Tuto accès externe au NAS avec ouverture minimale de ports

# PITCH

Vous voulez accéder à votre NAS et à ses différentes applications (Drive, Moments, Vidéo Station, etc.) depuis l’extérieur sans avoir à ouvrir un port pour chaque application, que ça soit simple pour vous et les utilisateurs, et faire ça de façon la plus sécurisée possible.

# PRESENTATION

Le but de ce tuto est de présenter une technique permettant de concilier deux contraintes souvent opposées, qui sont la Sécurité et la Facilité d’utilisation, quand on veut accéder depuis l’extérieur à notre NAS et à ses principales applications, dans un cadre Domestique ou SoHo. Or, qui dit « accès depuis l’extérieur » dit « Sécurité » . Et Sécurité signifie généralement obligations et complications pour l’utilisateur. C’est pourquoi, grâce aux conseils recueillis sur le groupe Facebook « NAS-Forum » , « NAS Synology Francophone » et « Usagers Synology en Francophonie » , et en premier lieu - ils se reconnaîtront, je ne les nomme pas complètement par souci de vie privée - l’aide de E Lagarde et Ro HL. On présentera donc ici une technique qui permet de n’ouvrir qu’un seul port sur l’extérieur, tout en permettant un accès tout simple à n’importe quel utilisateur référencé ou invité, depuis un simple navigateur Web, sans aucun autre logiciel à installer (mis à part un Authentificator si vous utilisez la 2FA - cf Web - ce que je conseille).

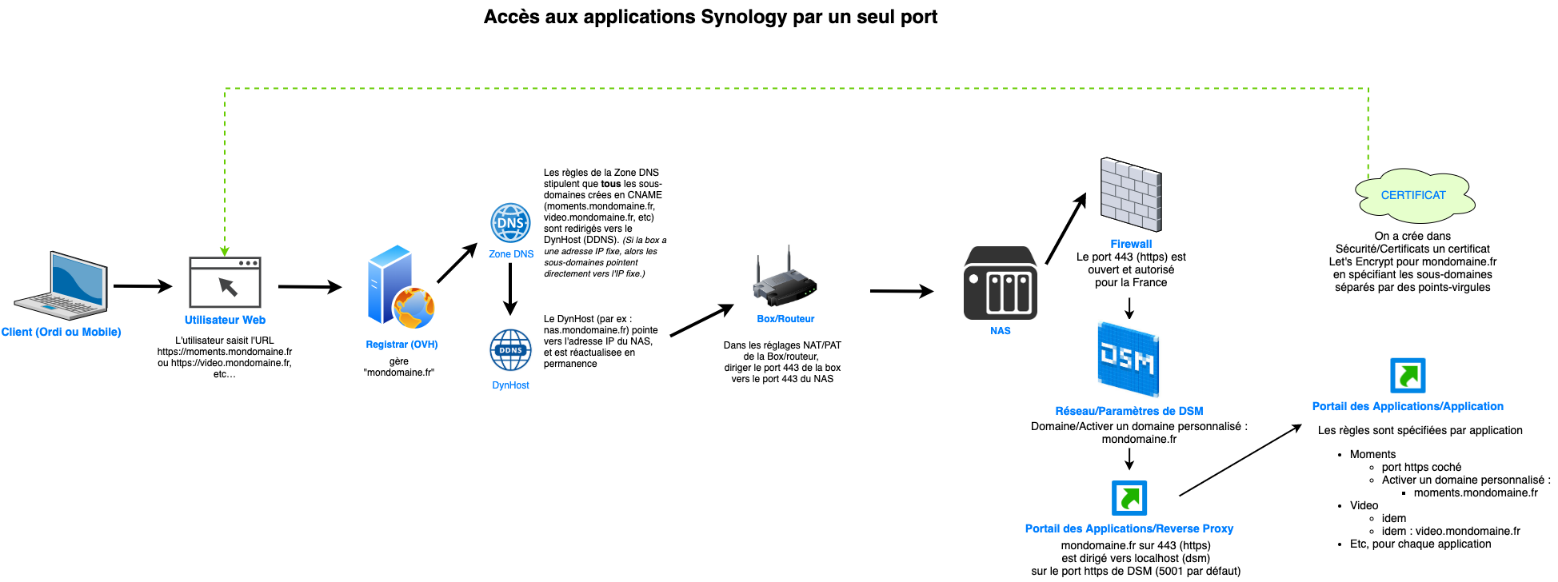
Dans notre cas, on part du principe que vous voulez pouvoir octroyer la possibilité à votre familles et amis (usage domestique) et/ou collaborateurs, clients et collègues (usage SoHo), d’accéder aux photos sur l’Applications Moments, ou aux fichiers par Drive, ou aux vidéos par Video Station, etc. Et pour ce faire, vous voulez utiliser votre nom de domaine (NDD) tel que mondomaine.fr, et même, on va montrer comment on peut éviter d’avoir à compliquer la vie des utilisateurs (on va éviter www.mondomaine.fr/10002) en leur permettant un accès facile à mémoriser, tel que :

* <https://moments.mondomaine.fr>
* <https://video.mondomaine.fr>
* <https://drive.mondomaine.fr>
* <https://audio.mondomaine.fr>
* etc…

Ce tuto s’appuie sur les infos contenues dans les principaux tutos sur le sujet :

* celui de Fenrir sur NAS-Forum.com, incontournable.
* celui de Kawamashi sur NAS-Forum, couvrant le Reverse Proxy.
* https://nas.maison
* https://leblogdejerome.com/2018/08/ajouter-un-nas-synology-a-un-dynhost-chez-ovh/
* https://www.adrienfuret.fr/2015/05/31/nas-synology-ddns-ovh/
* https://www.lucasehlinger.com/lier-un-nom-de-domaine-a-son-nas-synology/

# PLAN

PRÉ-REQUIS

Aucun tuto ne peut couvrir l’ensemble des connaissances nécessaires, on ne va pas décrire comment marche une souris ni non plus ellipser des points cruciaux : on part donc du principe que le lecteur a un ordinateur et un NAS Synology en état de marche. Il existe plein de tutos disponibles et très bien faits (Google est là pour ça), l’idée n’est donc pas d’être redondant avec ce qui existe, mais de présenter une technique peu ou pas assez facilement documentée, et qui mérite qu’on s’y intéresse. On se concentre donc ici sur la partie originale, pas sur ce qui est multi-documenté partout ailleurs (à chaque fois qu’une partie est évoquée ailleurs, la mention « cf Web » sera ajoutée).

Je ne peux que conseiller, d’emblée, de suivre, pour tout possesseur de NAS, le tuto de Référence par Fenrir pour sécuriser son NAS, avant toute chose.

# AVERTISSEMENT

Ici on ne parle que d’accès par le navigateur, qui sont donc consultatifs ou d’édition légère. Les clients de synchronisation sur ordi ou sur mobile (Synology Drive pour Mac ou PC, Drive ou Moments pour mobiles) ont un comportement particulier. Par exemple, (cf. plus loin dans la section NAS/Firewall) le logiciel client Drive chargé de synchroniser les données entre votre PC/Mac et votre NAS, lui, passera systématiquement par le port 6690, tandis que pour les applications mobiles, on doit spécifier le port 443… Dans mon cas, j’ai encore des ratés avec Synology Drive sur mon Mac, d’ailleurs si quelqu’un peut m’aider, je ne suis pas contre.

