Documentation projet INFRA SI B1

PROJET INFRA & SI

Les bonnes pratiques :

Il y a plusieurs bonnes pratiques à mettre en œuvre afin d'optimiser la gestion et la sécurité de votre réseau :

- Niveau 1 :

  - **Le premier niveau est celui qui correspondra au minimum de moyens que vous pouvez honnêtement opposer à une mise en accusation pour « négligence caractérisée ». Attention, ceci n'est pas une information officielle, mais un conseil issu d'une expertise technique et objective. Les moyens préconisés par l'Hadopi comme l'utilisation d'outils de journalisation de vos connexions ne sont pas des moyens obligatoires et leur utilisation peut vous obliger à renoncer à une certaine liberté et vie privée.**

- Changer le mot de passe de votre box. Par défaut, toutes les box ont le même mot de passe et il faut 10 secondes pour le retrouver sur internet. Si vous ne le changez pas, le pirate pourra accéder à la configuration de votre box.

- Protéger votre réseau Wi-Fi avec une clé WPA ou WPA2 et un mot de passe fort (composé de 6 lettres majuscules et minuscules mêlées, 2 chiffres et au moins un symbole de ponctuation). Par exemple : *jean6?5DigU est un mot de passe fort, il ne peut pas être trouvé dans un dictionnaire et ne correspond à rien qui vous concerne.

- Si les circonstances vous obligent à créer un réseau Wi-Fi en mode WEP (un réseau AdHoc temporaire par exemple), n'utilisez jamais un mot de passe que vous utilisez pour autre chose, si quelqu'un le découvre il pensera aussitôt à l'utiliser sur votre messagerie ou autres.

Documentation projet INFRA SI B1

- Niveau 2 :

  - **Le second niveau correspond à un mélange de moyens de sécurisation du réseau et de pratiques de vigilance. Il faudra aussi mettre en place les moyens de sécurisation de l'ordinateur, ainsi que ceux du niveau 1.**

    - Paramétrer votre pare-feu pour interdire tous les accès
      entrants, quels qu'ils soient.

    - Consulter le journal de votre box régulièrement afin de vérifier qu'aucune machine inconnue ne s'est connectée (ceci peut ne pas être suffisant car les hackers s'arrangent parfois pour ne pas utiliser le serveur DHCP, qui n'est pas obligatoire).

    - Utiliser le mode routeur de votre box.

    - Mettre en place une règle translation d'adresses IP (NAT).

    - Interdire l'utilisation du port-forwarding (PAT).

    - Interdire l'utilisation de UPnP.

Documentation projet INFRA SI B1

- Niveau 3 :

  - **Le dernier niveau est indissociable d'un grand nombre de paramétrages et de contrôles fréquents sur votre box comme sur votre ordinateur. Pour une sécurité maximale, vous ne devez négliger ni l'un ni l'autre.**

    - Utiliser le filtrage par adresses MAC dans le pare-feu, ce qui vous obligera à saisir vous-même les adresses MAC des ordinateurs que vous autorisez, y compris vos amis de passage. Vous devrez supprimer les entrées crées une fois qu'elles ne seront plus nécessaires.

    - Interdire l'utilisation du protocole ICMP pour empêcher la découverte de votre box depuis internet ainsi que des ports ouverts.

- Désactiver l'administration à distance de votre box.

- Contrôler régulièrement les journaux de sécurité et d'association de votre box (si disponibles) afin de contrôler qu'une machine inconnue ne s'est pas connectée, ou, plus simple, utilisez Achiwa.

Voici les bonnes pratiques issues d'une expertise technique et objective à mettre en œuvre pour protéger votre réseau.

Maintenant nous allons voir certaine bonne pratique pour optimiser le réseau de votre entreprise.

Documentation projet INFRA SI B1

- Configurer les IP de vos machines en respectant le plan d'adressage établie.

