

# TUTORIEL ACCES EXTERNE JEEDOM EN SSL

(et SURTOUT : comment se passer du loopback des box)

## Prérequis :

- NAS Synology
- Livebox (ou autre box internet de n'importe quel FAI)
- Disposer d'un domaine de type « mondomaine.com » auprès de OVH ou autre service identique, et créer un sous-domaine de type « jeedom.mondomaine.com », lien vers tuto OVH : <https://docs.ovh.com/fr/domains/utilisation-dynhost/>
- Activer ou disposer de l'accès en SSL à son Jeedom (vérifier qu'on accède à Jeedom en HTTPS sur le réseau local même si l'on a un message d'erreur à propos du certificat, il sera résolu par ce tutoriel)

## Objectif du tutoriel :

Enlever quasiment toute la gestion du réseau par la box (il est pratique de ne plus être lié à la configuration réseau de la BOX et parce que beaucoup de box empêchent le loopback... et puis on ne va pas se mentir : PARCE QUE LES BOX SONT DES BROUETTES ET QU'ELLES SONT LIMITEES DANS LEURS FONCTIONNALITES ^^) + faire gérer une grande partie au NAS (DNS / DHCP / Certificat)

## Informations complémentaires :

Certaines indications de ce tuto sont soumises à personnalisation et ne peuvent être saisies directement telles quelles :

- Le sous domaine : jeedom.mondomaine.com est à personnaliser
- Les IP des appareils : BOX en 192.168.1.1 / NAS en 192.168.1.8 / JEEDOM sont à adapter en fonction de l'adressage IP du réseau local (idem pour les DNS en fonction du FAI)

---

Auteur :

k6

---

# 1. Configuration de la Box internet :

En premier lieu, il va falloir ouvrir les ports de la box + désactiver le DHCP.

Se connecter à l'interface de sa box (captures d'écran pour Livebox 4, mais les manipulations se ressemblent entre toutes les box : le principe reste identique).

Tout d'abord, désactiver le DHCP de la BOX :

Retour **Réseau**

DHCP NAT/PAT DNS UPnP DynDNS DMZ NTP IPv6

Le serveur DHCP de votre Livebox attribue automatiquement une adresse IP à chaque équipement de votre réseau local.  
Uniquement pour des équipements IPv4.

---

### Paramètres du serveur DHCP

Activer le serveur DHCP

Adresse IP de votre Livebox

Masque de sous-réseau du LAN

Adresse IP de début

Adresse IP de fin

Créer les règles NAT sur le port 80 et 443 pointant vers le NAS :

**Retour Réseau**

DHCP NAT/PAT DNS UPnP DynDNS DMZ NTP IPv6

Les règles NAT/PAT sont nécessaires pour autoriser une communication initiée depuis Internet avec un équipement particulier de votre réseau. Utiles pour certaines applications comme des jeux en lignes ou des serveurs de type FTP ... Assurez-vous que cet équipement a une adresse IP statique (paramétrable dans l'onglet DHCP).  
Uniquement pour des équipements IPv4.

Vos règles personnalisées

Choisissez des ports qui ne sont pas bloqués par le pare-feu.  
Nous vous déconseillons la création d'une règle sur le port 53 (service DNS).  
Les équipements doivent être configurés avec une adresse IP statique pour être disponibles.

FTP Server 21 21 TCP Toutes Créer  
ex. : 1000 ex. : 1000-2000 IP externes autorisées

Activer	Application/Service	Port interne	Port externe	Protocole	Équipement	IP externe	
<input checked="" type="checkbox"/>				TCP/UDP		Toutes	
<input checked="" type="checkbox"/>	Web Server (HTTP)	80	80	TCP/UDP	DS1517	Toutes	
<input checked="" type="checkbox"/>	Secure Web Server (HTTPS)	443	443	TCP/UDP	DS1517	Toutes	
<input checked="" type="checkbox"/>				TCP/UDP		Toutes	

Dans le cas d'une Livebox 4, on ne peut pas spécifier d'adresse IP en destination mais uniquement un équipement, pour cela, il faut que l'équipement soit détecté par la BOX, aller dans « mes équipements connectés », trouver le NAS et le nommer à sa convenance :