# PREMIERS PAS

## Attribuer une IP fixe (le signe => signifie « si vous connaissez, sautez »)

Cette étape dépend du modèle de Box qu’on utilise (Livebox, Freebox, SFR box, Bbox, etc. : cf. Web). Je pars du principe qu’on n’a pas, en plus de la Box un routeur, car dans ce cas, on connaît généralement déjà toute cette partie. Toutes ces box grand public sont aussi des routeurs (basiques), et c’est donc leur boulot que de fournir une adresse IP, qu'elle soit fixe (comme chez Free) ou dynamique (comme chez les autres). En effet, les périphériques qui se connectent sont de 2 types : soit c’est un périphérique de passage (par ex le smartphone d’un ami qui se connecte une fois à notre Wifi), soit c’est un périphérique permanent, a fortiori un serveur, puisque les autres appareils devront se connecter à lui. Dans ce cas, il faut lui donner une adresse IP fixe : cf. Web. Le système de la Box/Routeur qui fait cela s’appelle DHCP et il attribue donc des adresses IP soit dynamiques, soit permanents : dans ce cas, on appelle cela des « baux DHCP permanents ». Pour ce faire, DHCP se base sur un identifiant unique de chaque périphérique (son adresse MAC, mais rien à voir avec les ordis Mac), et il peut lui assigner ainsi une adresse IP fixe, qu’on choisit librement. Il faut juste choisir les derniers chiffres après le dernier point (ex : 192.168.1.XX), en veillant à ce que ce ne soit pas déjà pris ou interdit : en effet, certaines adresses sont déjà prises par le système (par ex 22, 80, 443, et quelques autres, cf. Web). Une métaphore me paraît parlante en la matière, qui est celle du restaurant. Imaginez un énorme restaurant avec une centaine de tables, sur plusieurs étages. Les clients sont attablés selon la place que leur a donnée le maître d’hôtel à leur arrivée. Sauf certains habitués de l’établissement (riches et célèbres 🙂) qui ont leur table réservée et dont on sait qu’ils sont toujours aux tables qui donnent sur la grande baie vitrée avec vue sur toute la ville. Ajoutons que cet ami « habitué » n’a pas de téléphone portable, on ne peut pas l’appeler, et on a besoin de lui parler. Qu’on soit un ami de passage dans le restau ou qu’on appelle le restau depuis l'extérieur pour lui faire passer un message, on a besoin de savoir à quelle table il est. Donc dans ce cas, une personne de passage sera introuvable, mais la personne connue du maître d’hôtel avec une table fixe sera aisément joignable. « Passez-moi monsieur Van Der Beck, je vous prie ». Le maître d'hôtel sait que le riche homme d’affaires est toujours à la table 7… Donc, pour les périphériques « habitués », comme le NAS, on attribue une adresse fixe pour communiquer facilement avec lui.

## Utilisateurs =>

Créer les utilisateurs du NAS : soi-même, et familles/collègues/clients/amis. Cf Web.

# NOM DE DOMAINE (NDD) =>

Si vous voulez disposer de votre NDD, du type humphreybogart.fr si d’aventure vous vous appelez ainsi, vous devez l’acheter chez un Fournisseur de noms de domaine (ou Registrar). Ce n’est nullement obligatoire, et votre NAS peut vous fournir un NDD chez lui, du style humphreybogart.synology.me, ou humphreybogart.DiskStation.me, etc. Par la suite, plutôt que de humphreybogart.fr, on parlera par convention de mondomaine.fr ou machin.com, que vous adapterez à votre cas. Et dans ce cas, vous pourrez avoir un sous-domaine, qui permet d’accéder directement, à travers une URL claire et simple, aux différentes applications de votre NAS.

* <https://moments.monlogin.synology.me> pour Synology Moments
* <https://video.monlogin.synology.me> pour Video Station
* etc…

L’inconvénient de cette technique est que si un jour vous passez chez QNAP ou autre, tout est à recommencer, et que vous restez lié à Synology. Enfin, en cas de panne chez leur serveur de nom de domaine, tout est en panne.

Dans notre cas, on part du principe que vous voulez utiliser votre NDD mondomaine.fr, et vous allez pour cela faire ce qu’il faut chez un Registrar. Les plus répandus dans le monde du NAS - parce que bien documentés et sur lequel vous trouverez le plus d’infos et d’aide - sont OVH et Infomaniak. A vous de choisir, ici nous suivrons la procédure chez OVH.

## Acheter un NDD chez OVH

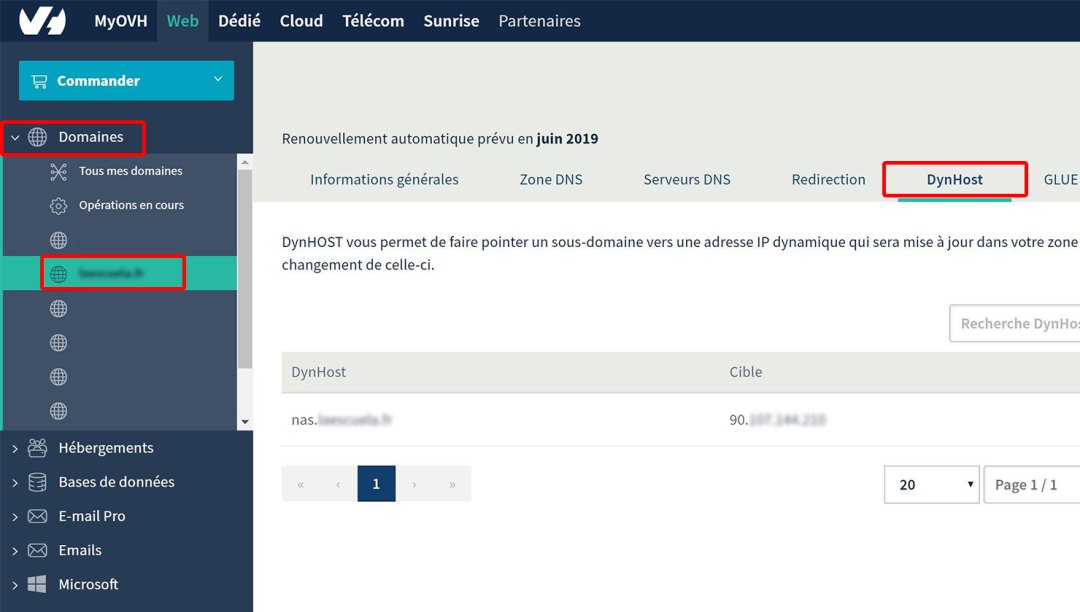
Se référer à ce tuto. Nota bene : on part dans l’idée que vous ne demandez pas à OVH de stocker votre site web chez eux, vous voulez juste qu’ils routent les visiteurs vers votre NAS, c’est donc quelque chose de très léger pour eux et pas cher, vous prenez la formule « sans hébergement ». Le tuto est très complet, et il y en plein d’autres : cf. Web.

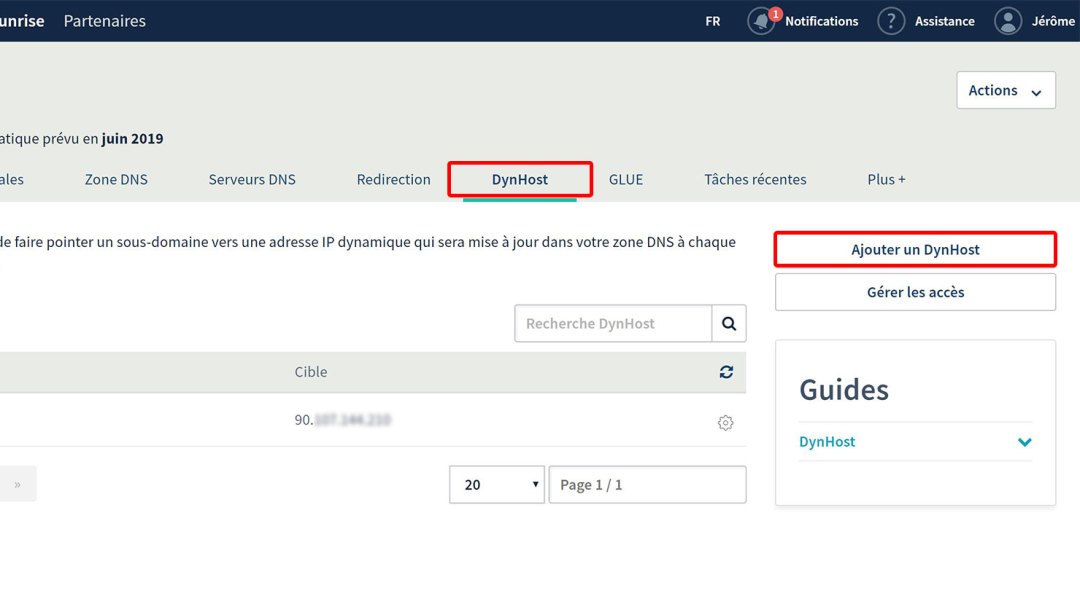
## Créer un DynHost (DDNS)

