**NAT (Network Address Translation)**

3 types

1. Nat statique traduit une adresse IP privée en une adresse publique.

L’adresse publique est toujours la même.

1. NAT dynamique les adresses IP privées sont mappées au pool d’adresses publique.
2. PAT (adresse Port Translation) une adresse IP publique est utilisée pour tous les périphériques internes, mais un port différent est attribué à chaque adresse IP privée. Également connu sous le nom de surcharge de NAT.

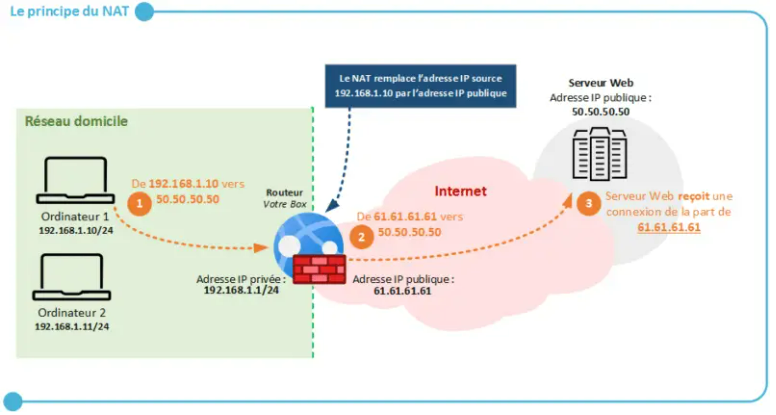
Comment ça marche ?

Aller :

Mon ordinateur IP 192.168.1.10/24 va tenter de se connecter au serveur Web 50.50.50.50.

La requête envoyée passe par la box (passerelle, routeur), le routeur va modifier le paquet réseau et remplace l’@ par 61.61.61.61 qui est l’adresse publique de ma box et le paquet est émis au server Web.

La requête arrive au serveur Web et voit que la requête provient de IP.61.61.61.61 et à aucun moment il n’a connaissance de mon adresse privée.

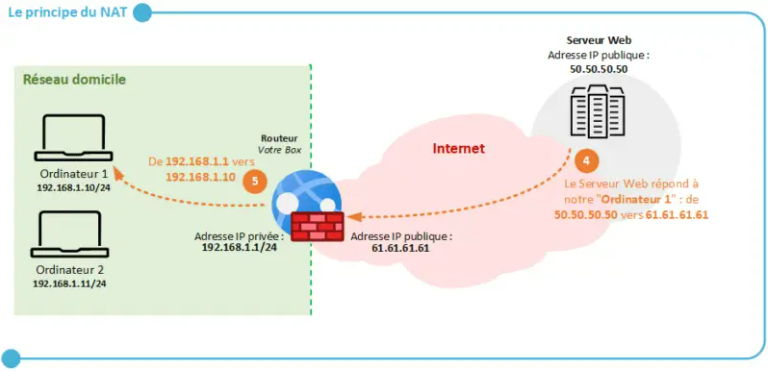


Retour :

Le serveur Web répond en envoyant sa réponse sur l’adresse IP publique 61.61.61.61 du routeur.

Le routeur réceptionne, et le routeur a mémorisé cette connexion (grâce à une table de translation) et donc il sait qu’elle doit adresser le paquet reçu de la part du serveur web à l’ordinateur 1.

A partir de son adresse IP 192.168.11, le routeur envoie la réponse à l’ordinateur 1, mais l’ordinateur 1 voit la réponse comme si elle provenait directement du serveur Web 50.50.50.50.



L’objectif du NAT Statique (NAT one-to-one) : est de traduire une IP privée en un adresse IP public, en fonctionnant par association statique, c’est-à-dire un pour un. (@ privée est associée à une @ publique)

|  |  |  |
| --- | --- | --- |
| Appareils | Adresse IP privée | Adresse IP publique |
| PC1 | 192.168.1.10 | 61.61.61.61 |
| PC2 | 192.168.1.11 | 61.61.61.62 |

Ainsi l’ordinateur 1 accédera à Internet par l’intermédiaire de son IP 61.61.61.61.

Ainsi l’ordinateur 2 accédera à Internet par l’intermédiaire de son IP 61.61.61.62.

Ce mécanisme montre rapidement ses limites car chaque machine du réseau interne doit disposer à la fois d’une adresse IP privée et une adresse IP publique.

Cette configuration peut servir à rendre accessible un serveur Web en lui attribuant (en quelque sorte) une adresse IP publique.

Cependant pour publier un serveur Web sur Internet de façon sécurisé, il est préférable d’utiliser un reverse proxy, ou éventuellement une règle de redirection de port pour autoriser uniquement les flux HTTPS, par exemple.

Pour finir, sachez qu’avec du NAT statique, l’équipement du réseau local est accessible depuis Internet via son @ IP publique puisqu’il y a un mappage entre les deux @ IP (privée/publique)

L’objectif du NAT Dynamique est différent du NAT statique car : les associations entre une adresse IP privée correspondante à une machine et une adresse IP publique disponible sur le routeur seront **dynamiques et temporaires** !

L’objectif du PAT (port address translation) est une forme de NAT dynamique, que l’on appelle NAT overlay ou Masquerade NAT avec quelques différences très intéressantes, qui font du PAT le mode le plus couramment utilisé. C’est une association dynamique et temporaire entre @IP public/privée sauf qu’il ajoute un numéro de port d’où le terme PAT.

Grâce au PAT une seule et même adresse IP publique peut être utilisée par X machines connectées sur le réseau local. C’est exactement ce qu’il se passe à la maison.

Si deux ordinateurs se connecte au même serveur Web le serveur verra deux connexions différentes en provenance de l’adresse IP public 61.61.61.61 mais pas le même port grâce au PAT.

Un numéro de port est associé à chaque connexion cela constitue la table de traduction (table de translation).

*DNAT pour les redirections de ports* :

Le port forwarding on parle de Source NAT quand c’est l’adresse IP source du paquet qui est modifiée (un PC du réseau local accède à un site internet) de Destination NAT (quand c’est l’adresse IP de destination du paquet qui est modifiée (un PC connecté à Internet accède à un NAS du réseau local)

Grâce à une redirection de port, une machine connectée au réseau local et qui dispose d’une adresse IP privée pourra être accessible depuis l’extérieur, sur un ou plusieurs ports spécifiques via l’adresse IP publique du routeur (box)

*Une seule règle par port TCP/UDP* :

Il ne peut y avoir qu’une seule règle par port TCP/UDP ! Autrement dit, s’il y a deux serveurs Web avec deux adresses IP privées différentes, ils ne pourront pas tous les deux être accessibles en HTTPS sur le port 443, car le port extérieur ne peut être associée à une seule adresse privée (puisque l’on a une seule adresse publique si on avait deux ce serait possible)

Dans ce cas il sera nécessaire de passer par un reverse proxy (recommandé) pour travailler niveau http/HTTPS directement et identifier le nom de domaine dans les requêtes.