**Retour Mes équipements connectés**

Carte Liste

Wi-Fi Ethernet

Paramétrer l'équipement

Type d'équipement NAS

nom DS1517

Adresse IP 192.168.1.8

Adresse MAC

Connexion Internet connecté

Paramétrer son accès à Internet

Autoriser en permanence  
 Bloquer en permanence  
 Planifier

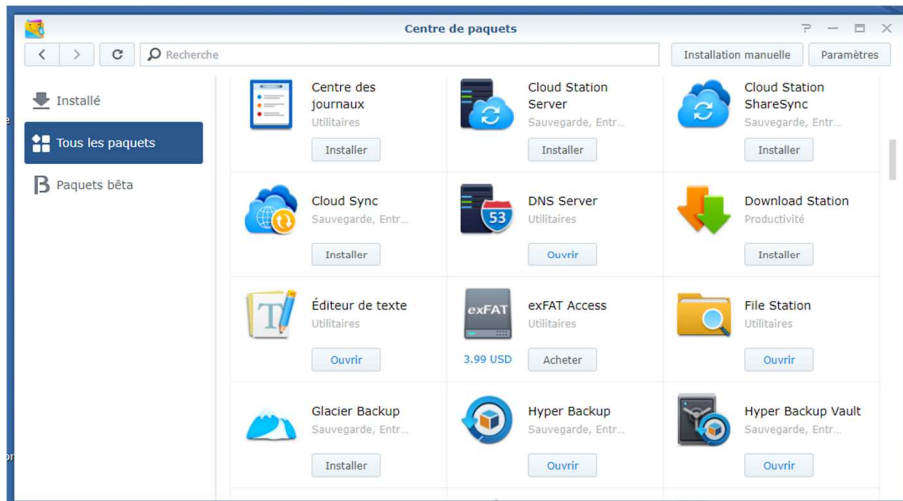
Annuler Enregistrer

DS1517 DS214se Google-Home Google-Nest NVIDIA SHIELD

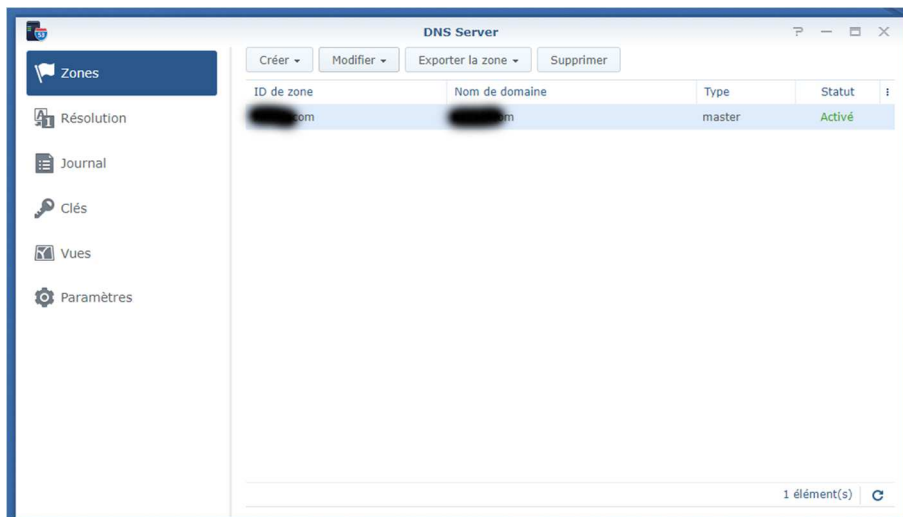
## 2. Configuration du NAS Synology :

Dans un second temps, il va falloir basculer les rôles de DNS / DHCP au NAS et ensuite mettre en place la gestion des certificats et du proxy inversé.

Se connecter à l'interface du NAS par le DSM, et installer le paquet « DNS Server » par le biais du « centre de paquets » :



Paramétrages du DNS sur le NAS :



Créer une zone DNS comme ci-dessous avec « mondomaine.com » :

### Modifier les paramètres de zone

ID de zone: [redacted] .com

Nom de domaine: [redacted] .com

Statut: Activer ▼

Format série: Nombre entier ▼

Limiter le transfert de zone

Spécifiez quelles zones slave peuvent demander les fichiers de zone de cette zone master.

Règle de transfert de zone

Limiter le service IP source

Spécifiez quels hôtes peuvent interroger le serveur DNS sur cette zone.

Liste d'IP source

Activer la notification des zones esclaves

Spécifiez quelles zones esclaves doivent être notifiées lorsque la zone principale de ce serveur DNS change.

Liste des IP des zones esclaves

Limiter la mise à jour de zone

Spécifiez les clients qui peuvent demander une mise à jour de zone à partir de cette zone principale.

