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 : <u>https://docs.ovh.com/fr/domains/utilisation-dynhost/</u>
- 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 :

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 | Rése | eau | | | | | | |
|------------------------------------|--|------------------------|---------------------------|--------------|------------|-------------|------------|-----------------------|
| - DUIDD | NATIONT | DNIG | | D. D.10 | 5147 | NTO | 10.0 | |
| | NAT/PAT | DNS | UPnP | DynDNS | DMZ | NIP | IPv6 | |
| Le serveu réseau lo Uniqueme | r DHCP de vi cal. ent pour des é | otre Liveb équipeme | oox attribue nts IPv4. | e automatiqu | iement une | e adresse I | P à chaque | e équipement de votre |
| Parame | ètres du se er le serveur l | erveur l | DHCP | | | | | |
| Adresse I Livebox | P de votre | 19 | 2.168.1.1 | | | | | |
| Masque o | e sous-résea | u du 25 | 5.255.255. | 0 | | | | |
| Adresse I | P de début | 19 | 2. <mark>16</mark> 8.1.10 | 0 | | | | |
| Adresse I | P de fin | 19 | 2.168.1.15 | 0 | | | | |
| | | | | | | An | nuler | Enregistrer |

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

| Retour | Rés | eau | | | | | | | | | |
|---|--|---|--|---|-------------------------------------|--|--------------------------|-------------------------------|------------------------------------|------------------------------|--------|
| DUCP | | DNS | LIDeD | DupDNS | DMZ | NTD | IDve |) | | | |
| DHOP | NAI/FAI | DNS | UFIIF | DynDias | DIVIZ | INTE | IF VO | J | | | |
| Les règle votre rése équipeme Uniqueme | s NAT/PAT s eau. Utiles po ent a une adr ent pour des | ont nécess our certain resse IP sta équipeme | saires pour es applicat atique (par nts IPv4. | r autoriser un tions comme ramètrable da | e commu des jeux ans l'ongl | unication init en lignes o et DHCP). | iée depuis u des serv | s Internet av veurs de typ | rec un équipement e FTP Assurez | particulier d vous que ce | e t |
| Vos règ Choisisse Nous vou Les équip | gles perso ez des ports s déconseille ements doiv | onnalisé qui ne son ons la créa vent être co | es t pas bloqu tion d'une onfigurés a | ués par le par règle sur le p ivec une adre | re-feu. bort 53 (s esse IP st | ervice DNS atique pour |). être dispo | onibles. | | | |
| | | | | | | | | | | | |
| FTP Ser | ver | ▼ 21 | | 21 | то | P V | | | ▼ Toutes | | Créer |
| | | ex. : 1 | 000 | ex. : 1000-2 | 2000 | |] | | IP externes a | utorisées | |
| | | | | | | _ | _ | | 4 . | - | |
| Activer | App | lication/S | ervice | Port in | terne | Port extern | ne P | | Equipement | Toutes | 命 |
| | We | h Server (k | | 80 | | 80 | T | | DS1517 | Toutes | 品 |
| | Secure | Web Serve | er (HTTPS) |) 44 | 3 | 443 | т | CP/UDP | DS1517 | Toutes | 命 |
| | 2 Source | | | - | | - | т | CP/UDP | - | Toutes | 命 |

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 éq | uipements cor | nnectés | | |
|--|--|-----------------------|---------|-------------|
| Carte Liste | | | | |
| ŵ Wi-Fi ﷺ ﷺ ₩ DAP | Paramétrer l'équiper Type d'équipement nom Adresse IP | DS1517 192.168.1.8 | • | |
| DGS-1210-16 | Adresse MAC Connexion Internet | connecté | | |
| DS214se | Paramétrer son acc | ès à Internet | | |
| Google-Nest | Bloquer en permanenc Planifier | e | | |
| NVIDIA SHIELD | | | Annuler | Enregistrer |

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 :

| | | DNS Server | | ? - 8 X |
|--------------|-----------------|-----------------------------------|--------|----------------|
| Tones | Créer 🗸 Modifie | er 🗸 Exporter la zone 👻 Supprimer | | |
| 1 Londo | ID de zone | Nom de domaine | Туре | Statut : |
| Résolution | Com | Market Market | master | Activé |
| Journal | | | | |
| 🔊 Clés | | | | |
| Vues | | | | |
| 🔯 Paramètres | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | 1 élément(s) C |

