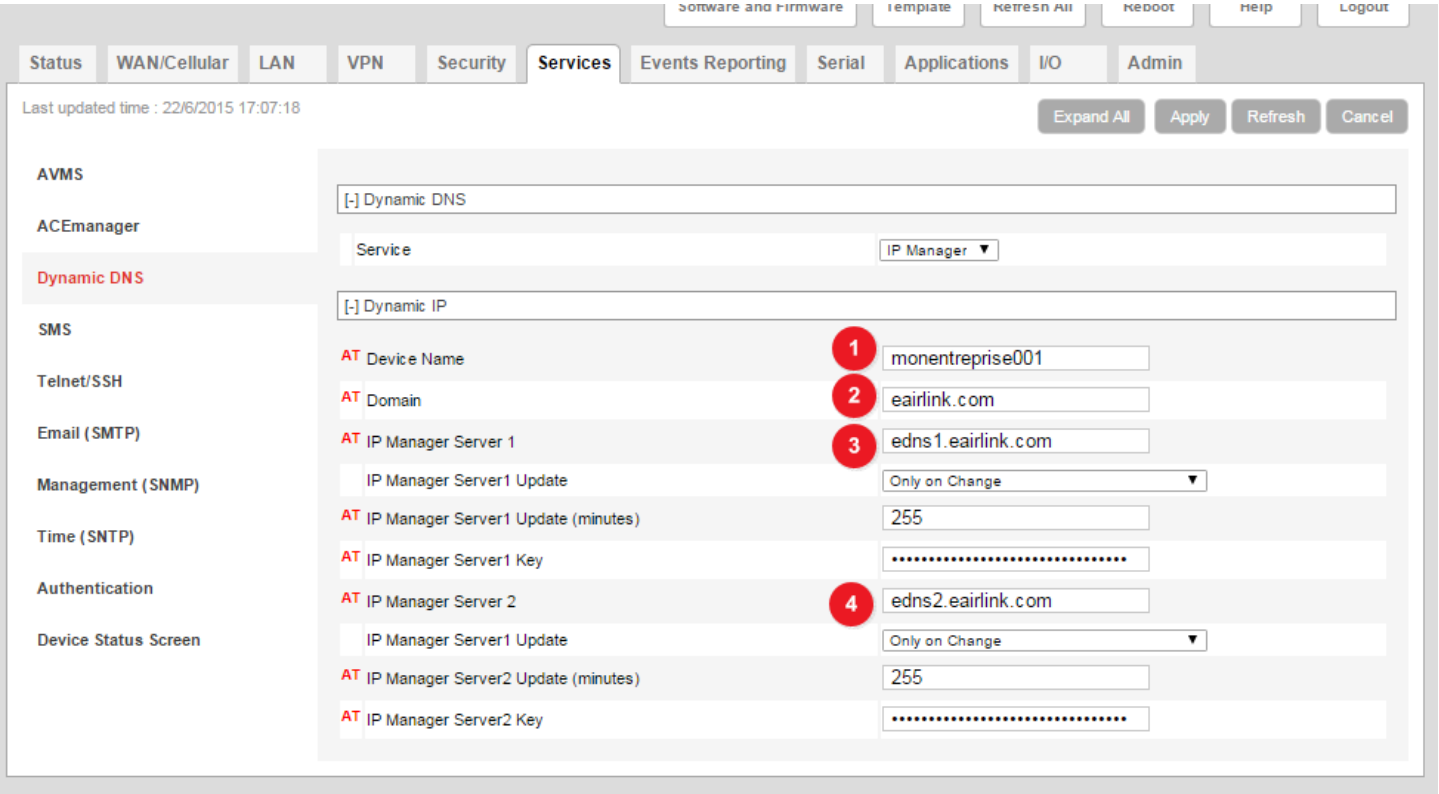
1 - Ouvrez l'onglet < Services >
2 - Cliquez sur le lien < Dynamic DNS >
3 - En face de "Service < IP Manager >



1 - En face de "Device Name" (par défaut, le nom correspond au numéro de série du produit). Il n'y a pas de vérification de doublons, donc mettez un nom **unique mais simple à se rappeler, nom de votre société suivi par exemple d'un numéro (pas d'espace et < à 20 caractères).**