*Le port mapping* :

Il faut savoir que ce n’est pas obligatoire d’utiliser le même numéro de port pour la source et la destination. Le NAS en local peut être accessible via le port 443, mais on peut décider de le rendre accessible depuis l’extérieur sur le port 65001, dans ce cas on parle de port mapping même principe que le port forwarding sauf que l’on utiliser deux numéros de port différents.

A savoir :

Le port externe impacte le client connecté à internet :

Si l’on met le port 65001 pour une interface web, le client devra saisir <https://ippub:65001>

Le port interne impacte le serveur/la machine de destination :

Si l’on met le port 443 le service sur serveur de destination devra être en écoute sur ce port, donc on ne peut pas le choisir au hasard il faut que ce soit cohérent.

Même si le numéro de port n’est pas le même, le client ne verra pas la différence si l’on fait une correspondance 65001 :65001 ou 65001 :443

Plage d’adressage

|  |  |  |
| --- | --- | --- |
| Adresse IP privées Non routable | | Adresse IP privées Non routable |
| Classe | Plage d’adresse IP privée | Plage d’adresse IP publique |
| A | 10.0.0.0 – 10255.255.255 | 1.0.0.0 – 9.255.255.255  11.0.0.0 – 126.255.255.255 |
| B | 172.16.0.0 – 172.31.255.255 | 128.0.0.0 – 172.15.255.255  172.32.0.0 – 191.255.255.255 |
| C | 192.168.0.0 – 192.168.255.255 | 192.0.0.0 – 192.167.255.255  192.168.0.0 – 223.255.255.255 |
| D | 224.0.0.0 – 239.255.255.255 | Adresse de multicast |
| E | 240.0.0.0 – 255.255.255.255 | Adresses réservées par l’IETF |
|  | 127.0.0.0 localhost | |
|  | 0.0.0.0 réservé utilisé pour définir une route par défaut sur un routeur | |

**Proxy reverse-proxy**

Serveur mandataire, est un serveur qui jouera le rôle d’intermédiaire entre un client et un serveur distant. Les ports sont 3128 et 8080

Le but :

Filtrage : permettre de bloquer certains sites ou certaines catégories de sites.

Cache : permettre de mettre en cache les requêtes, pour les retourner plus rapidement aux postes de travail.

Compression : permettre de réduire le poids des pages au moment de retourner le résultat aux clients.

Journalisation : toutes les requêtes reçues de la part des clients (poste de travail) seront stockées dans des journaux (logs).

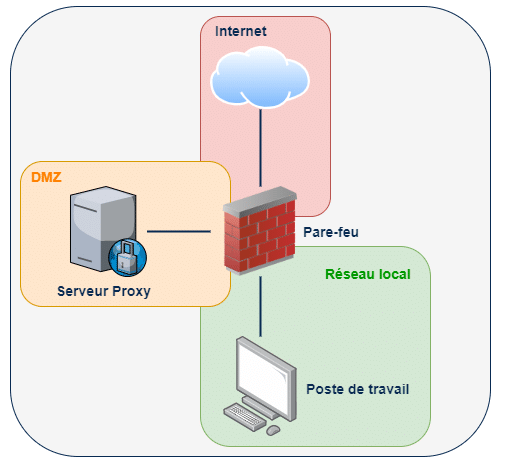
Anonymat : le poste de travail se cache derrière le proxy, le serveur Web verra seulement le proxy.

Doits d’accès : il peut servir à positionner des droits d’accès pour filtrer les accès, au-delà du filtrage Web.

1. Intégrer un proxy et proxy transparent

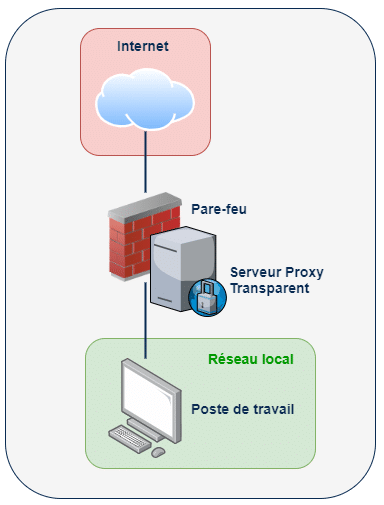
En entreprise ou milieu scolaire il est très fréquent de l’utiliser pour réaliser du filtrage Web afin de sécuriser la navigation Internet des utilisateurs.

Proxy classique

Le proxy est déclaré sur le poste client

Le proxy dans une DMZ donc les clients contactent le serveur proxy isolé et c’est le serveur qui se connecte à internet et non les postes clients directement. Dans certains cas la fonction de proxy est assurée directement par le par-feu et dans ce cas il n’y a pas de notion de DMZ.

Proxy transparent (implicite)

Le proxy ne doit pas être configuré sur le poste et ce dernier l’utilisera sans s’en rendre compte, car le proxy sera utilisé comme passerelle au niveau de la configuration du poste client. C’est la configuration idéale pour filtrer le trafic émis par les postes clients.

Regroupée sur un même serveur/équipement. Même si l’on pourrait mette le serveur proxy transparent sous le pare-feu et que les trames soient relayées entre le proxy et le pare-feu.

Pour la configuration poste à poste nous avons les solutions pour un parc informatique :

Utiliser ne GPO pour déployer les paramètres de configuration sur les postes (niveau windows ou navigateurs)

Utiliser un GPO pour préciser l’emplacement d’un script d’auto-configuration (proxy.pac (proxy automatique configuration)) fonction javascript FindProxyForURL dont l’objectif est d’indiquer si pour une URL le navigateur doit passer par le proxy.

1. Les logiciels pour mettre en place un proxy

Gratuit :

Squid un logiciel qui permet de monter un proxy (ou reverse-proxy) sous linux.

Si l’on monte u pare-feu avec PfSense il est possible d’installer le paquet Squid pour ajouter la fonctionnaliter de proxy à son pare-feu. En complément, l’installation du paquet Squid-Guard permettra d’effectuer du filtrage Web.

Payant : Olfeo et UCOPIA.

