[Synology] 8 méthodes pour sécuriser l'accès à votre NAS

SEPT 03 2013

Système (Votez !) Réagir !

« Ne cassez plus le fil de vos écouteurs / casques
(modifié le 3 septembre 2013 à 0:18)

Les NAS Synology sont un excellent rapport qualité prix, à tel point qu'ils **se multiplient sur la planète et nombreux sont ceux connectés à internet**, directement ou non.

Il serait dommage qu'**un pirate entre sur votre NAS et supprime le contenu de vos photos**, musiques, films, sauvegardes... ou volent des informations confidentielles relatives aux données personnelles.

Aucune faille n'est connue à ce jour sur les NAS Synology, grâce à l'utilisation du système d'exploitation Linux ainsi qu'à de très régulières mises à jour par Synology. Pourtant, **un petit malin pourrait bien finir par forcer la porte de votre NAS**.

Voyons **comment s'en prémunir** au maximum.

Vérifiez les notifications

Avant tout **vérifiez que votre Synology peut vous envoyer un mail**, car si vous n'avez plus de smartphone c'est la seule possibilité pour obtenir un code (contrairement à Gmail qui génère des code imprimables à l'avance). Par ailleurs en cas de pépin votre NAS vous enverra un mail (défaut du RAID, surchauffe, panne électrique, etc).

Pour **configurer la notification** :

1. Rechercher "**Notification**" en haut à droite de DSM
2. Choisir le premier résultat
3. Configurer le SMTP, dans mon cas chez Numericable j'utilise :
   - smtp.numericable.fr
   - port 25
   - pas de SSL/TLS et pas d'authentification
4. Entrer votre adresse email dans le champ "email principale" (une adresse Gmail pour mon cas, que le relai numericable accepte tout de même de délivrer)
5. Cliquer sur le bouton "*Envoyer un courriel de test*"
6. Si vous avez reçu le mail vous pouvez passer à l'étape suivante. Si vous ne recevez pas l'email, vérifiez qu'il ne soit pas en spam. Enfin, pensez à activer le port sortant 25 sur votre box car la plupart des FAI le bloque d'usine.

Activez la double vérification

La **vérification en deux étapes**, ou double vérification, ajoute une couche de sécurité supplémentaire sur votre NAS Synology (depuis DSM 4.2).

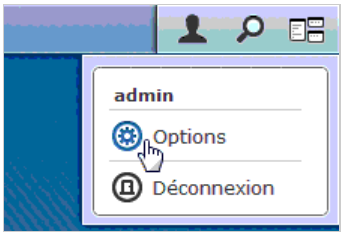
Elle évite à quelqu'un qui aurait (ou trouverait) votre mot de passe d'accéder à votre NAS. Vous utilisez probablement ce système sur votre messagerie Gmail, et si ce n'est pas le cas je vous encourage à le faire (sauf si les données de votre boite email ne valent rien...).

Si vous avez un smartphone vous pouvez aussi activer cette double vérification sur les comptes sensibles de votre Synology, typiquement le cas du compte admin s'il est actif.

Sur chaque type de smartphone une application est disponible, c'est cette application qui vous fournira le code à entrer en plus de votre mot de passe.

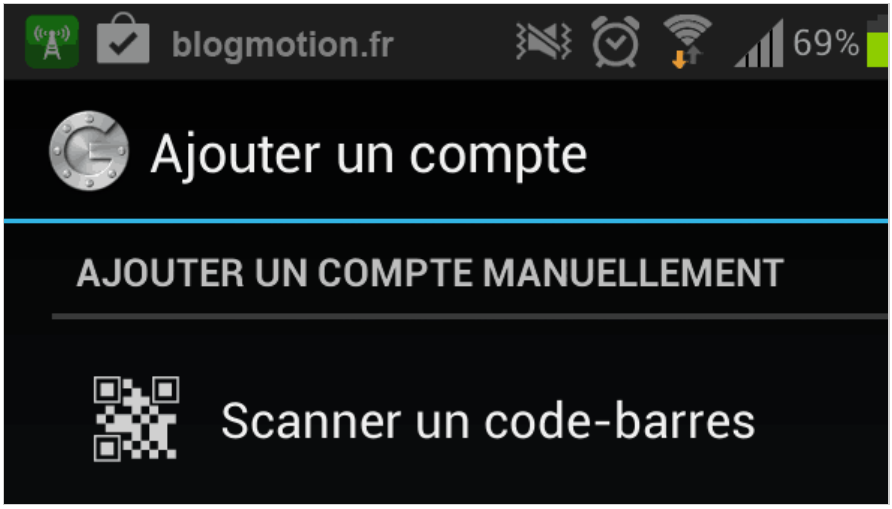
- Installez l'application Google Authenticator (compatible Android, iOS , Windows Phone et Blackberry)

Une fois connecté sur DiskStation Manager (DSM) avec l'utilisateur pour lequel activer la double vérification, cliquer sur les options en haut à droite :



Cliquer sur "Vérification en deux étapes" et se laisser guidé par l'assistant :

Une fois arrivé sur le code QR, il suffit de lancer l'application *Google Authenticator* pour **lier votre NAS à votre smartphone** en flashant le QR Code (via touche menu > configurer un compte) :



C'est fini !