2 - En face de “Domain”, tapez **eairlink.com (nom du domaine utilisé par sierra)**
3 - En face de “ IP Manager Server 1”, tapez **edns1.eairlink.com**
4 - En face de “ IP Manager Server 2”, tapez **edns2.eairlink.com**

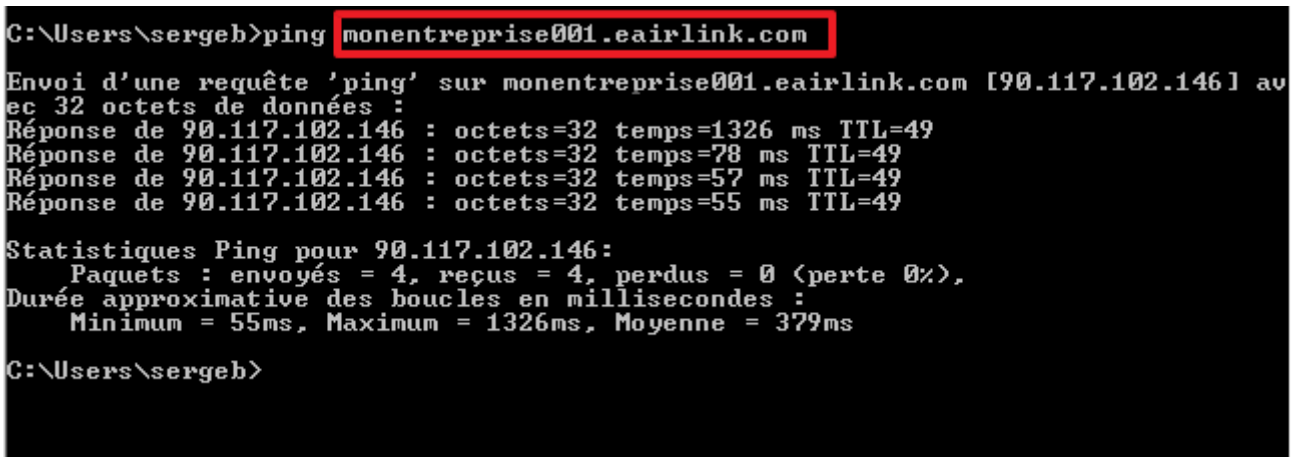
(Attention: ne pas modifier les autres champs, il s’agit des clés d’authentification du serveur distant)



“Apply” puis “Reboot” pour la prise en compte
Attendez le redémarrage de votre passerelle (2 minutes pour la série LS300).

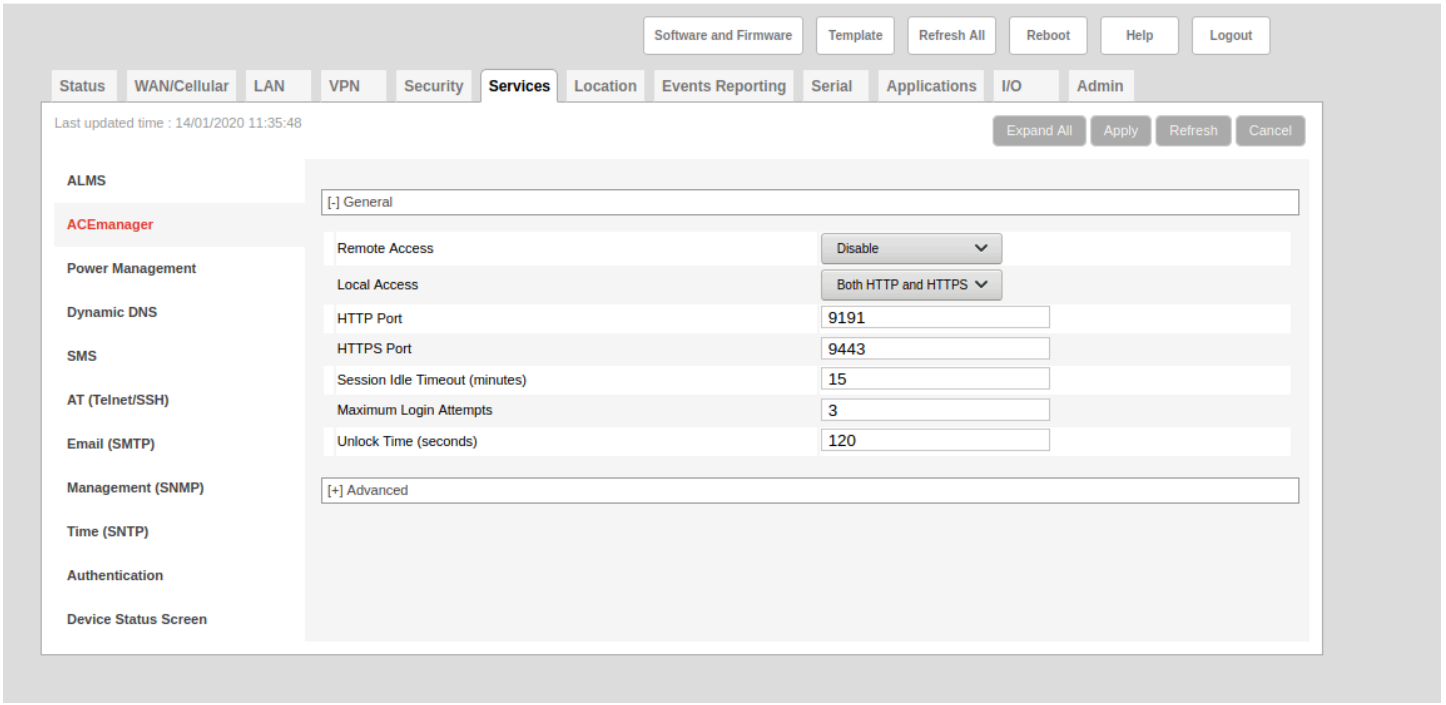
Votre passerelle est désormais joignable sur son nom de domaine depuis n'importe quel accès internet (ex: http://nomentreprise003.eairlink.com:9191) et même si l’adresse change.