1. Proxy de mise en cache

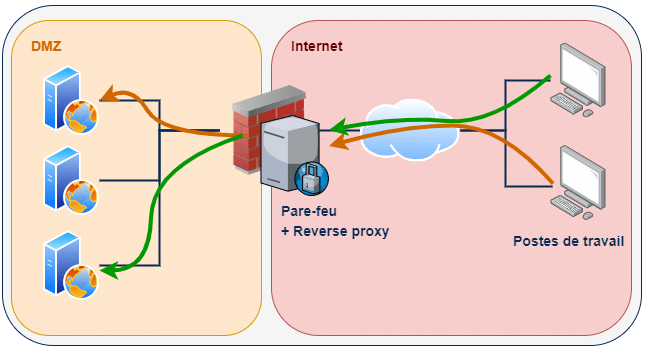
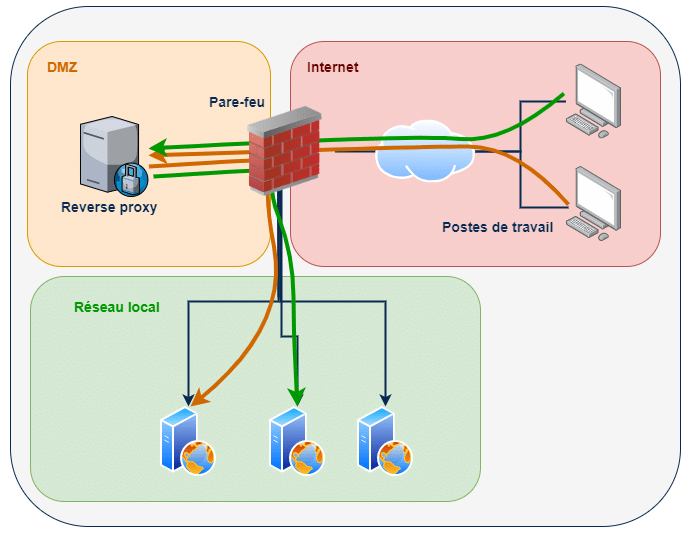
Un proxy de mise en cache appelée proxy-cache effectue la mise en cache des données sur son disque local. On peut l’utiliser pour distribuer des mises à jour de logiciels : le proxy télécharge une fois la mise à jour sur internet et la mettre en cache, et ensuite la distribuer aux postes clients directement plutôt que chaque poste se connecte sur internet pour télécharger la mise à jour comme l’éditeur ESET propose une fonctionnalité de mise en cache pour distribuer les mises à jour des signatures antivirus.

**reverse-proxy**

Il permet aux utilisateurs externes d’accéder à une ressource du réseau interne.

Vous accédez à une ressource protégée par un reverse proxy, vous contactez le reverse proxy et c’est lui qui gère la requête pour contacter le serveur cible à votre place et vous retourner la réponse. Le client n’a pas de visibilité sur le ou les serveurs cachés derrière le reverse proxy.

Un cas d’usage courant c’est d’avoir plusieurs serveurs Web derrière une reverse proxy. Ce dernier va pouvoir répartir la charge entre les différents serveurs Web et en cas de panne d’un serveur vous ne verrez pas la différence, car le proxy orientera les requêtes en conséquence selon l’infrastructure.



Si le serveur reverse proxy est un serveur à part entière, on va venir le positionner en DMZ et dans ce cas les serveurs web peuvent être connectés au réseau local. Il peut aussi mettre en cache des ressources (script javascript) afin de soulager les serveurs Web, mais aussi pour améliorer les performances du site grâce à la compression des données.

1. L’en-tête http et le champ X-Forwarded-For

Le proxy peut configurer l'en-tête "X-Forwarded-For" pour ajouter à l'en-tête des requêtes HTTP l'adresse IP du client d'origine. De cette façon, le serveur qui reçoit la requête du reverse proxy pourra tracer le client d'origine malgré tout puisque le reverse proxy lui communique l'information.

Cette notion est importante d'un point de vue de la sécurité, notamment si elle est gérée sur le serveur Web directement : on pourra bloquer uniquement ce client s'il effectue une attaque brute force sur notre serveur Web, plutôt que de bloquer le reverse proxy, ce qui serait forcément problématique.

1. Logiciel de reverse-proxy

Apache et son module (mod\_proxy).

Nginx

Windows IIS

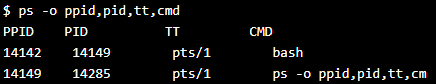
HAProxy gratuit et open source.

Squid ou si on utilise un par feu PfSense nous pouvons lui ajouter le paquet Squid.

**Gérer votre serveur Linux et ses services**

1. Service linux (deamon)

Processus : ps -o ppid,pid,tt,cmd



Avec SystemV

/etc/init.d #répertoire contenant les scripts de démarrage/arrêt des

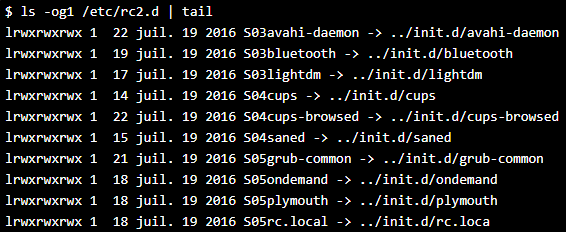
#deamons (start/stop/restart/reload/status)

runlevels 0 à 6 (0 arrêt, 1 maintenance root sans réseau, 6 redémarrer le système)

runlevels 2 à 5 modes multi-utilisateurs graphiques ou console. Le mode par défaut dans /ect/inittab.

Pour chaque runlevels nous trouvons un répertoire /ect/rcX.d, où X est le runlevel /etc/rc2.d/ dans ce répertoire vous trouvez les liens vers les scripts de /etc/init.d qui sont démarrer ou arrêter dans ce tunlevel. Les lines commencent par S pour deamons démarrer et K arrêter et la lettre est suivie d’un nombre de 00 à 99. Les scripts sont exécutés les uns après les autres dans l’ordre croissant des nombre et ordre alphabétique.

ls \_og1 /etc/rc2.d | call



Sous ubuntu avant le runlevel était 2 donc pour lancer apache au démarrage du système, il suffit de créer le lien symbolique :

lancer



Arrêt



Système simple mais les daemons sont lancés les uns après les autres, une gestion statique donc pas de changement d’état (coupure réseau, nouveau matériel) donc un nouveaux système de gestion :

1. Upstart et systemd

Upstart basé sur évènement avec le script de configuration dan /ect/init/ et la commande initctl permet de gérer les processus : sudo initictl start apache2

Systemd (toutes distribution et le nouveau) basé sur évènements souple et dynamique avec une gestion fine des dépendances (démarrage en parrallèle)

sudo systemctl start smbd #start/stop/status/enable/disable)

sudo systemctl list-units #les services sont de types service

sudo systemctl list-units --type=service #on peut voir qu’il y a 59 unité

sudo systemctl cat smbd.service #affiche le script du service [edit pour changer]

sudo systemctl deamon-reloade #relance ma configuration

plus le run-level mais target :

sudo systemctl get-default #graphiqcal.target

sudo systemctl list-dependencies graphical.target #voir les services qui seront lancées avec la target

sudo journalctl #affiche les log du système. [-b dernier log du boot système, -u smbd.service]

sudo journalctl -u smbd.service #affichie les logs d’un service

Utiliser les targets, on peut en avoir plusieurs en même temps.