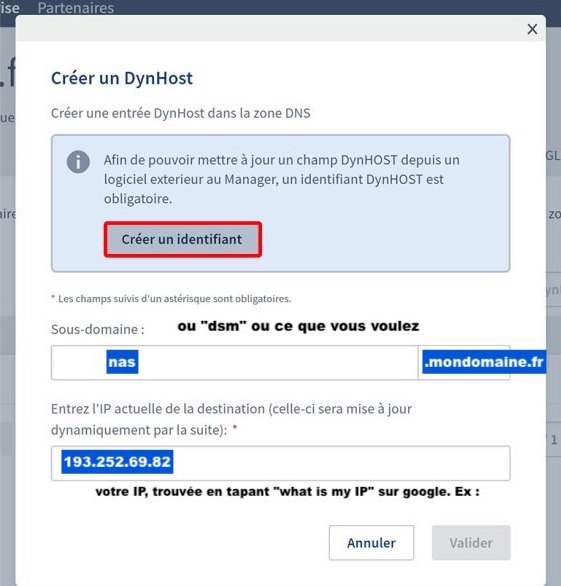
Comme évoqué plus haut, à part chez Free, les box/Routeurs n’ont pas d’adresse IP fixe publique, c’est-à-dire ouverte sur l’extérieur, car elle est changeante (à chaque redémarrage de la box, par exemple). Il faut donc trouver un système pour qu’on puisse vous retrouver dans le vaste World Wide Web. Métaphore faite maison : le Boîte Postale. Vous arrivez travailler dans une nouvelle ville, et vous n’avez pas encore de logement fixe, vous squattez chez des potes, un peu de AirBnB, un peu d’hôtel, bref : on ne sait jamais où vous êtes. Alors, vous prenez une boîte postale à la Poste, qui fait qu’on peut vous contacter à « Humphrey Bogart, BP 639, Dessous-les-Bras, Nièvre ». Ainsi, même en l’absence d’adresse fixe, le lien est maintenu. Le jour où vous avez une adresse fixe, plus besoin de ce DDNS (ou DynDNS ou DNS Dynamique, que chez OVH on appelle DynHost), et votre NDD peut directement être redirigé vers votre adresse IP Fixe. Mais, pour la plupart des gens, ce DDNS est nécessaire, et traduira une adresse (URL) en toutes lettres en adresse IP que le navigateur pourra atteindre. Pour ce faire, 3 moyens :

* Le DDNS de OVH : le DynHost, qu’on va voir ici.
* Le DDNS de Synology : cf plus bas, à la section « DDN ».
* Autres DDNS (No-IP, etc.) : cf. Web.

Pour créer un DynHost chez OVH, cf. [Tuto complet ici](https://www.adrienfuret.fr/2015/05/31/nas-synology-ddns-ovh/https:/leblogdejerome.com/2018/08/ajouter-un-nas-synology-a-un-dynhost-chez-ovh/) sur le Blog de Jérôme© qui est remarquable. En résumé, avec ses copies d’écran, ça donne ça :

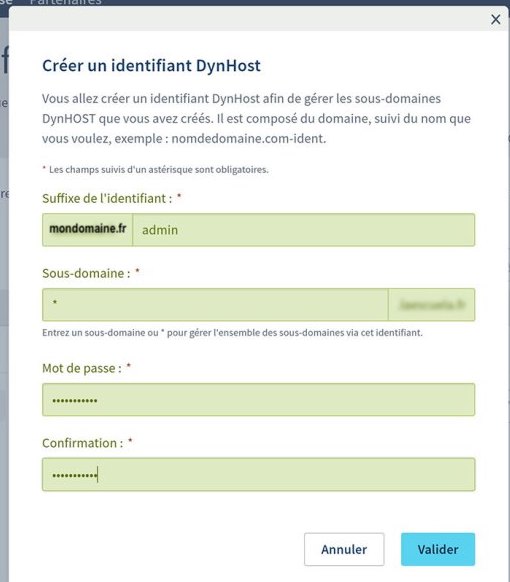






Saisissez le sous-domaine que vous voulez utiliser pour désigner votre NAS. C’est libre, prenons comme exemple nas.mondomaine.fr. L’idée est donc que nas.mondomaine.fr pointe vers chez vous, donc vous saisissez votre adresse IP (taper « what is my IP » sur Google, il vous la donnera tout de suite).

On crée au passage un identifiant (mais sinon on peut aussi juste créer le DynHost, et créer l'identifiant plus tard, en cliquant sur le nom du DynHost et gérer les accès.). Le choix de l’identifiant est libre, en général on met « admin ». L’identifiant sera donc « mondomaine.fr-admin ». Dans Sous-Domaine, on met un astérisque, afin que cet identifiant permette de gérer tous les sous-domaines de ce NDD.



Vous pouvez toujours modifier le DynHost ensuite : il suffit de cliquer dessus dans la liste des Dynhosts et de cliquer sur la petite roue à droite.

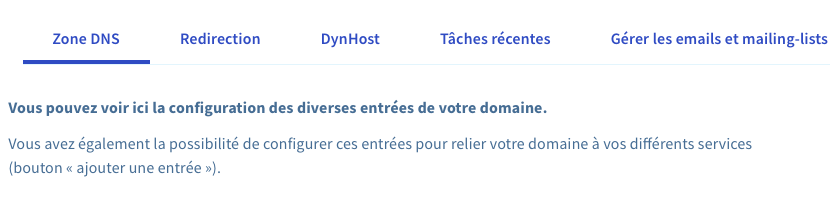


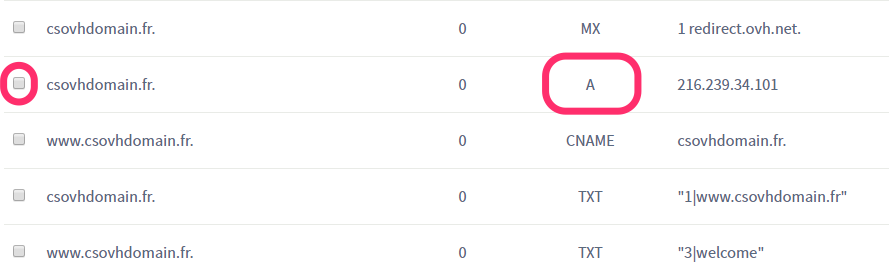
De même, vous pouvez créer l’identifiant ou le modifier ensuite, en cliquant sur le DynHost, et dans Gestion des Accès, vous modifiez ou créez l’administrateur de ce DynHost avec un identifiant, un mot de passe, et un astérisque.