Règle de mise à jour de zone

OK Annuler

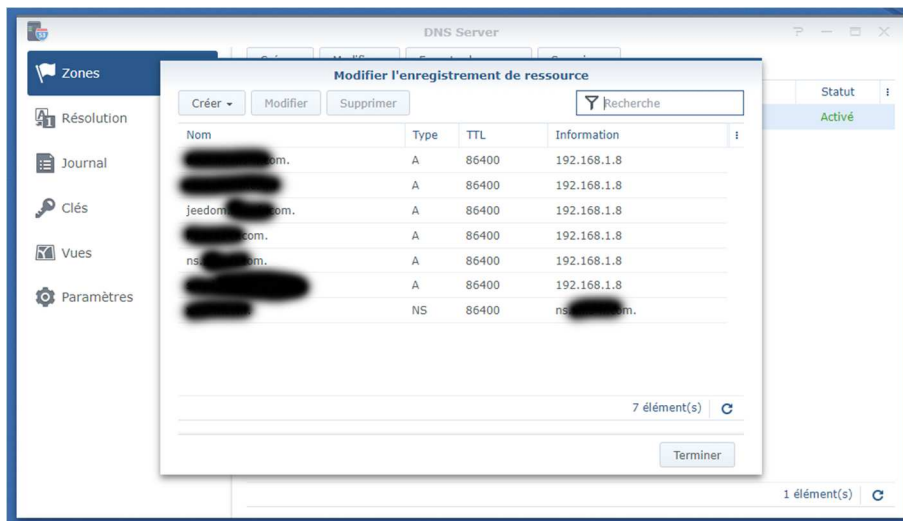
Cocher la case « limiter le service IP source » et renseigner le réseau local de type « 192.168.1.0 » :

Type	Liste d'IP source
Sous-réseau	192.168.1.0/255.255.25...

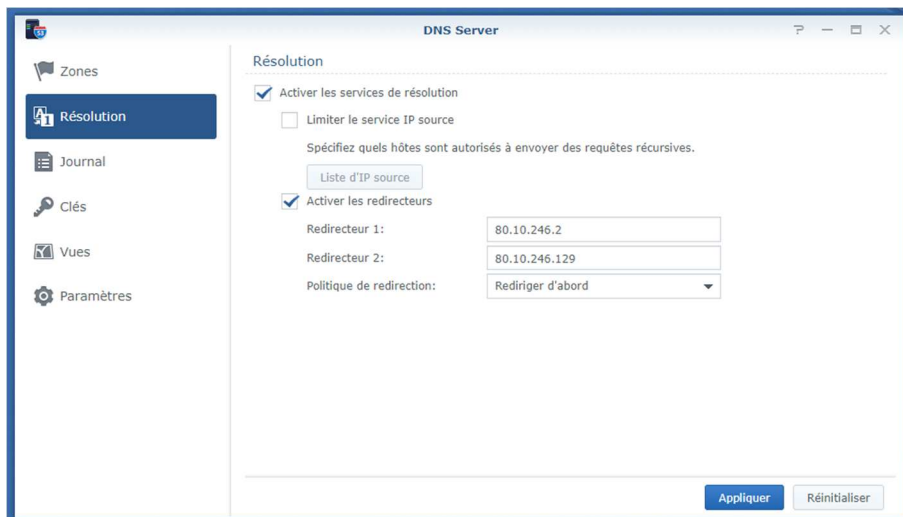
Paramétrer la rubrique « enregistrement de ressource » :

ID de zone	Type	Statut
[redacted]	master	Activé

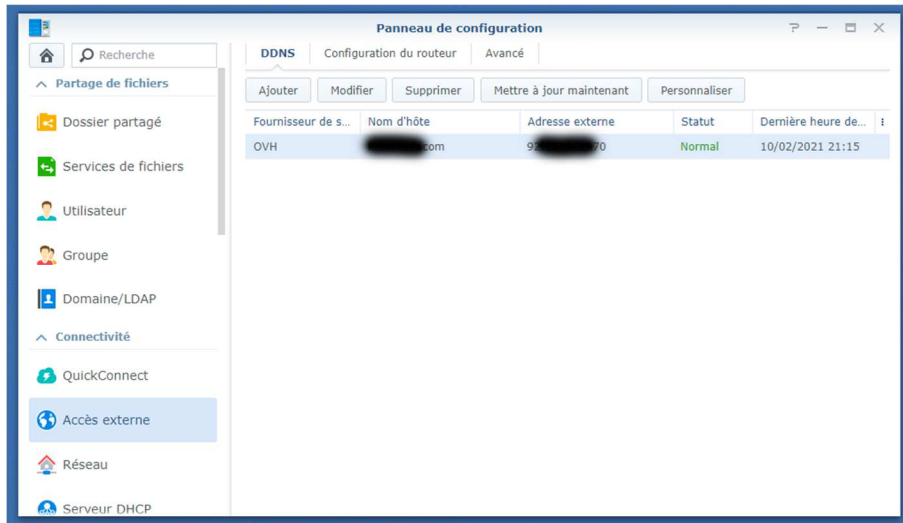
Faire pointer le sous domaine de type « jeedom.mondomaine.com » vers l'IP locale du NAS :