Certaines targets comme swap.target correspondent à des fonctions du système qu’on peut activer ou non, et d’autres graphical.targer à des états cohérents du système qui ont des dépendances des différentes autres targets. [systemctl list-dependencies graphical.target]

1. Serveur de temps NTP

sudo timedatectl set-time "yyyy-mm-dd hh:mm:ss "

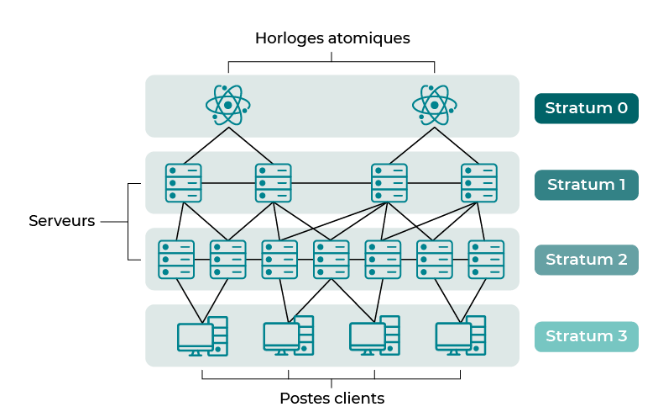
sudo timedatectl list-timezones | grep Paris #Europe/Paris

sudo timedatectl set-timezone Europe/Paris

sudo timedatectl status system-timesyncd.service #pour une machine mais plusieurs il faut un

#serveur NTP

NTP protocole de synchronisation de l’heure



Beaucoup d’organisations gèrent leurs propres serveurs de temps, certaines organisations permettent d’utiliser leur serveur d’autre privé. Le plus connu pool.ntp.org.

Ubuntu : systemd-timesyncd.service

Le serveur interne permet d’améliorer la synchronisation, , réduire le trafic, coupure internet …)

Serveur avec sudo apt-get install chrony

Configure chrony /etc/chrony/chrony.conf

Les lignes commençant pas pool indiquent l’adresse des serveurs NTP

Le fichier driftfile indique le fichier à utiliser pour enregistrer la dérive e temps de votre serveur par rapport au pool driftfile /var/lib/chrony/chrony.drift pour synchroniser plus vite chronyc sources. Expliciter l’autorisation de synchroniser avec allox 192.168.129/24 et lancer chrony (port UDP 123) on peut désactiver systemd-timesyncd par sudo timedatectl set-ntp false.

Configurer le client

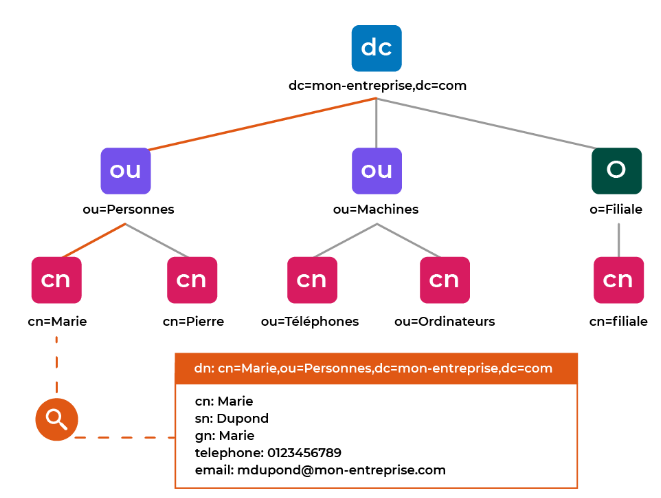
Ubuntu indiquer l’adresse du serveur dans /etc/systemd/timesyncd.conf et redémarrer systemctl restart systemd-timesyncd.

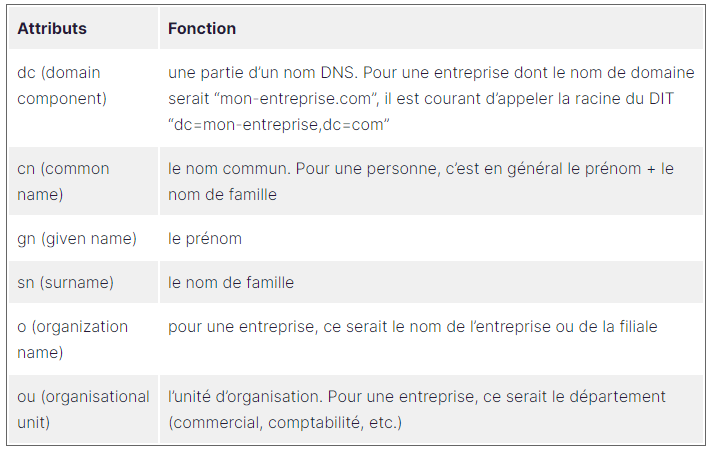
1. Annuaire LDAP (Lightweight Directory Access Protocol)

Base de données avec une structure hiérarchique plus rapide pour chercher mais lent pour modifier.

Utilisé pour l’authentification, informations de personnes (mail ; téléphone …) des objets (localisation, marque, modèle …), les applications d’entreprise (site web, e-mail, comptes système ordinateurs ....) pour valider les identifiants de connexions.

LDAP constitue un arbre appelé DIT (Dierectory Information Tree)





Le dn (distinguished name) de Marie : cn=Marie Dupond, ou =Personne, dc=mon-entreprise,dc=com.

Le RDN est la partie finale cn=Marie Dupond mais ne garantit pas l’unicité dans le DIT.

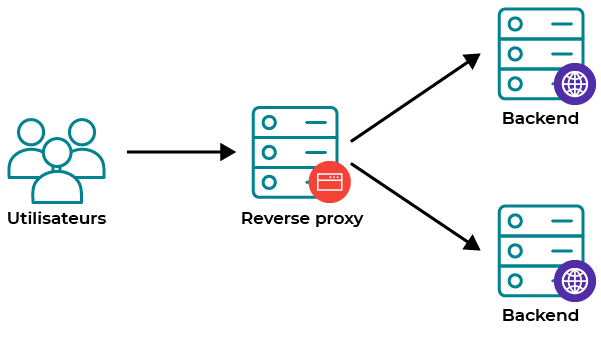
Ubuntu OpenLDAP sudo apt install slapd ldap-utils outils de config dpkg-reconfigure slapd.

ldapsearch commande cherche dans un annuaire.

LDIF (LDAP Directory Interchange Format) les modifications à réaliser dans LDAP.