## Zone DNS

ENTRÉE « A » : C’est vite fait :si vous avez une adresse IP fixe chez vous (vous êtes chez Free ou chez Orange Pros, à priori), vous allez dans l’espace de gestion de votre NDD et dans Zone DNS, et vous éditez votre entrée « A » pour la faire pointer vers votre adresse IP fixe (cf Web). Mais si, comme moi, vous n’avez pas d’adresse IP fixe, et vous réservez votre NDD comme étant 100% dévolu au NAS (ce que je vous conseille), vous supprimez l’entrée « A » qui est inutile. Pour ce faire, vous allez dans l’espace de gestion de votre NDD, et dans Zone DNS.



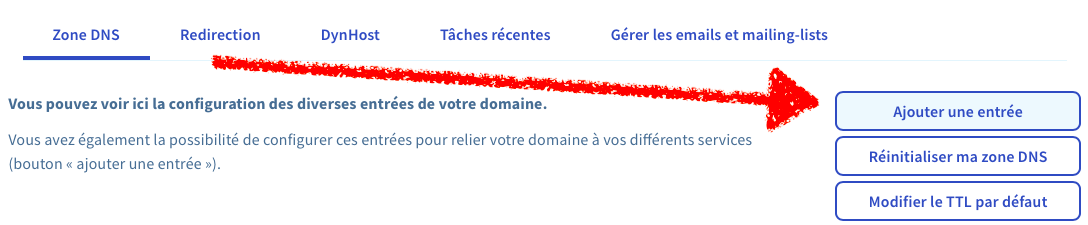




SOUS-DOMAINES en CNAME : Vous allez créer autant de sous-domaines que d’utilisations que vous avoir de votre NAS : regarder des vidéos, écouter de la musique, accéder et partager des fichiers, surveiller votre maison, etc. la liste est longue. Ici vous trouverez des exemples des usages de base, à vous de prolonger selon le modèle. (Une exception notable : Photo Station, qui peut poser problème, mais 1) l’application est vouée à disparaître 2) elle a un remplaçant, qui est Moments 3) il existe des moyens de résoudre la question.)

* moments.mondomaine.fr pour accéder à Moments
* drive.mondomaine.fr pour accéder à Synology Drive
* video.mondomaine.fr pour accéder à Video Station
* cam.mondomaine.fr pour accéder à Surveillance
* etc… Le nombre de sous-domaines ainsi que leur intitulé est libre : monorteil.mondomaine.fr peut très bien vous servir pour Surveillance…

Pour cela, vous allez dans Zone DNS/Ajouter une entrée, et vous allez faire en sorte que lorsque l’utilisateur tape https://moments.mondomaine.fr, il soit redirigé —sans le savoir - par OVH vers votre DynHost nas.mondomaine.fr, qui lui, est en permanence mis à jour vers votre adresse IP. Donc l’usager est de façon transparente emmené vers chez vous, et ira toquer à la porte de votre box/Routeur (cf plus loin).





Ici, machin.com c’est évidemment mondomaine.fr 😉 ATTENTION : ne pas oublier d’ajouter un point final dans la zone « Cible », sinon ce n’est pas reconnu : c’est le seul endroit où cette étrange syntaxe est nécessaire. Vous devez donc y taper « nas.mondomaine.fr. »



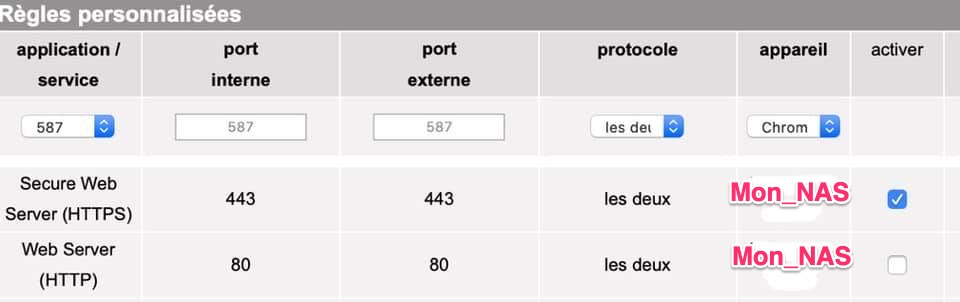
## BOX/ROUTEUR

On a vu que quand on toque à la porte de votre Box/Routeur, votre NAS est doté d’une adresse IP fixe sur le réseau domestique. Cependant, il faut encore préciser à quelle porte on toque chez lui. C’est pourquoi, plutôt que de parler de « ports » comme on le fait trop souvent en informatique, je préfère la métaphore de la porte, qui me paraît en définitive plus juste. En effet, un port, c’est un vaste espace avec des zones, et des quais où s’amarrent les bateaux. C’est grand et c’est encore très subdivisé. Alors qu’en réalité, on est ici comme dans un immeuble, ou le restaurant dont on parlait plus haut. Mettons l’immeuble : le concierge, c’est la Box/Routeur. Il reçoit du courrier pour « chez M. Humphrey Bogart, la jeune fille », et le concierge le porte donc chez M. Humphrey Bogart. Là, la personne responsable va traduire cela en « la jeune fille = Cindy » (car on a mauvais goût sur les prénoms chez les Bogart). Elle va donc dire : c’est encore un amoureux de Cindy qui lui écrit, et Cindy, je sais où elle dort, c’est ma fille, c’est la porte au fond du couloir. On aurait donc pu aussi libeller l’enveloppe des 2 façons suivantes : Cindy, chez M. Humphrey Bogart, 75020 Paris (dans le cas où Bogart aurait apprécié les lofts du côté de Gambetta) porte au fond du couloir, chez M. Humphrey Bogart, Via Giambellini, Milano (dans le cas où Bogart a envie de choper le Covid). Tout ça ce sont des façons différentes et équivalentes de toquer à la porte de Cindy. C’est pourquoi, quand on lit « port » en informatique, je pense « porte », ou chambre dans un grand hôtel : https://nas.mondomaine.fr:443 (c’est-à-dire port 443) je le traduis comme « je m’adresse de façon confidentielle (https), chez M. Humphrey Bogart (nas.mondomaine.fr), à sa fille Cindy (porte 443), qui est à la porte à droite dans le couloir » ou bien comme « Grand Hôtel, étage du NAS, chambre 443 », et le concierge (la Box/Routeur) sait qui loge dans la chambre. Prenez la métaphore que vous préférez, du moment que ça vous parle 😉. Pour assurer ce travail, comment fait le concierge ?

Paramétrer le NAT de la Box/Router : cf Web.

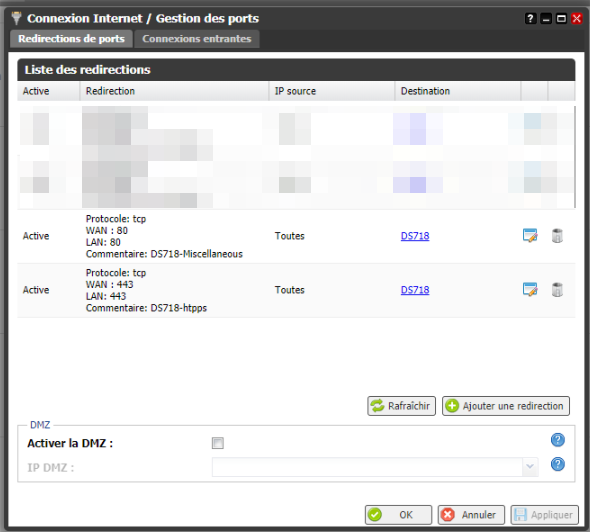
On part du principe que le Firewall de la Box (Livebox en l’occurrence) est réglé sur « moyen ».

On informe la box que ce qui arrive sur le port 443 doit être envoyé sur la NAS. Ici la copie d’écran de Ro HL sur le groupe FB NAS Synology francophone.



A la place de « Appareil» , vous choisissez votre NAS qui apparaît dans la liste.