Déconnectez-vous et reconnectez-vous à DSM pour **vérifier que ça fonctionne**.

Ne laissez pas les port(e)s ouvert(e)s

Premièrement **ne configurez pas votre Synology en laissant les ports par défaut** (5000 et 5001) **visibles depuis l'extérieur**.

Deux solutions :

1. soit vous le faites depuis votre routeur en définissant un port externe exotique avec du **NAT** sur le port 5000/5001 (pas toujours possible)
2. soit vous le faîtes au niveau de DSM (panneau de configuration > paramètres DSM >

port du routeur).

Si vous ne faites pas ceci vous risquez fortement d'être victime de scans de serveurs (robots) qui feront des tentatives de connexion depuis la chine par exemple.

Source = moi uniquement

Pour **ne pas laisser votre Synology à l'écoute de tout le monde**, je vous conseille aussi de **filtrer sur l'IP source** :

- au niveau de votre routeur / box s'il le permet
- au niveau du Synology lui même dans la partie pare-feu

De mon côté j'autorise seulement une poignée d'IP depuis lesquelles je me connecte régulièrement, configurées dans mon routeur fonctionnant avec le firmware libre Tomato. Rien ne vous empêche ensuite de **laisser un accès distant sur votre routeur** pour ajouter une IP différente si vous êtes dans la panade, soit HTTPS avec un **port exotique**, soit au travers d'un tunnel SSH (encore sur un port exotique).

httpS uniquement

Pour éviter une attaque de l'homme du milieu **bannissez de manière générale tout flux HTTP au profit de HTTPS**. Cela vous évitera bien des ennuis sur des hotspots non sécurisés (free wifi) ou sur des honeypots (fake ap). Bien que la double vérification protège l'accès à votre NAS (un code généré par GG Authenticator ne peut être entré deux fois, même rapidement).

Vous pouvez aussi générer un certificat StartSSL (Classe 1) pour éviter les alertes des certificats auto-générés.

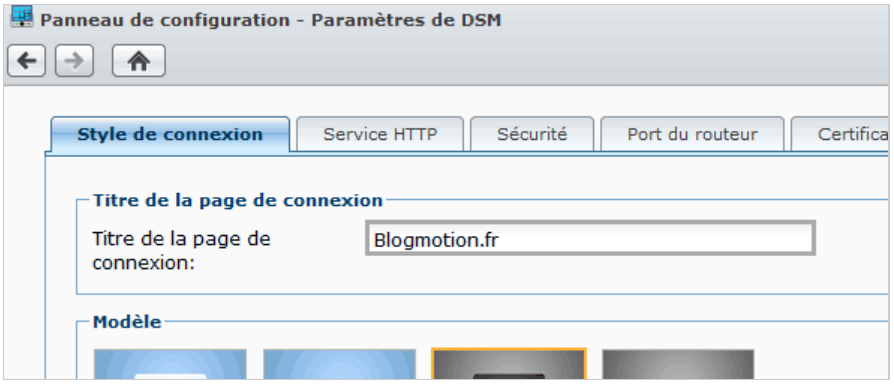
Compte admin non admis

L'idéal est de **désactiver le compte "admin"** de votre NAS afin d'éviter toute tentative de connexion. Créez plutôt un second compte admin avec un nom exotique (4 lettres suffisent) et un mot de passe solide.

Cachez votre NAS

Pas derrière un placard non ! Mais il possible de **masquer le nom réel de votre NAS** (le miens ne s'appelle pas "Blogmotion.fr"). Inutile qu'une personne de l'extérieur prenne connaissance d'un nom tel que "backup", "ldap" ou que sais-je. Si l'attaquant s'aperçoit que la machine est critique cela ne fera que l'encourage dans sa quête...