Configuration avec LAM ou phpdapAdmin

1. Reverse Proxy



Nginx performant pour servir des fichiers statiques et pour analyser des URL.

Nginx écoute sur le port 80 et 443.

Apache : 7080 et 7443 + port Vhost pour a virtualisation.

Installer Nginx la configuration est /etc/nginx

/etc/nginx /\*.conf

/etc/nginx/modules-enables/\*.conf

/etc/nginx/sites-enabled/\*

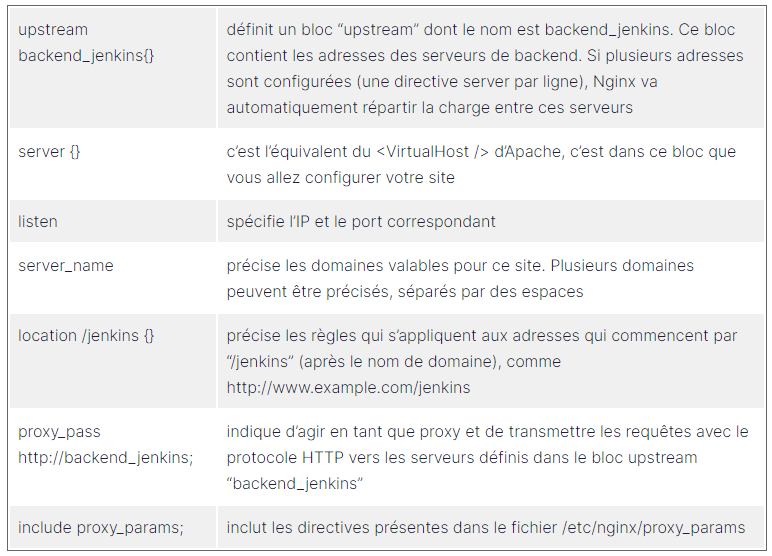
/etc/nginx/sites-availables #configuration de vos sites

Dans Nginx les virtual hosts s’appellent des server blocs cars ils sont configurés dans des blocs server{}

Créer le fichier

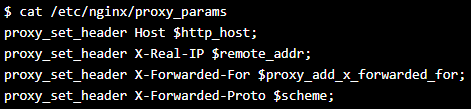
/etc/nginx/sites-available/01-www.example.com.conf #il permettra de joindre Jenkins et Apache et il contient :





Le fichier proxy\_params contient les directives les plus courantes pour les proxy web.

Elles indiquent les en-têtes http à transmettre :



L’en-tête host va permettre à Apache de savoir à quel virtual host transmettre la requête.

Les autres requêtes vont permettre à Apache de savoir que c’est un proxy qui transmet les requêtes, et de connaître la véritable IP des clients. Sans ça Apache s’imaginerait que toutes les requêtes viennent de 127.0.0.1.

Il reste à activez le sever block en faisant un lien symbolique vers les répertoires sites-enabled, et à recharger Nginx pour prendre en compte votre configuration :

$ sudo ln -s /etc/nginx/sites-available/01-www.example.com.conf /etc/nginx/sites-enabled/01-www.example.com.conf

$ sudo systemctl reload nginx

Enfin, même si Apache reçoit maintenant la veritable IP des clients dans l’en-tête X-Forwarder-For, il reste à installer le module rpaf pour que cette IP apparaisse dans les logs en tant qu’IP source des requêtes (et non 127.0.0.1)



Maintenant vous aurez l’adresse réelle de vos clients dans vos logs Apache.

!! si votre proxy Nginx et Apache sont sur des machines différentes, il faudra indiquer l’adresse IP de votre proxy dans le fichier de configuration du module /etc/apache2/mods-available/rpaf.conf

Au final dans la configuration ci-dessus, toutes les requêtes vers [www.example.com](http://www.example.com) commençant par /jenkins seront redirigées vers l’application Jenkins hébergée par Tomcat, et toutes les autres vers Apache.

Configurer Nginx pour utiliser HTTPS :

Certificat signés par Let’s Encrypt.

Voici la configuration dans le fichier /etc/nginx/sites-available/01-www.example.org.conf



Ce qui change server{} pour le port 80 contient une directive pour rediriger les requêtes en HTTPS.

Pour le port 443 la directive listen précise ssl en plus du port et ssl\_certificate et ssl\_certificate\_key indiquent les fichiers certificats à utiliser.

Vous pouvez utiliser le proxy pour vous connecter à vos backends, mais il est toujours possible à vos clients de se connecter directement à vos backends. Il faut donc configurer vos backends pour n’autoriser les connexions que depuis votre proxy.

Si c’est sur la même machine il faut les faire écouter que sur l’interface locale 127.0.0.

1 d’autres configuration utilise un pare feu.

Pour Apache mettre à jour /etc/apache2/ports.conf et ../site-available/01-www.example.com.conf pour remplacer les port 7080 par des 127.0.0.1 :7080 (idem 7443).

Pour Jenkins utiliser une valve tomcat permet d’agir comme un préprocesseur pour chaque requête. Elle va faire ses traitements entre réception de la requête et l’émission de la réponse.

Vous trouvez les valves suivantes :

. la valve de journal d’accès : org.apache.catalina.valves.AccessLogValve.

. la valve de filtre d’adresse distante: org.apache.catalina.valves.RemoteAddrValve.

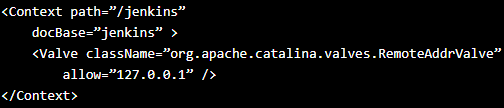
. la valve de filtre d’hôte distant: org.apache.catalina.valves.RemoteHostValve.

. la valve de dump: org.apache.catalina.valves.RequestDumperValve.

Nous allons utiliser la valve filtre d’adresse distante. Pour Jenkins créer un fichier context copiez le fichier context du Manager pour créer celui de Jenkins



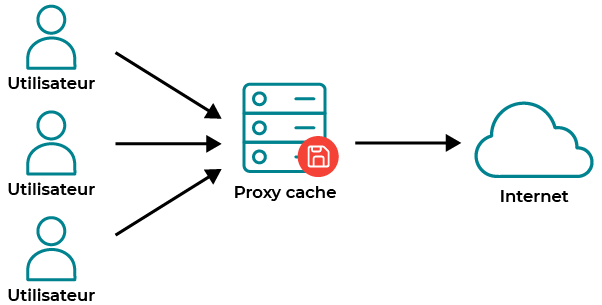
Editez ensuite la balise <Context /> du fichier jenkins.xml comme ceci :



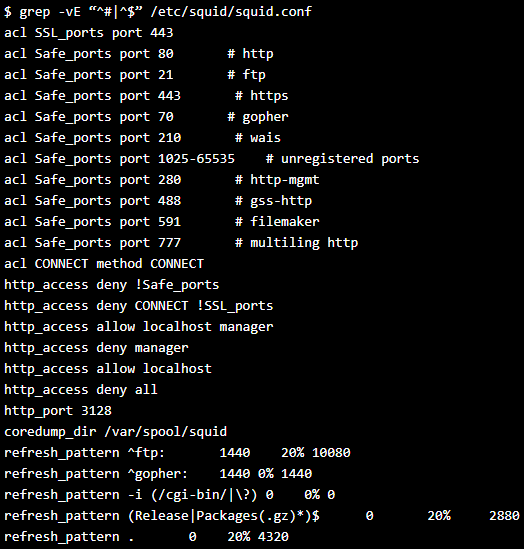
Redémarrer.