vérification par la commande “ping” :



Services / Acemanager

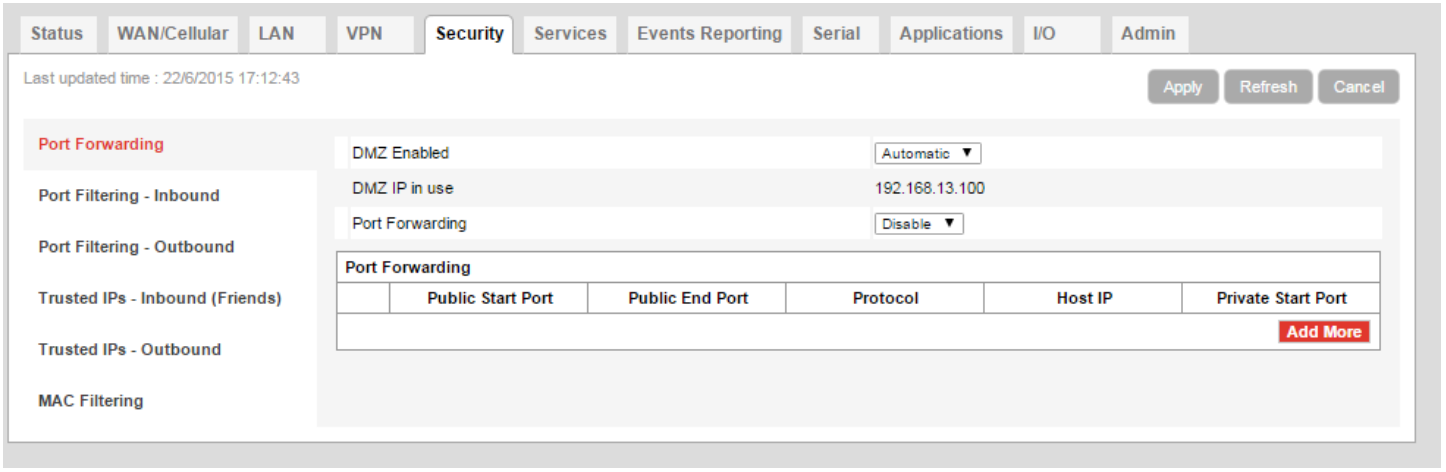
Par défaut l'accès remote est désactivé sur le produit, pensez à l'activer via HTTPS only , ou both (HTTP+HTTPS)



SECURITY - PORT FORWARDING (redirection de port)