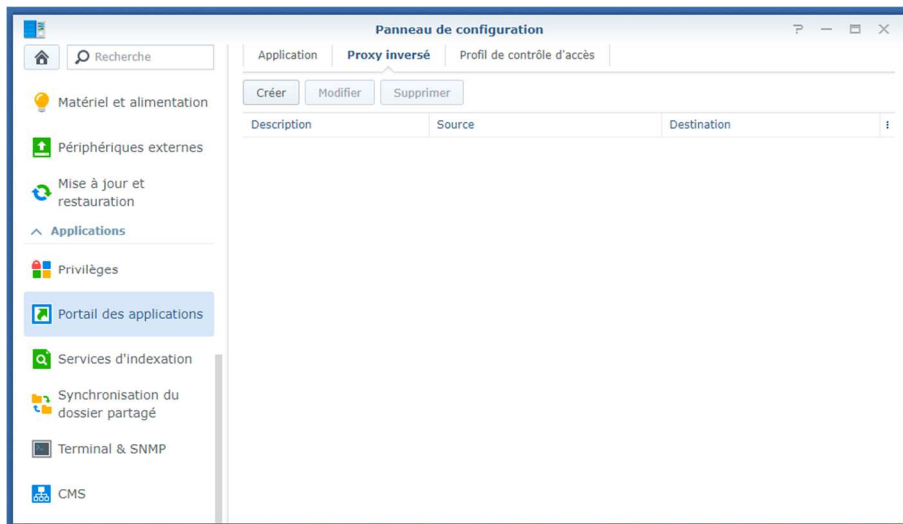
Dans la rubrique « Résolution », cocher « Activer les services de résolution » + « Activer les redirecteurs », et indiquer les DNS de votre FAI (sur la capture ce sont les DNS d'Orange) :



Aller dans « Panneau de configuration » du DSM puis dans la rubrique « Accès externe », Ajouter le DDNS de type « jeedom.mondomaine.com » avec son utilisateur et mot de passe, et cliquer sur « mettre à jour maintenant », le NAS détectera le changement d'IP et le mettra à jour automatiquement par la suite :



Aller dans la rubrique « portail des applications », puis « Proxy inversé », puis cliquer sur « créer » :





Renseigner le sous-domaine « jeedom.mondomaine.com » dans description et nom d'hôte + protocole « HTTPS » et port « 443 » dans source et destination + cocher la case « activer HTTP/2 » + renseigner l'IP locale de Jeedom de type « 192.168.1.X » :