1. Proxy-cache avec Squid

Celui-ci se place sur le réseau client en intermédiaire avec des sites internet distants. Pour un accès plus rapide et un gain de bande passante au niveau de la connexion internet. Il peut autoriser l’accès ou interdire des sites web, ports/services etc.



La configuration se fait dans /etc/squid/squid.conf



http\_port indique l’adresse et le port sur lesquels écoute Squid (port 3128), on peut configurer plusieurs directives http\_port pour que Squid écoutes sur plusieurs adresse ou ports.

Coredump\_dir indique le répertoire dans lequel Squid peut écrire des fichiers core qui sont des fichiers d’erreur.

Refersh\_pattern précisent les règles qui établissent si un fichier est frais ou périmé (supprime en cache).

Directives importante acl (access control list contrôle d’accès qui seront utilisés par la directive) et http\_access (autoriser et interdire les connexions http en fonction de ces critères).

acl nom\_acl type(src source, dst destination, port,time) valeur (en fonction du type @reseau port)

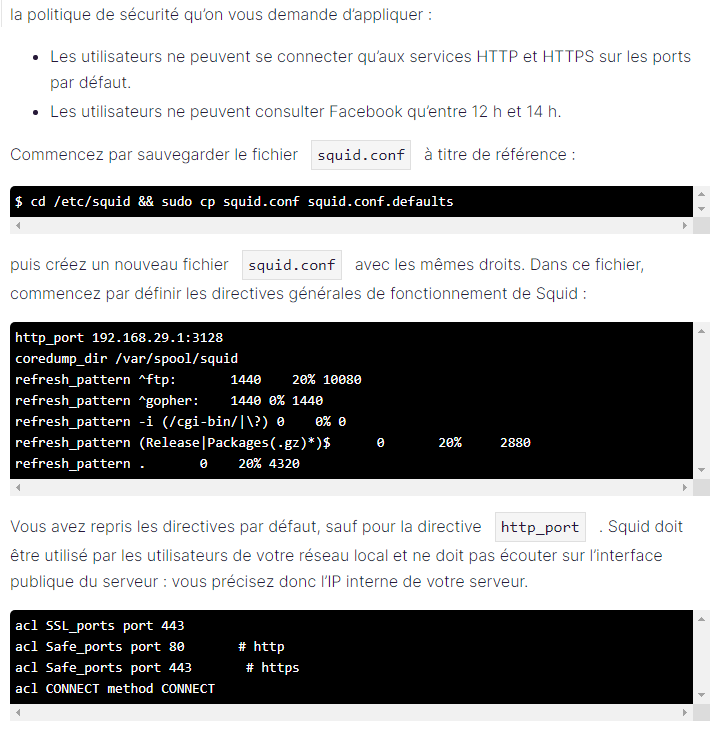
http\_access (allow, deny) nom de l’acl

http\_access deny !Safe\_ports #avccès interdit à tous les ports définis dans l’ACL Safe\_ports

http\_access deny all #pour interdire l’accès si aucune règle ne correspond)

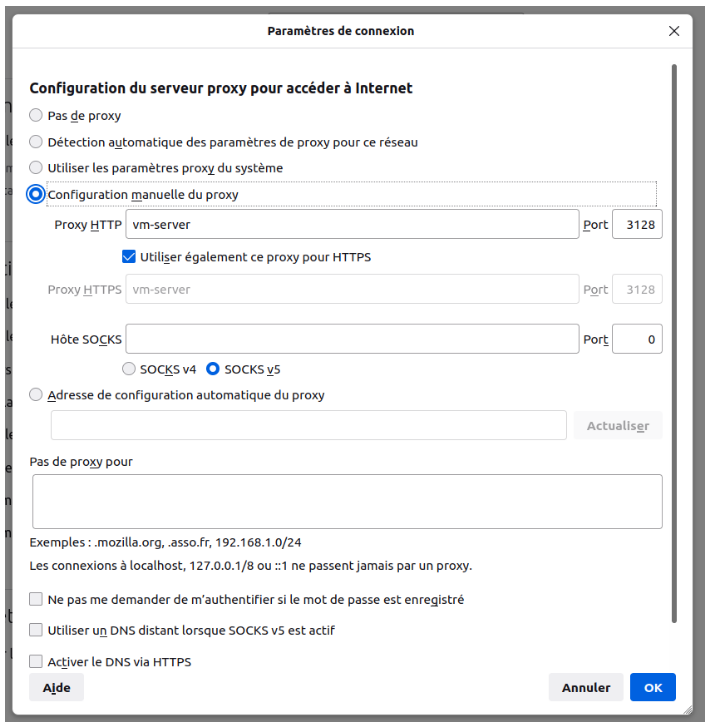
Squid fourni un cahe manager interface web accès avec l’outil squidclient, pour avoir un aperçu installez le paquet squidclient et lancez la commande $ squidclient mgr :info

Cas





Sur le poste client comme firefox



**VirtualBox**

VM : 10.0.2.15/24

Config Réseau : NAT, Accès pont, Réseau interne, Réseau privé hôte, generic driver, Réseau NAT, cloud Network, aucune connexion.

Mode NAT

La machine virtuabox hérite de ce mode de fonctionnement.

L’avantage est que la VM accède à Internet via la même connexion que l’hôte physique, sans pour autant obtenir une adresse IP sur votre réseau local. C’est le serveur DHCP de virtualbox qui va attribuer une adresse IP à votre machine virtuelle, et non le serveur DHCP de votre réseau local.

Inconvénient de ce mode, nous ne pouvons pas accéder aux services de votre VM (RDP, site web …) à partir de votre réseau local.

C’est le principe du NAT et virtualbox, au sein du réseau virtuel, va jouer un rôle de routeur pour que la VM accède au réseau local puis à internet. Néanmoins virtualbox intègre un assistant qui permet de créer une règle de redirection de port.