Il est possible de masquer ce nom dans les paramètres de DSM, cela n'aura **aucune influence sur son vrai nom** :

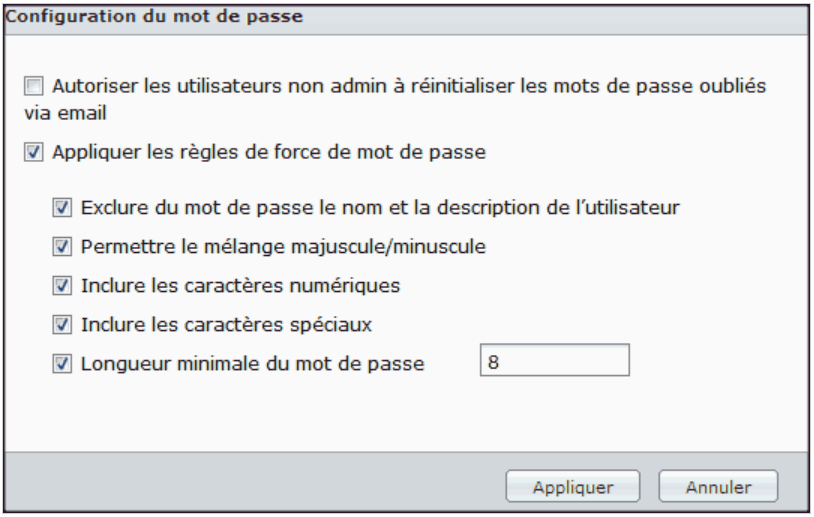


Attention aux accès pour les "amis"

Si vous créez des comptes d'accès pour des amis, vérifiez qu'ils n'ont pas de droit destructeurs car si quelqu'un obtient leur identifiant / mot de passe les dégâts seront au rendez-vous. Personnellement j'ai créé un groupe en lecture seule, sur certaines ressources seulement.

Toutefois vous pouvez monter d'un cran le niveau de sécurité dans:

- panneau de configuration > utilisateur > bouton configuration du mot de passe :



Conclusion

Si vous suivez ces conseils **votre Synology ne s'en portera que mieux, et vous dormiez tranquille** !

Prenez aussi en compte qu'une tentative de connexion sortira votre NAS de sa veille... pour rien et consommera de l'électricité pour rien.

Vous risquez d'être aussi intéressé par :

- Télécharger DSM 4.2 en version finale
- Comment activer un serveur SFTP sur un NAS Synology
- Synology DSM 5 final est disponible
- [Synology] DSM 4.3 disponible en version finale
- [Synology] Activer les notifications SMS

Pourquoi la protection DDoS est imposée chez OVH »

Auteur : Mr Xhark

Fondateur du blog et passionné par les nouvelles techno, suivez-moi sur twitter

Tags: connexion, hack, login, nas, protéger, sécurisé

Déjà 12 commentaires

TomTom - *@th_vador*
dit :
3 septembre 2013 à 10h11

Bonjour,
tu parles de ton routeur alors je vais poser une question un peu HS mais pas trop :
le WNR3500L est-il toujours le routeur à acheter aujourd'hui ou en as-tu un autre à conseiller?

J'ai aujourd'hui un WRT54GS et il me fait des misères quand je transfère de gros fichier sur mon NAS DS 213.

En fait, dès que j'effectue un transfert de fichier qui dure trop longtemps, mon pc se déconnecte du réseau wifi.
Le réseau est toujours fonctionnel sur d'autres appareils et seul le PC qui effectuait le transfert est touché.

J'ai lu ici ou là que le fait de brancher un appareil Gigabit sur le WRT54GS pouvait poser problème.
Et comme les différents tests que j'ai pu faire n'ont rien donné, je lui cherche un remplaçant, compatible avec le DS213 et en passant au 802.11n et au gigabit tant qu'à faire

Mr Xhark - *@xhark*
dit :
3 septembre 2013 à 11h18

@TomTom: j'aurai préféré que tu poses la question sur l'article sur le routeur (je surveille les commentaires sur tous les billets). Oui ce routeur est encore d'actualité, en v2 depuis (plus de mémoire pour stocker un firmware alternatif), tu peux y aller les yeux fermés !

Raz dit :
3 septembre 2013 à 14h04

Un tuto bien plus détaillé je trouve que le wiki syno sur la creation de certificat SSL:
http://missilehugger.com/819/

TomTom - @th_vador
dit :
3 septembre 2013 à 14h11

@Mr Xhark: désolé. En plus, j'ai hésité!

Merci pour ta réponse, je pense que je ne vais pas tarder à sauter le pas

sam dit :
3 septembre 2013 à 20h55

Bonjour
Article très intéressant. Je n'avais pas remarqué l'authentification forte disponible dans DSM.
Je rajouterai également le blocage auto ip qui est assez utile pour bannir automatiquement les IP qui font trop de tentative de connexion.

Gizeek - @Gizeek
dit :
12 septembre 2013 à 6h54

Merci de l'info ! Je n'avais pas fais attention que l'option existait !

aexm - @aem38
dit :
5 janvier 2014 à 21h41

Merci pour la double authentification, je ne connaissais meme pas … j'ai pu mettre à jour mon article !