Sur Freebox :



NOTA BENE : De temps en temps, il est nécessaire d’ouvrir le port 80, notamment pour créer le certificat (cf plus loin) qui permet à vos visiteurs d’établir une connexion sécurisée https, et régulièrement, pour renouveler ledit certificat. Soit vous l’ouvrez de temps en temps, soit vous le laissez ouvert et vous préciserez au niveau du Firewall du NAS que vous n’autorisez le trafic sur le port 80 que depuis la France et les USA, d’où se connecte Let’s Encrypt, qui est l’autorité qui délivre les certificats.

C’est fait, le concierge a pris l’enveloppe pour la chambre 443 de l’hôtel, et il la porte à l’étage du NAS, où se trouve ladite chambre 443. On va donc toquer à la porte du NAS…

## NAS

### Firewall

Le Firewall, c’est le garde du corps de votre NAS : pour moi, c’est le gros videur baraqué à l’entrée de la boîte de nuit qui vus dit « désolé, c’est une soirée privée, ça va pas être possible» . Il est paramétré pour laisser passer les habitués, c’est-à-dire toutes les communications domestiques, donc au sein de la maison. Mais il ne permet à personne d’entrer à moins d’y avoir été expressément autorisé. La règle est donc :

Ceux qui habitent dans la maison (le LAN ou « Local Area Network» ) : Autoriser

Moi-même, quand je suis en déplacement (le fameux VPN) : Autoriser comme si j’étais chez moi

Les proches et notre entourage, qui savent à quelle porte toquer (la 443) : Autoriser

Le facteur, les livreurs toquent à la porte 80 : Autoriser mais à surveiller (en temps normal on peut n'ouvrir ce port que pour la création et/ou renouvellement du certificat, car Let’s Encrypt en a besoin)

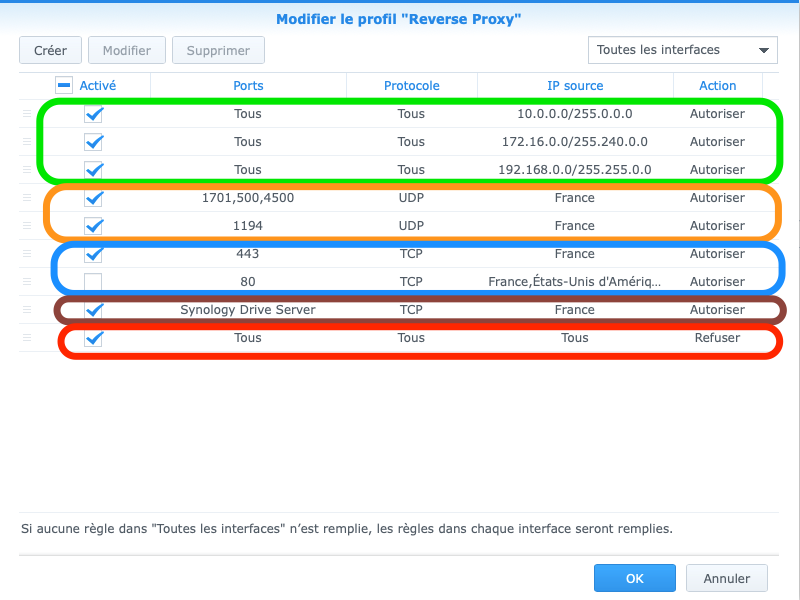
Ports spécifiques au Serveur VPN (lui a ses propres entrées) : autoriser

Tous les autres : Refuser

On va donc (et ce sera quasiment tout le temps le cas) dans Panneau de Configuration



Et là on va dans Sécurité/Pare-feu, et on règle tout comme ceci (je me suis basé sur le Tuto de Fenrir, mais il y a des choses que j’ai recopiées sans chercher à comprendre ;-). Le plus important est de finir par « tous» « refuser» , à placer en dernier, car les règles sont lues par le NAS de haut en bas. ATTENTION : Si jamais vous vous trompez, et que cette règle « tout refuser» n’est pas placée en dernier, vous pouvez vous retrouver bloqué…



Les 3 premières règles en vert (configurées pour toutes les interfaces ; si vous voulez entrer dans des détails, cf Web) sont faites pour laisser entrer vers le NAS toutes les communications locales, ou sécurisées par le VPN, ce qui équivaut à du local. (la 2e, je me demande si c’est pas pour un protocole VPN obsolète et donc déconseillé, le PPTP, mais là je m’avance peut-être : vos infos sont les bienvenues).

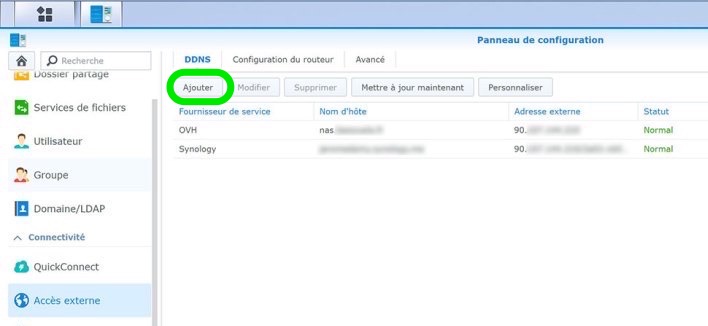
Les 4e et 5e règles en orange (UDP 500, 1701, 4500 et UDP 1194) sont utilisée respectivement par les protocoles L2TP-IPsec et par OpenVPN. Ce sont les deux meilleurs : OpenVPN est le plus sécurisé et open source, mais il n’est pas implémenté nativement sur les appareils clients (smartphones, ordis). L2TP-IPsec est un poil moins sécurisé, mais, vous l’avez deviné, il est d’office reconnu par vos ordis, smartphones, etc. Personnellement, j’utilise les deux, au cas où. Plus d’infos sur le tuto de Fenrir consacré à ce sujet ici.

Les 6e et 7e règles en bleu (80,443) servent à autoriser les ports http et https par défaut. Le port 80 permet à Let’s Encrypt de communiquer avec le NAS pour la création ou renouvellement des certificats (cf plus bas). Le port 443 est à utiliser en permanence, puisque selon la technique que nous allons employer, c’est l’unique porte d’entrée depuis l’extérieur (les suivantes, on va voir pourquoi c’est différent).

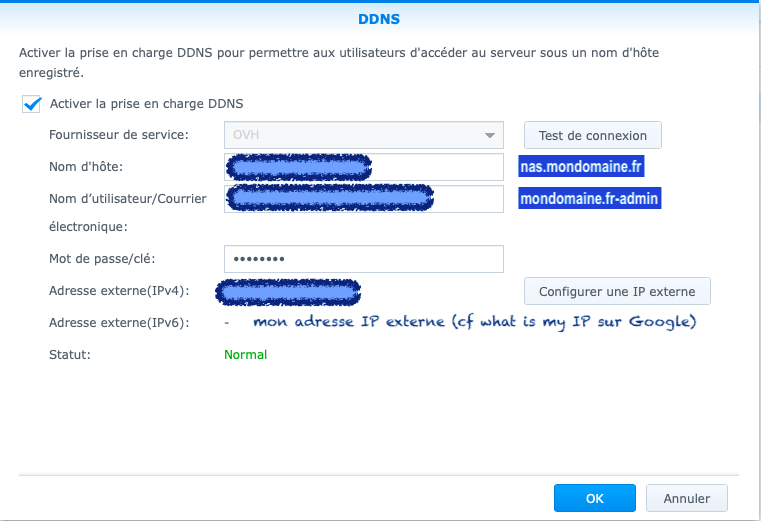
La 8e règle en bordeaux sert pour les applications particulières, comme Drive (ou Photo Station) : Drive exige de pouvoir passer par le port 6690, quoiqu’on fasse, quand il s’agit de se connecter avec le logiciel client pour ordinateurs, qui est chargé de la synchronisation. Nota bene : sur les clients Drive mobiles, il faut ajouter le numéro de port 443 à l’adresse de notre sous-domaine. Cf plus loin, en conclusion)

### DDNS

Dans Panneau de configuration/Accès externe/DDNS, on va maintenant « relier « notre NAS à l’adresse DDNS (DynHost chez OVH) créée précédemment. Pour l’exemple, on avait choisi comme adresse « nas.mondomaine.fr « ou « nas.machin.com « . Et le NAS, en se connectant au service dédié chez OVH, va mettre à jour cette adresse à chaque fois que la Box va changer d’adresse IP.