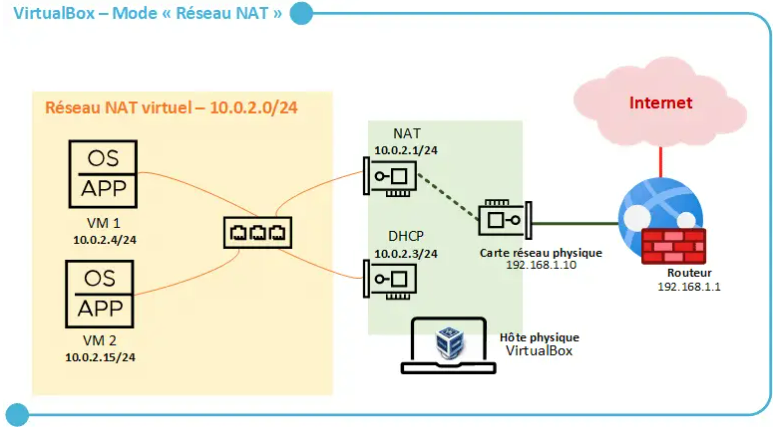
Pour le mode NAT la VM hérite de ip(10.0.2.15/24) tandis que virtualbox utilise 10.0.2.2.

Mode pratique pour connecter une seule VM à Internet sans exploiter le réseau local sur lequel est connecté l’hôte physique.

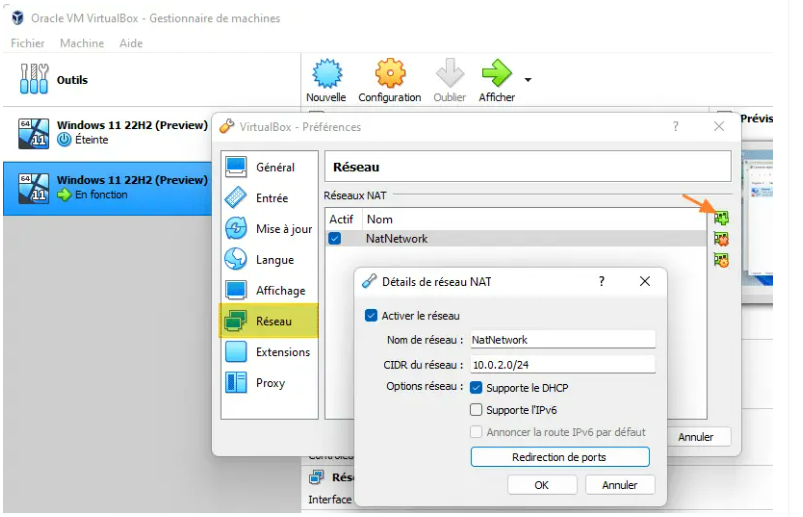
Pour profiter de plusieurs machines virtuelles, il est recommandé de créer un Réseau NAT.

**Réseau NAT**

L’avantage de créer plusieurs réseaux NAT :

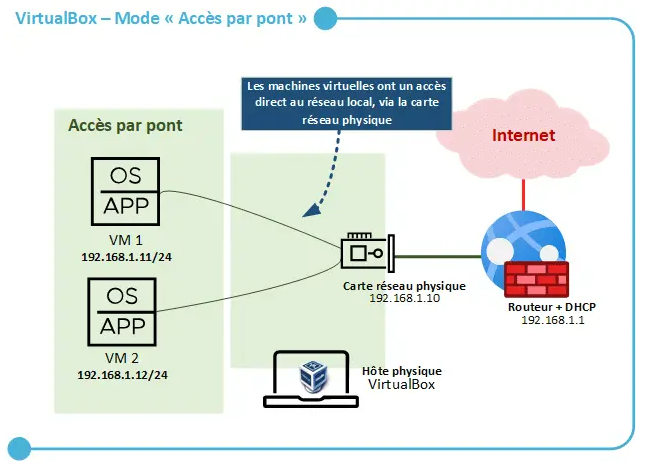


Configuration et ne pas oublier les redirections de ports avec les @ip obligatoires.



Accès par pont (Bridge)

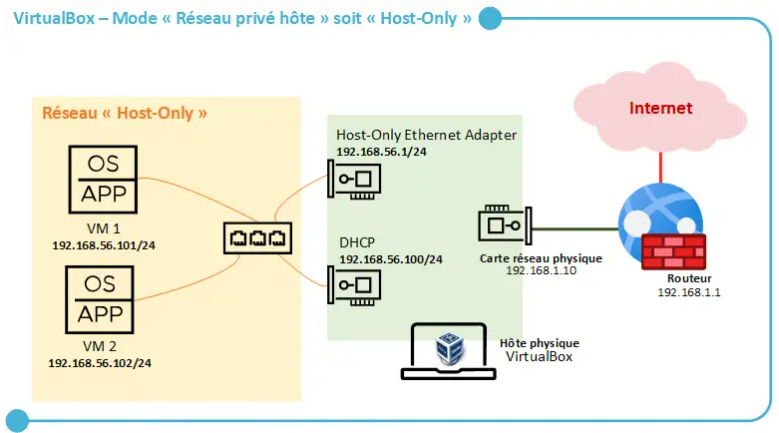
La machine virtuelle aura un accès à votre réseau au même titre que votre ordinateur physique. De ce fait si elle est configurée en DHCP elle va solliciter le serveur DHCP du réseau local pour l’@ip et pourra contacter les autres machines de votre réseau local et pourra être contactée par les autres machines de ce réseau contrairement au NAT. Il faudra sélectionner la carte réseau.



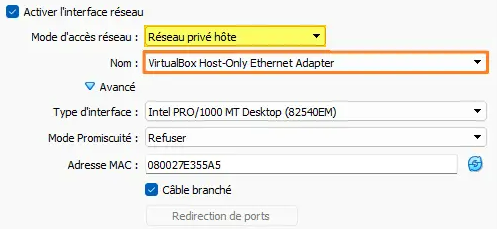
**Mode Host-Only**

Réseau privé hôte. La VM peut contacter l’hôte physique où est installé virtuabox et elle peut contacter également les autres machines virtuelles connectées sur ce même réseau Host-only.

Cependant la VM ne peut accéder à votre réseau local ni internet.