Au passage on peut ajouter bcp plus de regles pour securiser …

- la force des mots de passe,
- le blocage IP auto,
- désactivation des services inutiles,
- activation anti virus
etc …

Sebastien

kid A dit :
15 janvier 2014 à 10h32

Bonjour,

Merci pour cet article qui me donne des pistes supplémentaires pour sécuriser l'accès de mon NAS (RS812RP+) DSM 4.3...

Ma problématique est la suivante : mon NAS est integré dans un domaine AD de Microsoft, sa fonction principal étant de faire un serveur de fichier.
Je me suis aperçu que les utilisateurs de mon domaine pouvait se connecter sur le NAS en utilisant bien sur leur identifiant du domaine, il se retrouvent alors dans l'environnement web du Synology... Hors je ne souhaite pas qu'ils interfère dans toute la configuration du Synology
(Partage de dossier etc...) (je souhaite que seul l'admin du domaine ou l'admin locale accede à la page web du synology); mais quid des autres services (DS File, DS Cloud etc)seront-ils toujours accessibles pour mes utilisateurs du domaine ?

Merci pour vos suggestions.

Cordialement.

Mr Xhark - @xhark
dit :
15 janvier 2014 à 15h14

> @kid A: Il est vrai que l'accès web fonctionne mais reste très limité et se cantonne aux accès de l'utilisateurs avec FileStation. Rien n'est outrepassé et cela ne pose pas de problème de sécurité. A ma connaissance il n'existe pas d'option particulière permettant d'interdire cet accès. Sinon avec le pare-feu ou au niveau IP pour que ce soit plus radical.

p6ril dit :
9 avril 2014 à 8h02

Bonjour, article intéressant.

Pour ceux qui ont activé l'identification en 2 étapes, sachez qu'il y a un moyen de sauvegarder vos codes de sécurité (en cas de souci avec les notifications, ce qui m'est arrivé).

Pour cela il faut un accès ssh au système. Dans le répertoire /usr/syno/etc/preference/ se trouve un fichier appelé google_authenticator. Celui ci contient les codes d'activation d'urgence. A priori vous pouvez même ajouter des codes supplémentaires si vous avez déjà utilisé les 5 disponibles.

Je me suis retrouvé bloqué après un reset de mon téléphone (j'avais oublié que j'avais Google Authenticator dessus) et des notifications qui ne fonctionnaient pas. Cela m'a permis de restaurer mon accès (fort heureusement j'avais laissé le serveur ssh actif sur le système).

En terme de sécurité, je pense qu'il manque un point essentiel : l'activation d'un VPN. En effet dans les paquets additionnels Synology, il existe un serveur VPN qui permet de mettre en oeuvre une connexion OpenVPN depuis internet. Cette approche est sécurisée car pour mettre en place le tunnel il faut disposer du certificat. Ainsi depuis l'extérieur il suffit de ne laisser qu'un seul port ouvert (le 1194 en standard pour openVPN mais on peut le NATer) et de limiter les accès "classiques" au sous-domaine (privé) derrière la box / le routeur. C'est plus sécurisé que de laisser un accès ouvert en ssh sur le routeur pour ouvrir des adresses IP supplémentaires. Seule limite (mais de taille pour un PME), le VPN ne supporte que 5 connexion simultanées au maximum.

chreggy dit :
20 mai 2014 à 11h28

Bonjour,

sympa cette discussion autour de la sécurité du Nas. J'ai quand même un point personnel qui me dérange sur les Synology (même si je suis fan que je possède un DS-213+), c'est qu'on ne peut pas désactiver le bouton Reset pour le mdp admin. Du coup, çà laisse au gars qui pique le nas de monter les volumes cryptés.

Existe-t-il une solution ? Le fait de désactiver le compte admin corrige le problème ?

Mr Xhark - @xhark
dit :
21 mai 2014 à 10h15

@chreggy: normalement tu choisis une clé que tu exportes, je n'ai jamais testé mais je doute qu'un reset supprime cette clé. As-tu testé ?

Commentaire (NO FOLLOW) (requis, restez courtois et/ou constructif)
Un nom de site abusif à la place d'un pseudo/nom sera signalé comme spam :

Pseudo (requis)

Email (requis, ne sera pas publié)

Site web (pub abusive sera sanctionnée)

Identifiant Twitter (facultatif, sans @)

Me notifier des réponses par email (ou m'abonner sans commenter)

Tags xhtml autorisés :
<a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <del datetime=""> <i> <q cite=""> <strike>

Une combinaison de touche secrète se trouve dans cette page, saurez-vous la trouver ?

chargement