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

| Modifier | les paramètres de zone |
|---|--|
| ID de zone: | and the second |
| Nom de domaine: | and the com |
| Statut: | Activer 👻 |
| Format série: | Nombre entier 👻 |
| Limiter le transfert de zone | |
| Spécifiez quelles zones slav zone master. | e peuvent demander les fichiers de zone de cette |
| Règle de transfert de zon | e |
| Limiter le service IP source | |
| Spécifiez quels hôtes peuve | nt interroger le serveur DNS sur cette zone. |
| Liste d'IP source | |
| Activer la notification des zo | ones esclaves |
| Spécifiez quelles zones escl de ce serveur DNS change. | aves doivent être notifiées lorsque la zone principale |
| Liste des IP des zones es | claves |
| Limiter la mise à jour de zo | ne |
| Spécifiez les clients qui peu cette zone principale. | vent demander une mise à jour de zone à partir de |
| Règle de mise à jour de z | zone |
| | |
| | |
| | OK Annuler |

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

| | Liste d'IP sou | Irce |
|----------------|----------------|------------------------|
| Créer Modifier | Supprimer | |
| Туре | | Liste d'IP source |
| Sous-réseau | | 192.168.1.0/255.255.25 |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

Paramétrer la rubrique « enregistrement de ressource » :

| 5 | | | DNS Server | | | 7 - 0 | × |
|------------|------------|-----------------------------------|--|-----------|--------|--------------|---|
| Tones | Créer 🗸 | Modifier 👻 | Exporter la zone 👻 | Supprimer | | | |
| Y- 20105 | ID de zone | Désactive | er | ne | Туре | Statut | E |
| Résolution | maximum | Paramètr | es de zone | | master | Activé | |
| Journal | | Enregistr Enregistr Changer | ement SOA ement de ressource à zone master | | | | |
| 🔊 Clés | | | | | | | |
| Vues | | | | | | | |
| Daramètres | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | 1 élément(s) | С |

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

| 6 | | DNS | Server | | | 7 - 8 | × |
|--------------|---------------------------|------------|--------------|--------------------|---|--------------|---|
| V Zones | Modifier | l'enregist | trement de l | ressource | | | |
| | Créer - Modifier Supprime | er | | X Recherche | | Statut | 1 |
| Resolution | Nom | Туре | TTL | Information | 1 | Active | |
| journal | former and the second | A | 86400 | 192.168.1.8 | | | |
| - | _ | А | 86400 | 192.168.1.8 | | | |
| JP Clés | jeedom | A | 86400 | 192.168.1.8 | | | |
| | Research Com. | A | 86400 | 192.168.1.8 | | | |
| Vues | ns. om. | A | 86400 | 192.168.1.8 | | | |
| Paramètres | | А | 86400 | 192.168.1.8 | | | |
| - Farametres | _ | NS | 86400 | nstanto incom. | | | |
| | | | | | | | |
| | | | | 7 ((()(-) | ~ | | |
| | | | | 7 element(s) | G | | |
| | | | | Termine | r | | |
| | | | | | | 1 élément(s) | С |

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) :

| 6 | DNS Se | erver | 7 - 8 X |
|--------------|------------------------------------|--|-----------------|
| Zones | Résolution | | |
| Résolution | Activer les services de résolution | | |
| Journal | Spécifiez quels hôtes sont aut | torisés à envoyer des requêtes récursives. | |
| P Clés | Activer les redirecteurs | 80 10 245 2 | |
| Vues | Redirecteur 2: | 80.10.246.129 | |
| 🔯 Paramètres | Politique de redirection: | Rediriger d'abord 💌 | |
| | | | |
| | | | |
| | | | |
| | | Applique | r Réinitialiser |

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 :

| | | Panneau de confi | guration | | 7 - E X |
|------------------------|------------------|---------------------|--------------------------|---------------|-------------------|
| Recherche | DDNS Confi | guration du routeur | lvancé | | |
| ∧ Partage de fichiers | Ajouter Mod | ifier Supprimer | Mettre à jour maintenant | Personnaliser | |
| Cossier partagé | Fournisseur de s | Nom d'hôte | Adresse externe | Statut | Dernière heure de |
| 🚭 Services de fichiers | OVH | Com | 92 70 | Normal | 10/02/2021 21:15 |
| 2. Utilisateur | | | | | |
| 👷 Groupe | | | | | |
| Domaine/LDAP | | | | | |
| ∧ Connectivité | | | | | |
| QuickConnect | | | | | |
| 🚯 Accès externe | | | | | |
| 🏠 Réseau | | | | | |
| 🔝 Serveur DHCP | | | | | |

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

| N. Contraction of the second s | Pannea | u de configuration | 2 - 5 | × |
|--|--------------------------|------------------------------|-------------|---|
| Recherche | Application Proxy invers | é Profil de contrôle d'accès | | |
| Matériel et alimentation | Créer Modifier Supp | rimer | | |
| Périphériques externes | Description | Source | Destination | 1 |
| • restauration | | | | |
| | | | | |
| Privilèges | | | | |
| Portail des applications | | | | |
| Q Services d'indexation | | | | |
| Synchronisation du | | | | |
| Terminal & SNMP | | | | |
| 👗 CMS | | | | |