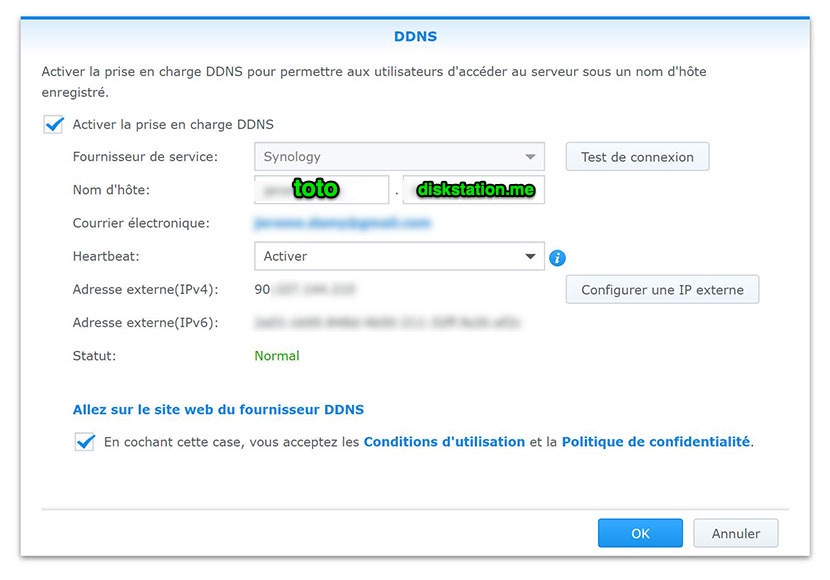
Nous allons donc cliquer sur « Ajouter» . S’ouvre la fenêtre d’édition du DDNS.



On renseigne ici notre identifiant DynHost de OVH (cf plus haut), qui est du type mondomaine.fr-admin ou machin.com-admin et que vous avez renseigné chez OVH, le mot de passe et le nom d’hôte : nas.mondomaine.fr.

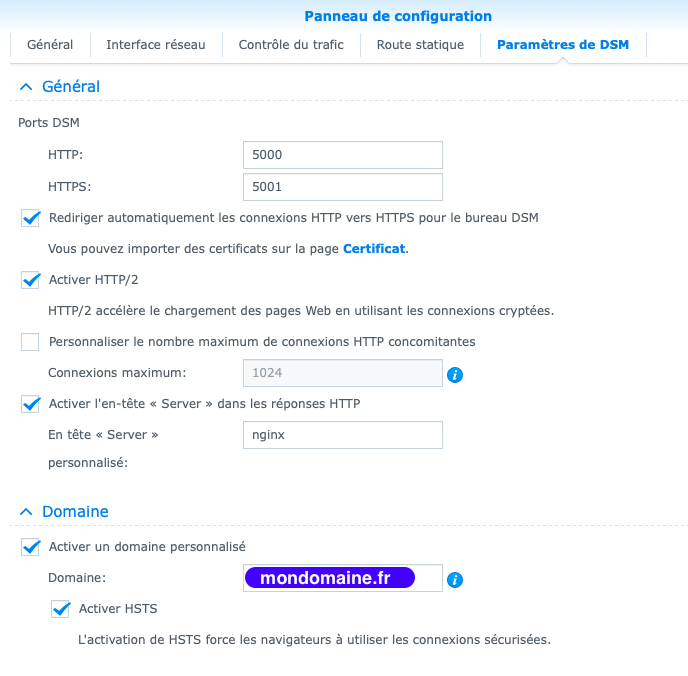
Attention : j’ai déjà eu des erreurs où, au bout de quelques jours, ça ne marchait plus. Bizarre : si je remplace dans le champ Nom d’hôte « nas.mondomaine.fr» par « mondomaine.fr» , cela remarche. Et quelques jours plus tard, ça peut arriver en sens inverse… A creuser.

Cela étant, vous pouviez tout à fait vous passer du service de OVH, et utiliser celui, natif, du Synology (je le fais aussi). Cela offre évidemment des avantages et des inconvénients : parmi les avantages, il y a bien sûr le fait qu’il soit intégré au système, et qu’il permette l’usage des wildcards, c’est-à-dire l’astérisque, qui vous permet de lui faire traiter tous les sous-domaines de mondomaine.fr d’un coup, lorsque, on le verra plus loin, il s’agira d’importer un certificat. L’inconvénient majeur est double : d’une part les DDNS Synology sont liés à la marque, et donc, si un jour vous changez de fabricant (Qnap par ex), vous ne pourrez plus vous en servir, et de l’autre côté, vous ne choisissez pas vraiment le nom du domaine : pour un particulier, ce n’est pas grave d’avoir comme ddns « josebellini.synology.me « « josebellini.diskstation.me» mais pour un professionnel, il préférera sans doute nas.josebellini.com. Après, il est aussi possible que l’utilisateur final ne voie jamais l’adresse de votre DDNS, puisque lui n’utilisera que l’accès par sous-domaines : à vous de voir. Dans mon cas, comme j’ai pris l’offre OVH et que c’est intégré, je m’en sers, même si c’est parfois avec des aléas. En revanche, j’utilise le DDNS de Synology pour les applications au comportement non-standard, comme par exemple le client pour ordinateurs Synology Drive (cf Firewall). Ici les réglages pour un DDNS Synology :



## DSM

On va maintenant s’assurer qu’au niveau central du système, les informations de base soient correctes : dans le panneau de configuration/Réseau/Paramètres de DSM, on vérifie que les ports HTTP et HTTPS sont bien les bons.

Parenthèse : on a parfaitement le droit de personnaliser ces ports, et de mettre 6009 et 6010 ou 7233 et 7234 si on veut, mais d’abord, il faudra en tenir compte partout, et certaines applications pourront avoir tendance à aller chercher les ports par défaut 5000 et 5001, et ensuite —si on suit les conseils de Fenrir sur son Tuto incontournable, qui est la référence en matière de sécurité - modifier le port par défaut ne ralentit un intrus motivé que de quelques secondes, alors qu'un mot de passe long et complexe avec une authentification à 2 facteurs est une barrière que moins de gens peuvent franchir. It’s a free country, faites comme vous le sentez.

On a bien coché aussi « rediriger automatiquement les connexions http vers https pour le bureau DSM.

On active HSTS et HTTP/2 : le premier force les communications à passer de http en https, et maintient la sécurité de bout en bout (Mais il y a un débat là-dessus, cf \* en fin de cette section), le second compresse certaines données afin d’accélérer les échanges.

Concernant l’en-tête Nginx, j’ignore si c’est nécessaire : commentaires bienvenus !