**Règles de proxy inversé** [X]

**Général** | En-tête personnalisé | Paramètres avancés

Proxy inversé

Description: jeedom.mondomaine.com

Source

Protocole: HTTPS

Nom d'hôte: jeedom.mondomaine.com

Port: 443

Activer HSTS

Activer HTTP/2

Activer le contrôle d'accès

Profil de contrôle d'accès: [dropdown] ⓘ

Destination

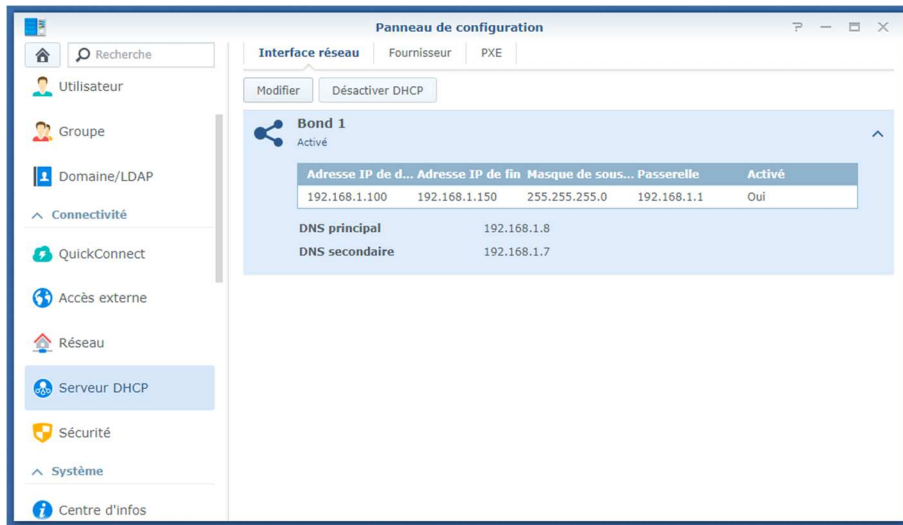
Protocole: HTTPS

Nom d'hôte: 192.168.1.X

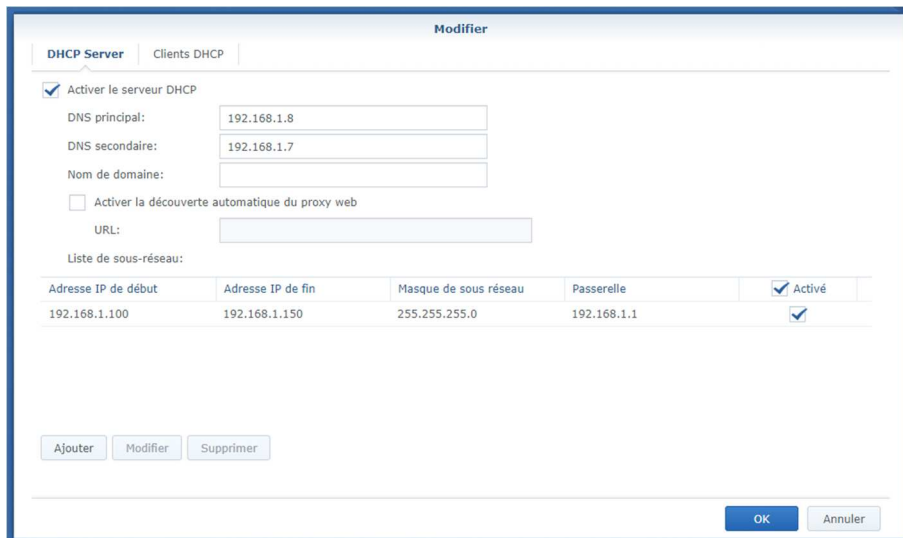
Port: 443

OK Annuler

Aller dans la rubrique « Serveur DHCP », localiser la carte réseau sur laquelle est connectée le NAS au réseau (sur la capture suivante, c'est un agrégat de 4 cartes réseaux, mais on a habituellement LAN1, LAN2, etc.), cliquer sur « Modifier » :



Cocher « Activer le serveur DHCP », renseigner l'IP du NAS en principal et le DNS du FAI en secondaire (sur la capture, j'ai un autre NAS qui fait DNS secondaire, ce qui explique une IP locale) :



Cocher « Ajouter » puis spécifier l'adresse IP de début + IP de fin + Masque + Passerelle (IP de votre BOX) + le bail en secondes (sur la capture le bail équivaut à 8 jours) puis valider par OK :

Modifier le sous-réseau DHCP

Adresse IP de début: 192.168.1.100

Adresse IP de fin: 192.168.1.150

Masque de sous réseau: 255.255.255.0

Passerelle: 192.168.1.1

Durée de bail de l'adresse: 691200

Options DHCP:

Activé	Co...	Nom	Valeur
<input type="checkbox"/>	7	log-server	
<input type="checkbox"/>	9	lpr-server	
<input type="checkbox"/>	13	boot-file-size	
<input type="checkbox"/>	16	swap-server	
<input type="checkbox"/>	17	root-path	
<input type="checkbox"/>	18	extension-path	

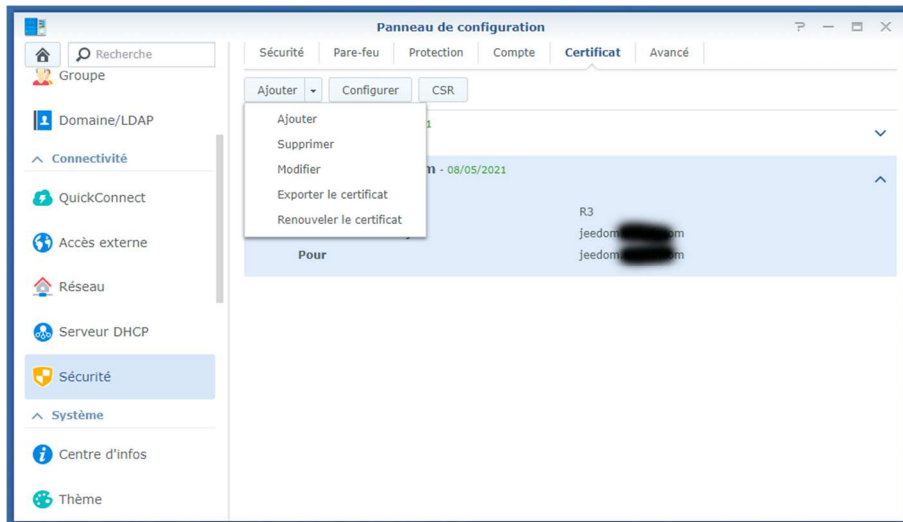
Dans la rubrique DHCP, il est possible de fixer les adresses IP des clients en cliquant sur le cadenas :