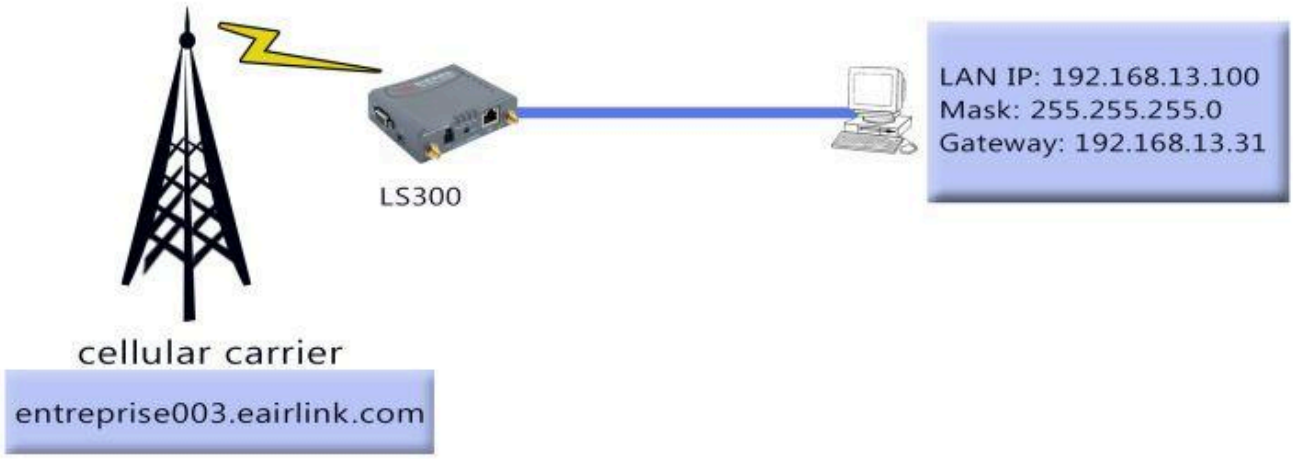
Pour accéder à vos équipements distants, il faut configurer le produit pour qu'il "redirige" les paquets vers le ou les équipements de votre réseau privé.

1 - Cliquez sur l'onglet "Security"
2 - Choisissez "Port Forwarding"



DMZ : Zone Démilitarisée, elle correspond à l'ouverture de tous les ports de la passerelle vers une adresse ip du réseau local.

Les ports entrants sont mappés à l'identique sur l'adresse DMZ, une connexion sur le port 80 protocole TCP vers nomentreprise001 sera redirigé vers l'équipement 192.168.13.100 sur le port 80 protocole TCP



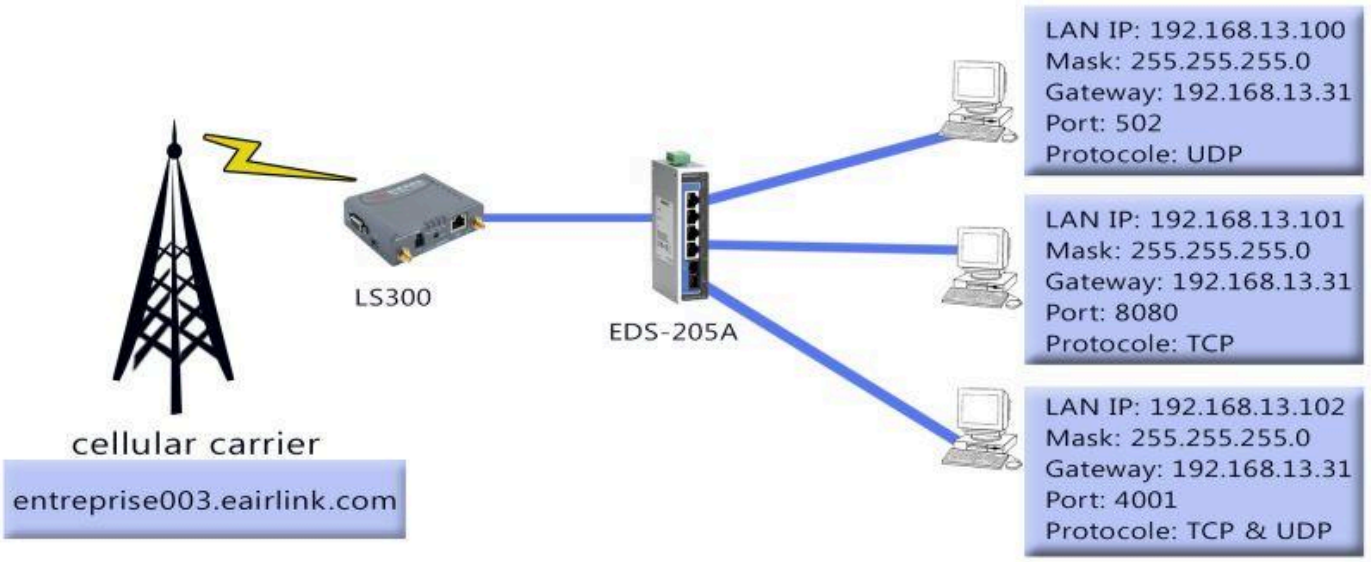
Attention par défaut, une DMZ est active et redirige les données vers l'adresse 192.168.13.100 (1ère adresse IP fournie par le serveur DHCP de votre passerelle)