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 » :

| Général | En-tête personnalisé Paramètres avancés | | | | |
|-----------------------------|---|--------|-----------------|---|---|
| Proxy invers | śé | | | | |
| Description: | | jeedon | n.mondomaine.co | m | |
| Source | | | | | |
| Protocole: | | HTTPS | | • | |
| Nom d'hôte: | | jeedom | n.mondomaine.co | m | |
| Port: | | 443 | | | |
| Activer | HSTS | | | | |
| Activer | HTTP/2 | | | | |
| Activer | le contrôle d'accès | | | | |
| Profil de | e contrôle | | | - | 9 |
| d'accès | : | | | | |
| Destinatio | 'n | | | | |
| Protocole: | | HTTPS | | • | |
| Nom d'hôte: | | 192.16 | 8.1.X | | |
| | | 443 | | | |
| Port: | | | | | |

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 » :

| | Panneau de configuration P - 🗖 🗙 |
|---------------------|--|
| Recherche | Interface réseau Fournisseur PXE |
| 2 Utilisateur | Modifier Désactiver DHCP |
| 👷 Groupe | Rend 1 Activé |
| Domaine/LDAP | Adresse IP de d Adresse IP de fin Masque de sous Passerelle Activé |
| ∧ Connectivité | 192.168.1.100 192.168.1.150 255.255.255.0 192.168.1.1 Oui |
| ØuickConnect | DNS secondaire 192.168.1.7 |
| 😚 Accès externe | |
| 🏠 Réseau | |
| \delta Serveur DHCP | |
| 🖯 Sécurité | |
| ∧ Système | |
| infos | |

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) :

| | | Modifier | | |
|-------------------------|------------------------------|-----------------------|-------------|--------------|
| DHCP Server Clients | DHCP | | | |
| Activer le serveur DHCF | , | | | |
| DNS principal: | 192.168.1.8 | | | |
| DNS secondaire: | 192.168.1.7 | | | |
| Nom de domaine: | | | | |
| Activer la découve | rte automatique du proxy web | 1 | | |
| URL: | | | | |
| Liste de sous-réseau: | | | | |
| Adresse IP de début | Adresse IP de fin | Masque de sous réseau | Passerelle | 🖌 Activé |
| 192.168.1.100 | 192.168.1.150 | 255.255.255.0 | 192.168.1.1 | \checkmark |
| 1 | - | | | |
| Ajouter Modifier | Supprimer | | | OK Annule |

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 :

| Active | | | м | lodifier le sous-rése | au DHCP | | |
|--------|------------------------|--------|----------------|-----------------------|---------|--|---|
| DNS | Adresse IP de début: | | 192.168.1.100 | | 0 | | |
| DNS | Adresse IP de fin: | | 192.168.1.150 | | 0 | | |
| Nom | Masque de sous rése | au: | 255.255.255.0 | | | | |
| | Passerelle: | | 192.168.1.1 | | | | |
| - La | Durée de bail de l'adi | resse: | 691200 | | | | |
| Liste | Options DHCP: | | | | | | |
| esse | Activé | Co | Nom | Valeur | | | |
| .168 | | 7 | log-server | | | | |
| | | 9 | lpr-server | | | | |
| | | 13 | boot-file-size | | | | |
| | | 16 | swap-server | | | | |
| | | 17 | root-path | | | | |
| | | 18 | extension-path | | | | - |
| outer | | | | | | | |

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

| | | Modifier | | |
|---|-------------------------------|---|---------------|-----------------------|
| DHCP Server Clients DHCP | | | | |
| Actualiser Ajouter Modifier | Effacer Clients DHCP | | | Y |
| Ajouter à la réservation d'adresse | IP | MAC/DUID | Nom d'hôte | Expiré dans |
| a | 192.168.1.102 | c8:1000000000000000000000000000000000000 | RMMini3 | 0 jour(s) 18 heure(s) |
| a | 192.168.1.111 | d4 | CLIMATISATION | 0 jour(s) 15 heure(s) |
| 6 | 192.168.1.116 | e4 manual man | FIGHT | 5 jour(s) 3 heure(s) |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| Remarque: Réservez l'adresse IP pour le p | ériphérique actuel en cliquar | nt sur l'icône du verrou. | | |
| | | | | |
| | | | | OK Annuler |