Actualiser Ajouter Modifier Effacer Clients DHCP

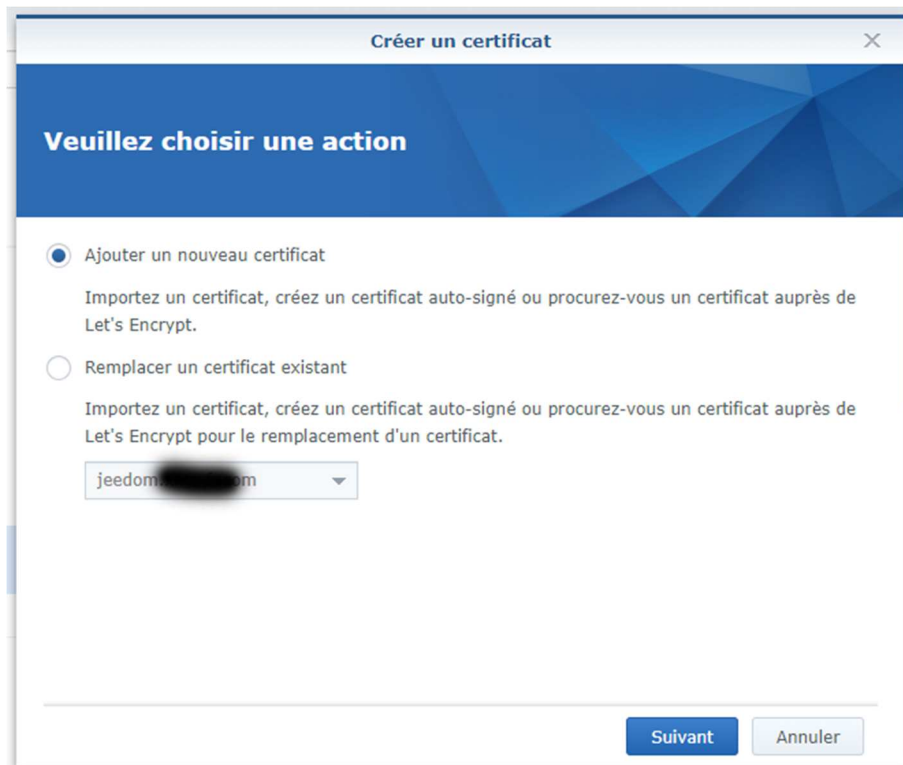
Ajouter à la réservation d'adresse	IP	MAC/DUID	Nom d'hôte	Expiré dans
	192.168.1.102	c8...	RMMini3	0 jour(s) 18 heure(s)...
	192.168.1.111	d4...	CLIMATISATION	0 jour(s) 15 heure(s)...
	192.168.1.116	e4...	FI...	5 jour(s) 3 heure(s) ...

Remarque: Réservez l'adresse IP pour le périphérique actuel en cliquant sur l'icône du verrou.

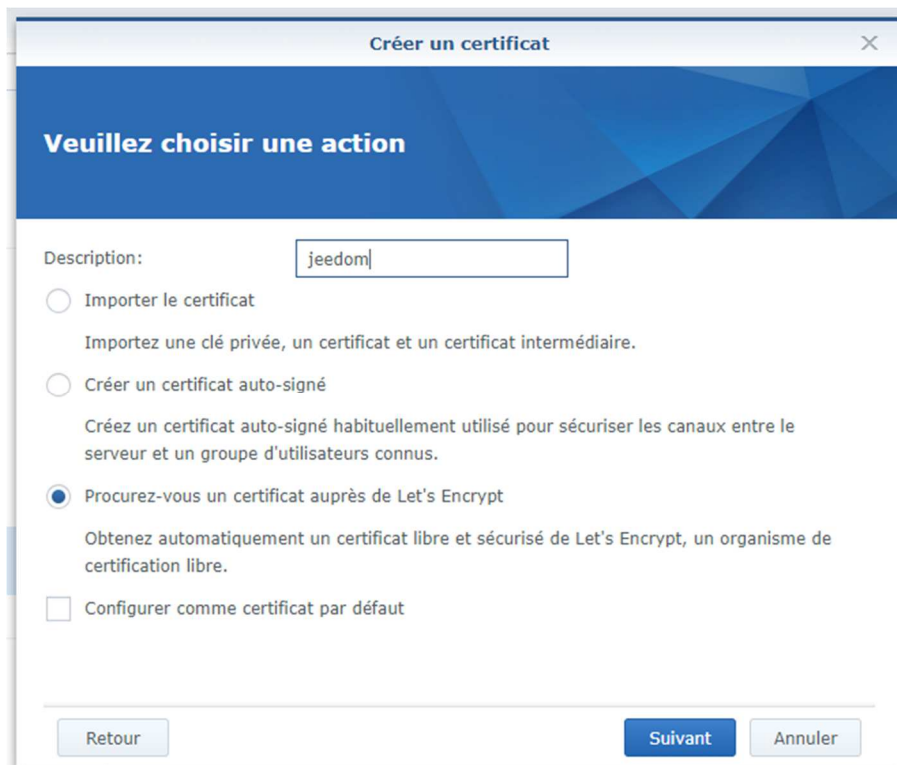
Aller dans la rubrique « Sécurité », puis dans « Certificat », afin d'ajouter le certificat Let's Encrypt (ne pas supprimer le certificat racine du NAS Synology) :



Choisir « Ajouter un nouveau certificat » :