Configuration :

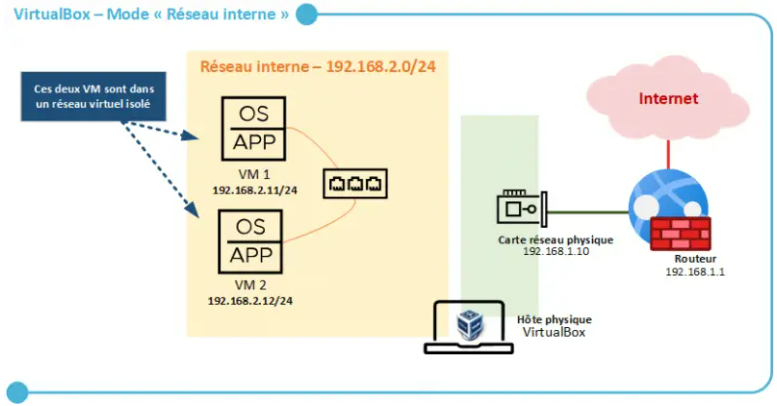


Créer des interfaces host-only supplémentaire Fichier/Gestionnaire de réseau hôte/Créer/oui

Une VM ne pourra pas communiquer avec une VM dans le secon réseau host-Only mais il sera possible de communiquer ave l’hôte physique VirtualBox

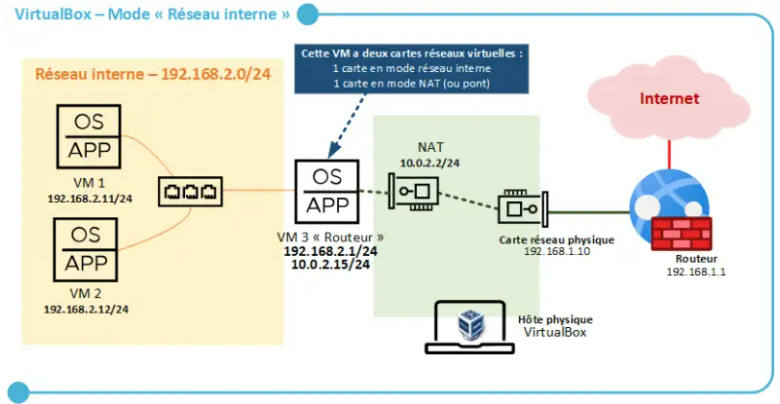
Réseau interne

Permet de créer une réseau virtuel isolé, les communications seront possibles uniquement entre les machines virtuelles connectées sur un même réseau interne mais ne peut pas communiquer avec l’hôte physique Virtualbox, ni le reste du réseau où est connecté cet hôte physique, ni internet.



Nous pouvons créer plusieurs réseaux internes en donnant des noms différents, l’avantage est de reproduire dans un lab puisque l’on positionne son propre routeur/pare-feu (VM3) pour permettre les communications vers l’extérieur de la même façon qu’on le fait avec un réseau réel.

Exemple la VM3 a une carte réseau configurée dans leréseau interne intnet ainsi qu’une carte réseau configurée en mode NAT afin de permettre aux machines du réseau interne d’accéder à internet. La VM3 peut être un pare-feu PfSense ou OPNSense mais aussi sous linux ou windows en activant les fonctions de routages.



**Cloud Network**

Il est possible d’intéragir avec Oracle cloud infrastructure (OCI) depuis VB.

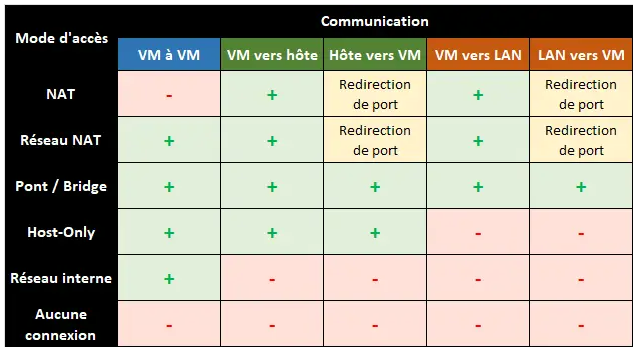
On peut créer une VM sur son environnement OCI (fonction expérimentale)

Generic driver

Spécifique rarement utilisé. On peut spécifier un pilote spécifique que l’on obtient par l’intermédiaire d’un pack d’extension selon deux modes Tunnel UDP, Réseau VDE (virtual distributed networking)

Mode aucune connexion

Pratique pour simuler une action de câble réseau débranché et oui comment faire avec une VM avec le statut câble réseau non connecté. Mais une autre alternative l’option coché câble branché.



**Proxmox**

CPU. 2 cœurs minimums recommandation 4 cœurs.

RAM. 2Go mais si l’on doit faire deux VM sous linux choisir 4Go.

Stockage. 128Go SSD pour le système et un second pour les ISO et VM.

Option Realm

* **PAM** est le module d'authentification enfichable utilisé dans les systèmes d'exploitation Linux/UNIX/BSD pour stocker les informations de l'utilisateur local. Il est stocké au niveau du système et délègue l'autorisation de se connecter à une machine. C'est le module par défaut sous Linux.
* **PVE** est une base de données stockée dans Proxmox qui stocke des informations sur les utilisateurs pouvant se connecter à l'interface Web de Proxmox. Elle n'accorde pas d'autorisation pour des choses comme la connexion SSH ou Shell au système d'exploitation sous-jacent, au lieu de cela, il délègue uniquement l'autorisation de se connecter aux interfaces Proxmox, comme la WebGUI ou l'API.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

-------------------------------------------------------------------------------------

https://www.youtube.com/watch?v=atcIeViaiZk

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*INSTALLER PROXMOX\* \*INSTALLER DOCKER\* \*INSTALLER DES CONTAINER SUR MACHINE VIRTUELLE\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Proxmox n'est disponible que sur Debian.

Donc il faut installer une machine virtuelle sur ubuntu

pour installer proxmox sur cette VM ou avec qme à voir.

1\*\*Pour installer promox, nous installons un manager de machine virtuelle.

sudo apt install virt-manager

redemarrer sinon erreur unable to connect to libvirt qemu ///system

2\*\*Sur ubuntu installer une machine VM debian

http://172.16.0.254:8080 #si proxy

Sur vda VM [Debian11]

erreur sudo fichier not found sudoers

#ajouter l'utilisateur dans le groupe sudo

su -

adduser <utilisateur> sudo

-----\*Depuis Ubuntu installer proxmox\*--------------------------------

sudo apt install virt-manager

Télécharger et installer proxmox taper l'os debian et non automatique.

root@pve:~# less /proc/version

nous pouvons nous connecter à proxmox

https://192.168.122.191:8006

Nous avons notre machine virtuelle sur debian avec proxmox

[acces: bein merde j'ai oublié le mot de passe !!!!!!!!!!!!]

https://pve.proxmox.com/wiki/Root\_Password\_Reset

https://www.youtube.com/watch?v=4s22pqfgu1c

ouvrir une console avec kvm

au moment de grub press e

un encadré s'ouvre et en bas à la suite de Quiet init=/bin/bash

boot ctrl X

root@:/# zpool status #ZFS modules running /sbin/modprobe zfs

root@:/# mount -rw -o remount /

root@:/# df -h #affichie les partitions disques

root@:/# passwd root

New password: root ...

reboot reset la vm

Nous pouvons nous reconnecter en https://192.168.122.192:9443 choix linux et pas proxmox