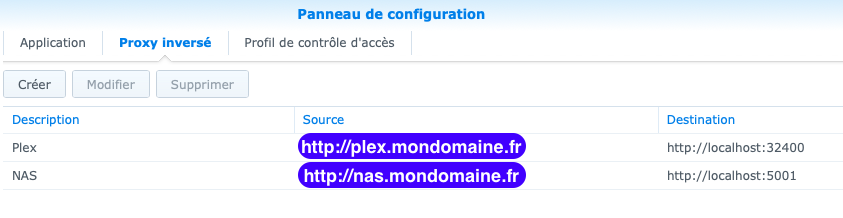
Enfin —et c’est capital - on coche « activer un domaine personnalisé» , afin que le système reconnaisse que le visiteur qui utilise votre nom de domaine mondomaine.fr soit bien arrivé au bon endroit. Cette partie ayant été faite à partir de conseils glanés ça et là sur les groupes Facebook et tutos Web, je ne fais donc que recopier ce qu’on m’a dit et qui marche chez moi. Je ne suis pas capable d’en expliquer moi-même les tenants et les aboutissants : pour cela, les contributions sont bienvenues et j’adapterai le tutoriel au fur et à mesure avec les explications qui me seront parvenues.

(\*) Il y a débat là-dessus parce qu’on met du https entre le visiteur et la box, alors on pourrait peut-être considérer qu’une fois qu’on a atteint la Box, on est au sein du LAN, et qu’on est train de crypter quelque chose de déjà crypté (donc charge et ralentissement inutile). Le visiteur a tapé https, il est arrivé par le port 443 de la box, à partir de là en théorie on devrait pouvoir se passer du https mais je préfère que les spécialistes se prononcent sur la question, notamment dans le passage suivant : le Reverse Proxy.

## REVERSE PROXY

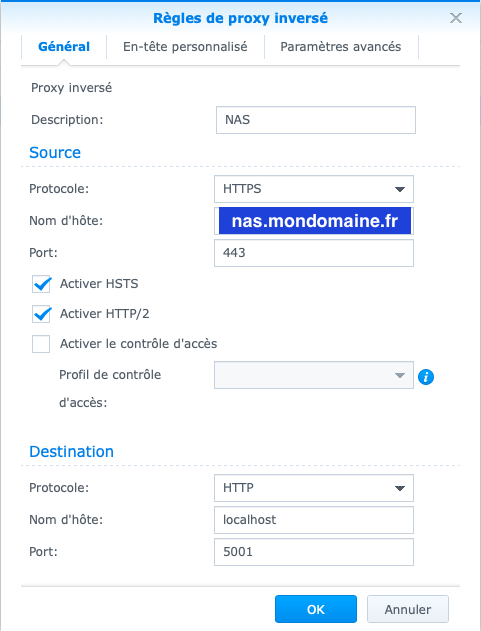
Dans la plupart des tutos, le Reverse Proxy joue un rôle non seulement central, mais surtout exhaustif. La particularité de la technique exposée ici est de lui conserver son rôle central, mais de le simplifier et de confier aux applications ce qui les concerne. Voyons cela :

On va dans Panneau de configuration/Portail des applications/Reverse Proxy. Le mien ressemble à ça, mais ignorez la ligne Plex.



Le principe du Reverse Proxy est encore celui du concierge d’hôtel : lui sait traduire « vous pouvez donner ceci au monsieur qui occupe la grande suite du dernier étage ? « en termes précis, qui signifient « on parle donc de la chambre 5001 et de M. Nasse, notre meilleur client « . Son boulot, ici, va être de prendre le visiteur et de l’emmener au bon endroit, sans qu’il ait à se soucier de longues adresses compliquées et de ports.

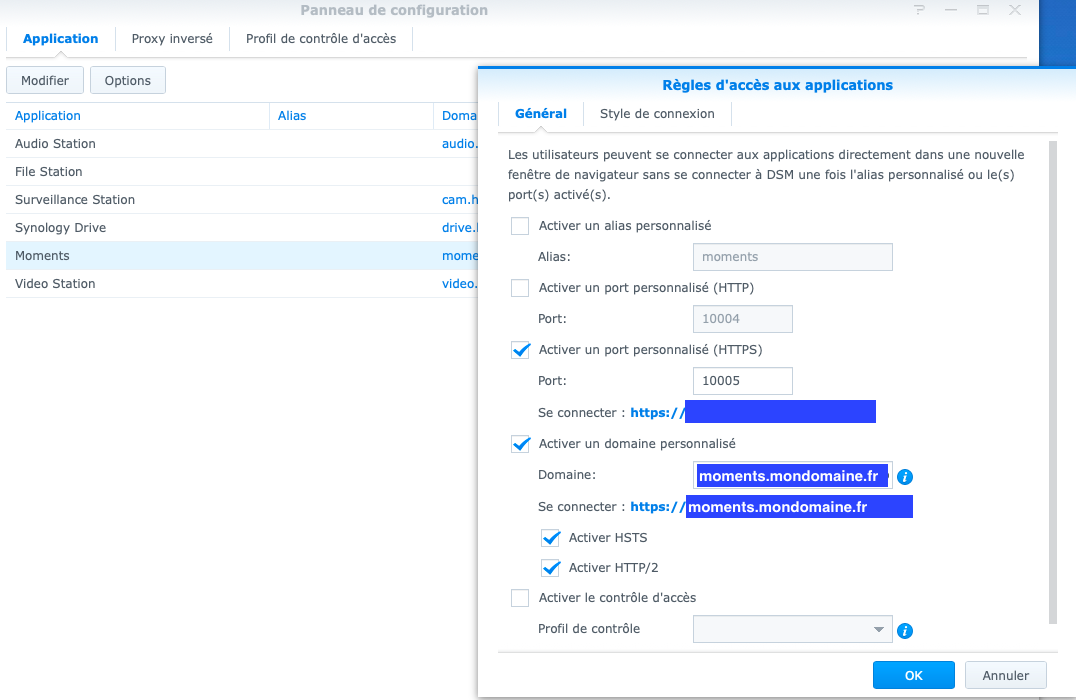
A ce stade, refaisons le parcours : le visiteur, qui à l’origine avait tapé sur son navigateur « https://moments.mondomaine.fr « a été emmené jusqu’ici par le DDNS de OVH, qui a dit « moments.mondomaine.fr, moi j’emmène ça vers nas.mondomaine.fr, qui est votre DDNS et qui pointe vers votre Box. Cette dernière a fait suivre au NAS. Et là, le Reverse Proxy, qui est un flemmard, lève à peine le sourcil et dit « moi je m’en fous, tout ce qui est adressé à mondomaine.fr je renvoie ça au système qui sait quoi en faire» d’où le « localhost» et « port 5001» « .



C’est ainsi qu’on va donc donner comme point d’entrée mondomaine.fr en https (en cochant HSTS et HTTP/2) et l’envoyer vers DSM (localhost, c’est son nom pour les intimes) sur le port 5001. C’est le directeur de l’hôtel, il sait quoi faire. Or, que va-t-il faire ? DSM va lire la requête de départ (moments.mondomaine.fr) et va constater qu’il y a une application qui lève le doigt et qui dit « c’est pour moi, c’est pour moi « . Comment ? Voyons cela, ça se passe dans la même partie « Portail des Applications» , mais dans le premier onglet.

## PORTAIL DES APPLICATIONS/APPLICATION

C’est ici qu'on spécifie les détails de chaque appli : quel port elle utilise, quel alias ou petit nom elle utilise, et notamment quel sous-domaine elle veut. Or, on aura donné à Moments le nom de domaine personnalisé moments.mondomaine.fr et donc DSM lui transmettra la requête et le visiteur aboutira à la page d’identification de Moments et on aura fait notre boulot.