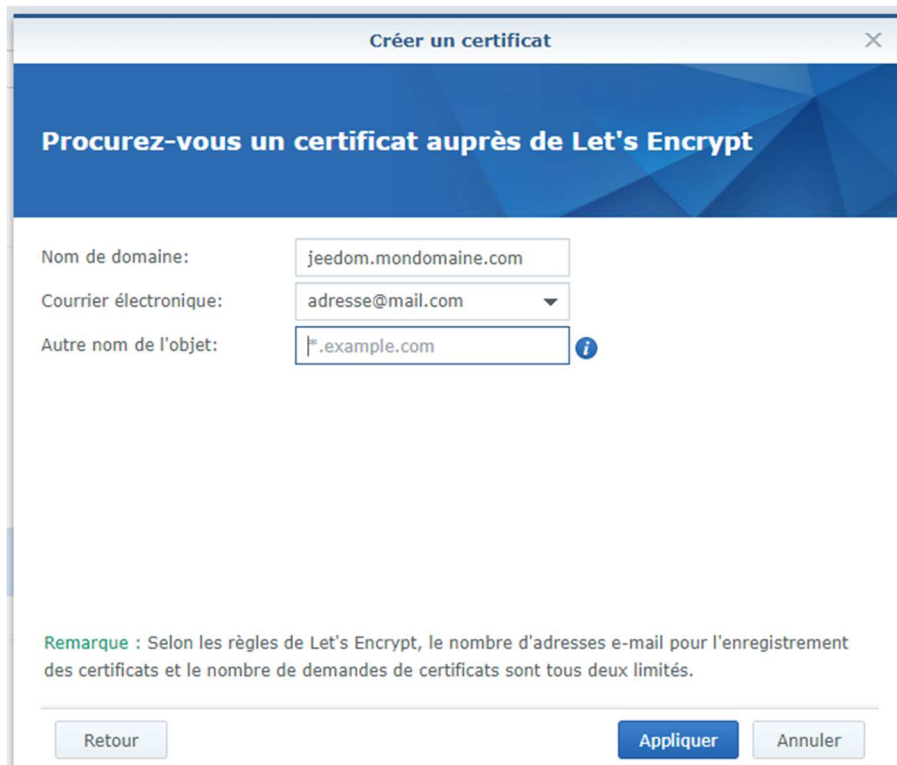


Saisir sa description, ex : jeedom, et cocher « Procurez-vous un certificat auprès de Let's Encrypt » :



The screenshot shows a dialog box titled "Créer un certificat" with a close button (X) in the top right corner. The main heading is "Veuillez choisir une action". Below this, there is a "Description:" label followed by a text input field containing "jeedom". There are three radio button options: "Importer le certificat" (unselected), "Créer un certificat auto-signé" (unselected), and "Procurez-vous un certificat auprès de Let's Encrypt" (selected). Below the selected option is a sub-heading "Obtenez automatiquement un certificat libre et sécurisé de Let's Encrypt, un organisme de certification libre." There is also an unchecked checkbox labeled "Configurer comme certificat par défaut". At the bottom, there are three buttons: "Retour", "Suivant", and "Annuler".

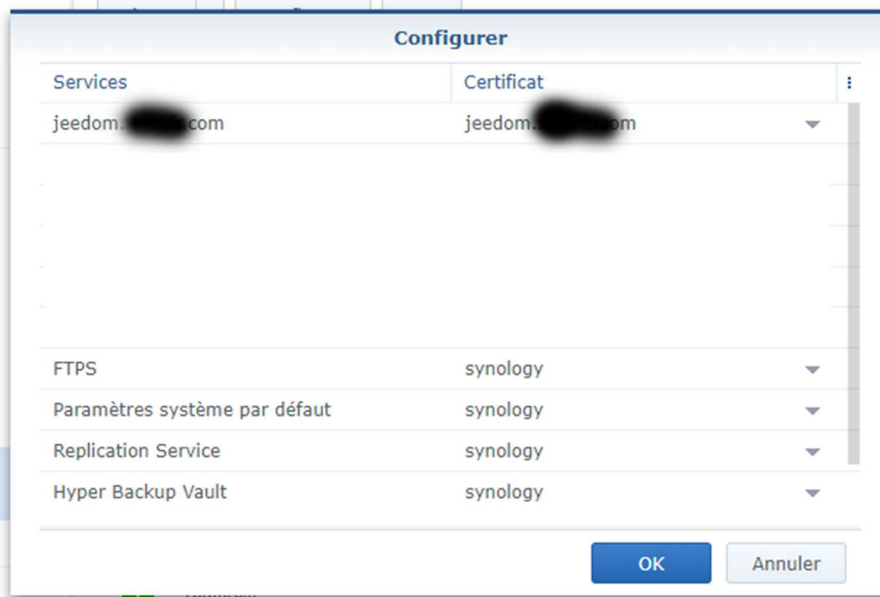
Saisir le nom du sous-domaine « jeedom.mondomaine.com » + adresse mail valide, et cliquer sur « appliquer » :