Port Forwarding: permet de rediriger un port ou une plage de ports vers une adresse IP précise et vers un port précis. Vous pouvez donc avoir plusieurs équipements (automates, serveurs, caméras...) en réception de l'adresse publique en précisant des ports différents.

Toutes les requêtes vers l'adresse opérateur (nomentreprise001.eairlink.com) seront renvoyées en fonction de vos règles de redirection vers les équipements désirés.

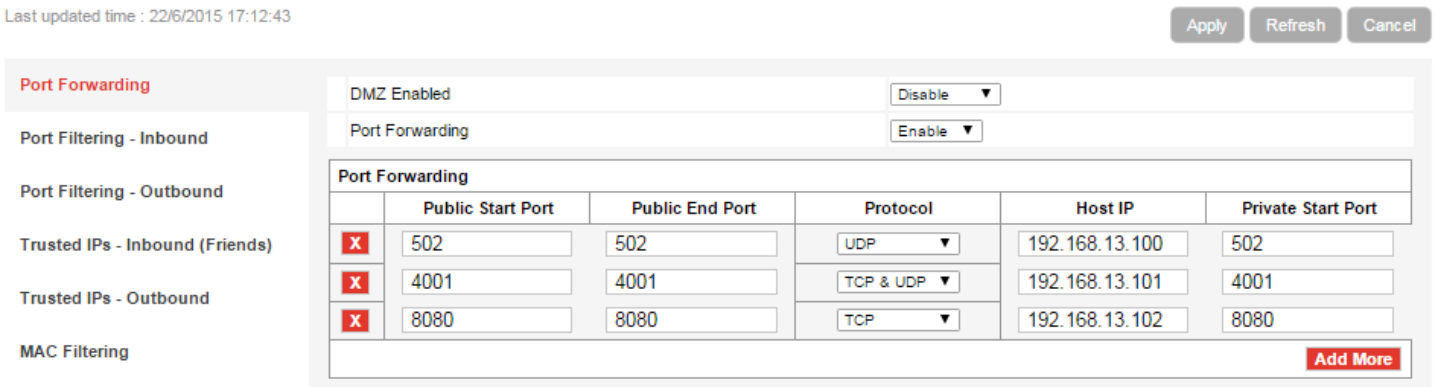
Exemple de connexion sur **nomentreprise001.eairlink.com**

Une connexion sur le port 502 UDP sera redirigée vers l'équipement 192.168.13.100 port 502 UDP
Une connexion sur le port 4001 TCP et/ou UDP sera redirigée vers l'équipement 192.168.13.101 port 4001 TCP et/ou UDP
Une connexion sur le port 8080 TCP sera redirigée vers le l'équipement 192.168.13.102 port 8080 TCP



Paramétrage:

1. Désactivez la fonction DMZ : "Disable"
2. Activez le Port Forwarding: "Enable"
3. Choisissez le port de début (**Public Start Port**)
4. Choisissez le port de fin (**Public End Port**)
5. Choisissez le protocole utilisé (TCP, UDP ou les deux)
6. Choisissez l'adresse IP de destination (adresse IP de l'équipement devant être accessible)
7. Choisissez le port de début pour l'adresse de destination (**Private Start Port**)
8. Cliquez sur "Add More" pour créer d'autres règles de redirection



Cliquez sur "Apply" puis sur "Reboot" pour la prise en compte des paramètres.