Et ainsi de suite, pour chacune des applications qu’on souhaite rendre accessible. Ce qu’on vient de faire application par application est au fond une forme light de Reverse Proxy, et donc en théorie on pourrait tout faire dans le Reverse Proxy, mais :

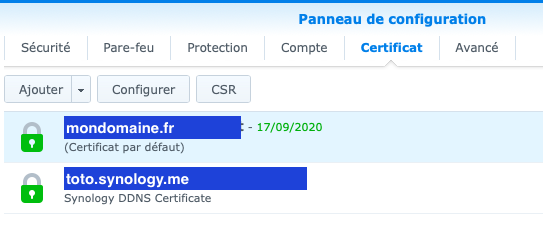
moi je n’ai pas réussi à le faire marcher et la méthode décrite ici marche chez moi 😉

elle a aussi un avantage : comme de toute façon, on doit avoir affaire aux réglages dans Portail des applications/Application, autant utiliser le Reverse Proxy avec une règle simple et immuable et gérer chaque application là où c’est prévu pour.

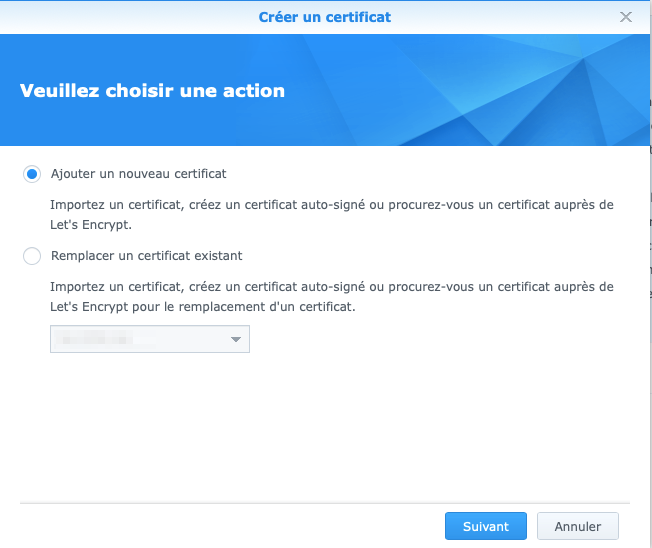
## CERTIFICAT

Le certificat, en deux mots, c’est l’équivalent du justificatif de domicile dans vos démarches administratives. Vous dites à la préfecture que vous habitez 11 rue du Chat qui Pue 94199 Fontenay-le-Creux, mais il faut qu’une entité tierce (EDF, Orange, Free, etc) le certifie. Ici, c’est Let’s Encrypt qui va se charger de dire que oui, le site humphreybogart.fr vous appartient. Mais il existe des alternatives (FreeSSL notamment, mais pour ça, je ne suis pas le mieux placé, je ne l’ai pas fait, cf tuto ici).

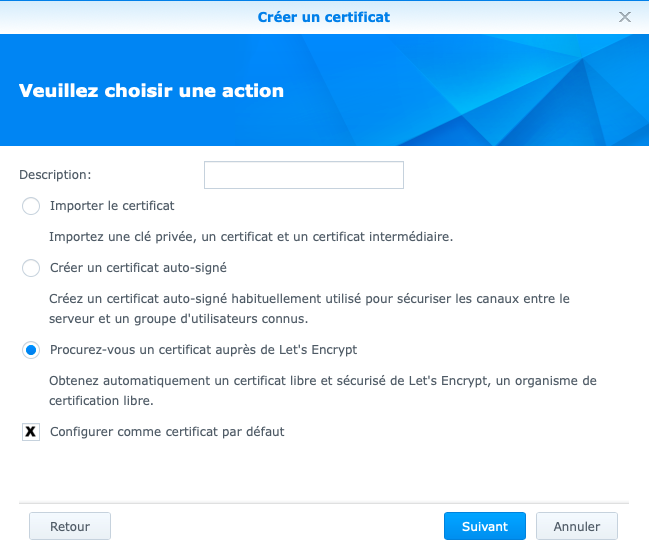
Enfin, on se procure un certificat pour permettre à tout cela de fonctionner de façon sécurisée, en https. Autrement, l’utilisateur verra apparaître un message de sécurité l’avertissant qu’il visite peut-être un site frauduleux, ce qui, bien que faux, fait mauvais genre. Pour cela, on va dans Panneau de configuration/Sécurité/Certificat

On fait Ajouter, puis on la choix : soit « Nouveau certificat» , soit « Remplacer un certificat existant» . Partons sur « Nouveau» , si c’est votre premier.

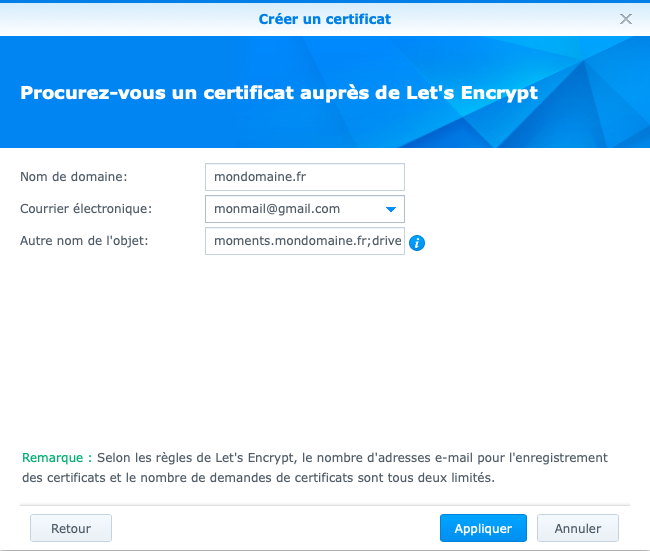
NOTA BENE : le certificat qui existe d’usine sur les NAS Synology ne sert à rien pour des accès depuis l'extérieur, car il est auto-signé. vous pouvez donc aussi choisir de le remplacer.



On demande donc un nouveau certificat auprès de Let’s Encrypt : cochez donc « configurer comme certificat par défaut» .



On arrive sur l’écran où on saisit les infos relatives à votre NDD.



Les certificats à partir de votre NDD doivent être libellés ainsi :

Nom de domaine : mondomaine.fr

Votre email, de préférence celui utilisé chez le Registrar

Autre nom de l’objet : c’est là où vous mettez vos sous-domaines, séparés par des points-virgules : moments.mondomaine.fr;video.mondomaine.fr;drive.mondomaine.fr et ainsi de suite

D’après notre ami Ro HL du groupe FB NAS Synology francophone, FreeSSL permet de contourner la limite de Let’s Encrypt concernant les NDD qui oblige à saisir tous les sous-domaines, et permet d’utiliser le wildcard, qui permet de les gérer tous d’un coup. Je ne m’embarque pas là-dedans, je ne l’ai encore jamais fait…

Certificats pour votre DDNS Synology

Dans ce cas, si vous n’utilisez pas de NDD à vous, c’est plus simple : dans « Autre nom de l’objet» vous pouvez ne mettre que \*.toto.synology.me (ou tout autre DDNS proposé par Synology, comme DiskStation.me, etc) et il acceptera tous les sous-domaines…

moments.toto.synology.me

drive.toto.synology.me

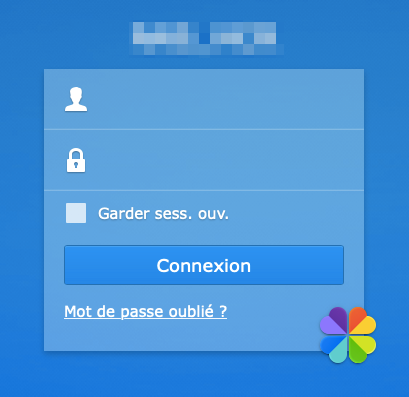
video.toto.synology.me

et ainsi de suite

Ça ne marche qu’avec les DDNS de Synology, sauf à passer par FreeSSL : tuto ici.

## CONCLUSION

Désormais, vous êtes censés, depuis l’extérieur de chez vous, taper sur un navigateur l’adresse moments.mondomaine.fr et tomber sur…



Et ainsi de suite pour toutes les applications configurées !