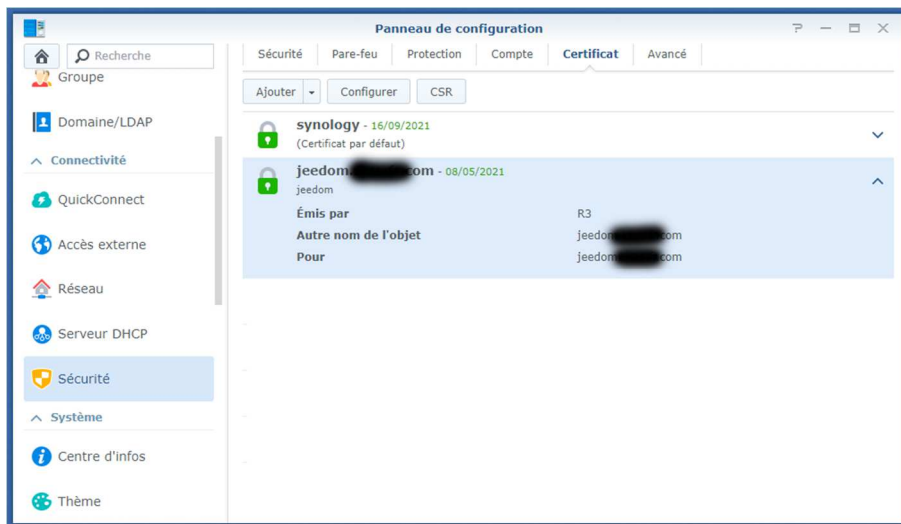
The screenshot shows the same dialog box, but now the heading is "Procurez-vous un certificat auprès de Let's Encrypt". The "Description:" field is empty. There are three input fields: "Nom de domaine:" with "jeedom.mondomaine.com", "Courrier électronique:" with "adresse@mail.com" (and a dropdown arrow), and "Autre nom de l'objet:" with ".example.com" (and an information icon). At the bottom, there are three buttons: "Retour", "Appliquer", and "Annuler".

**Remarque :** Selon les règles de Let's Encrypt, le nombre d'adresses e-mail pour l'enregistrement des certificats et le nombre de demandes de certificats sont tous deux limités.

Une fois le certificat créé, il faut l'associer au service adéquat, cliquer sur « configurer » puis associer le certificat au service jeedom (ne pas toucher aux autres services) :



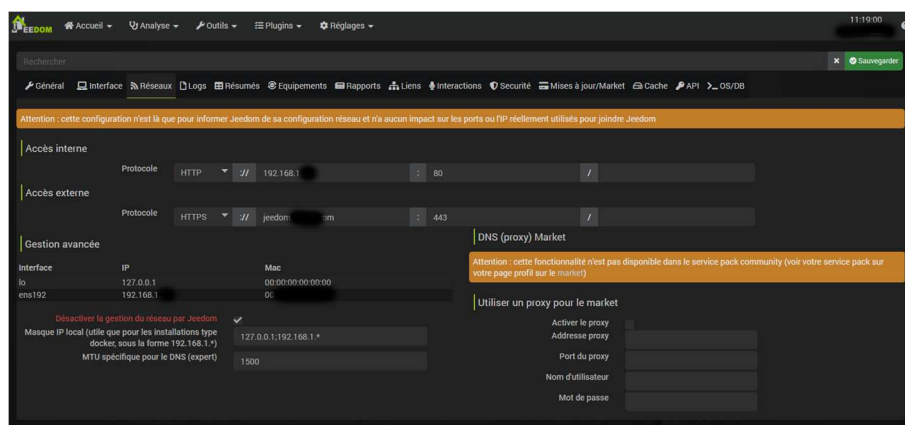
Le certificat se renouvellera automatiquement, il n'y a rien à faire \o/



### 3. Configuration de l'adresse externe de Jeedom :

Enfin, il suffira de finaliser la configuration de Jeedom afin qu'il connaisse son adresse externe.

Se connecter à Jeedom par l'adresse IP depuis le réseau local en HTTP puis aller dans « Réglages / Système / Configuration » puis « réseaux », et renseigner le « jeedom.mondomaine.com » en HTTPS et port 443, puis « Sauvegarder » :



Jeedom est désormais accessible avec certificat en SSL depuis l'adresse externe (https://jeedom.mondomaine.com), et ce, aussi bien en interne du réseau ou en externe depuis internet sans que le loopback soit nécessaire et sans erreur de certificat du navigateur...

Le NAS s'occupe de rediriger les requêtes aussi bien sur le réseau local que depuis internet et on a la main sur le DHCP / DNS / Certificats.

Nul besoin de deux raccourcis sur les PC fixes / PC portables / téléphones / tablettes avec soit IP soit domaine : UN SEUL LIEN => l'adresse externe de Jeedom en SSL \o/ ENJOY 😊