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) :

| | Panneau de configuration | 7 - E X |
|---------------------|--|---------|
| Recherche | Sécurité Pare-feu Protection Compte Certificat Avancé | |
| 🧱 Groupe | Ajouter - Configurer CSR | |
| Domaine/LDAP | Ajouter 1 | ~ |
| ∧ Connectivité | Supprimer Modifier 10 - 08/05/2021 | |
| ØuickConnect | Exporter le certificat | ^ |
| 😚 Accès externe | Renouveler le certificat R3 jeedom om Pour jeedom om | |
| 🏠 Réseau | | |
| \delta Serveur DHCP | | |
| 😌 Sécurité | | |
| ∧ Système | | |
| 👔 Centre d'infos | | |
| 🥵 Thème | | |

Choisir « Ajouter un nouveau certificat » :

| Créer un certificat | × |
|--|---------|
| Veuillez choisir une action | 6 |
| Ajouter un nouveau certificat | |
| Importez un certificat, créez un certificat auto-signé ou procurez-vous un certificat aup Let's Encrypt. | irès de |
| Remplacer un certificat existant | |
| Importez un certificat, créez un certificat auto-signé ou procurez-vous un certificat aup Let's Encrypt pour le remplacement d'un certificat. jeedom | rès de |
| Suivant Ann | nuler |

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



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

| | Créer un certificat | × |
|--|--|---|
| Procurez-vous u | n certificat auprès de Let's Encrypt | |
| Nom de domaine: | jeedom.mondomaine.com | |
| Courrier électronique: | adresse@mail.com 👻 | |
| Autre nom de l'objet: | *.example.com | |
| Remarque : Selon les règl des certificats et le nombr | es de Let's Encrypt, le nombre d'adresses e-mail pour l'enregistrement e de demandes de certificats sont tous deux limités. | |
| Retour | Appliquer Annuler | |

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) :

| Services | Certificat | 1 |
|-------------------------------|------------|---------|
| jeedom. | jeedom. | ~ |
| | | |
| FTPS | synology | - |
| Paramètres système par défaut | synology | · · · · |
| Replication Service | synology | |
| | ovpology | _ |

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

| | Panneau de configuration | - = × |
|---------------------|---|-------|
| Recherche | Sécurité Pare-feu Protection Compte Certificat Avancé | |
| 🧏 Groupe | Ajouter Configurer CSR | |
| Domaine/LDAP | synology - 16/09/2021 (Certificat par défaut) | ~ |
| ∧ Connectivité | jeedom 08/05/2021 | |
| 🕖 QuickConnect | ♥ jeedom Émis par R3 | ^ |
| 😚 Accès externe | Autre nom de l'objet jeedon com Pour jeedon com | |
| 🏠 Réseau | | |
| \delta Serveur DHCP | | |
| 💎 Sécurité | | |
| ∧ Système | | |
| 🕡 Centre d'infos | | |
| 🛞 Thème | | |

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 » :

| R EEDOM | 🛠 Accueil 👻 | 😲 Analyse | - PC | utils + | æ1 | Plugins 🗸 | 🗘 Réglag | 18 🕶 | | | | | 11:19:00 |
|----------------|------------------|------------------|---------------|--------------------|---------|-------------|---------------|----------------|--------|-----------|--|--------------------------|-------------------------------------|
| Rechercher | | | | | | | | | | | | | × Sauvegarder |
| 🗲 Général | 🖵 Interfac | e 🔊 Réseaux | Logs | 🎛 Rés | umés | Equiper | ients 📾 Ra | oports 🚓 L | iens | 🖢 Intera | ctions 🛛 Securité 🚍 Mises à jour/Mark | et 🖴 Cache 👂 API 🔪 OS/DB | |
| Attention : c | ette configural | ion n'est là qu | e pour info | rmer Je | edom di | e sa config | uration résea | ı et n'a aucur | n impa | ct sur le | s ports ou l'IP réellement utilisés pour joind | re Jeedom | |
| Accès int | erne | | | | | | | | | | | | |
| | | Protocole | | | | 92.168.1 | | | | | | | |
| Accès ex | terne | | | | | | | | | | | | |
| | | Protocole | | | | eedom | om | | | | | | |
| Gestion a | vancée | | | | | | | | | | DNS (proxy) Market | | |
| Interface | | | | | | Mac | | | | | Attention : cette fonctionnalité n'est par | | munity (voir votre service pack sur |
| lo | | | | | | 00:00:00:00 | 00:00 | | | | Construction of the second | | |
| ens192 | | 192.168.1 | | | | | | | | | Utiliser un proxy pour le market | | |
| Dé | | | | m v | | | | | | | Activer le provi | | |
| Masque IP | local (utile que | pour les insta | allations typ | ie *) | | | | | | | Addresse proxy | | |
| | MTU spéc | ifique pour le l | DNS (exper | | | | | | | | Port du proxy | | |
| | | | | | | | | | | | Nom d'utilisateur | | |
| | | | | | | | | | | | Mot de passe | | |
| | | | | | | | | | | | | | |

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 ③