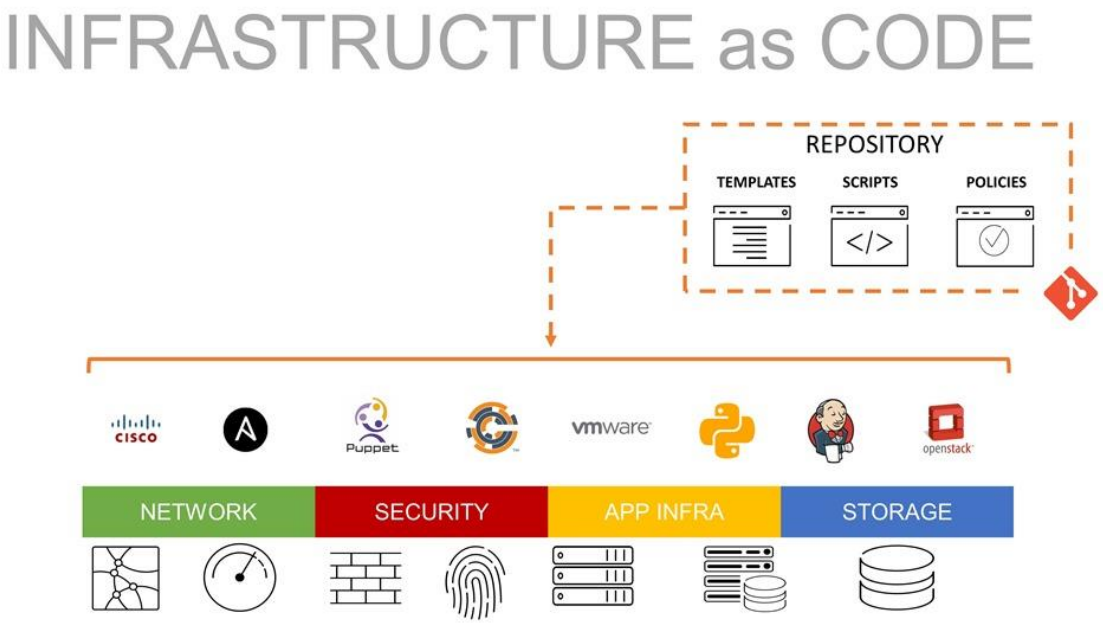
- Nommer toutes vos machines afin de pouvoir vous organiser et agir sur les machines plus rapidement.

- **ATTENTION !!!** Ne laisser aucune personne, extérieur a l'entreprise ou à la gestion/maintenance de votre réseau brancher ou connecter des appareils

- **ATTENTION !!!** Ne surtout pas relier vos serveurs de BackUp/hébergeur à internet. Vos serveurs doivent être accessible uniquement en local et pars des personnes agrées à la maintenance de serveur

Configuration

La configuration d'un logiciel, d'un matériel, ou d'un réseau informatique est un ensemble de caractéristiques techniques qui ne dépendent pas du constructeur mais découlent des choix de l'acheteur et de l'utilisateur, nous verrons par la suite la configuration d'un systèmes, d'un réseau et des services.

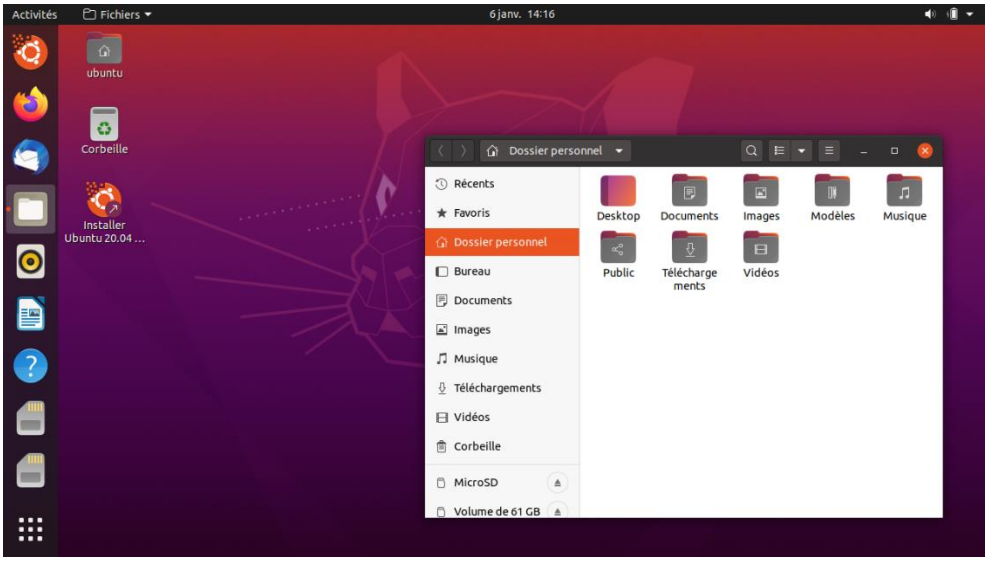


Configuration du système :

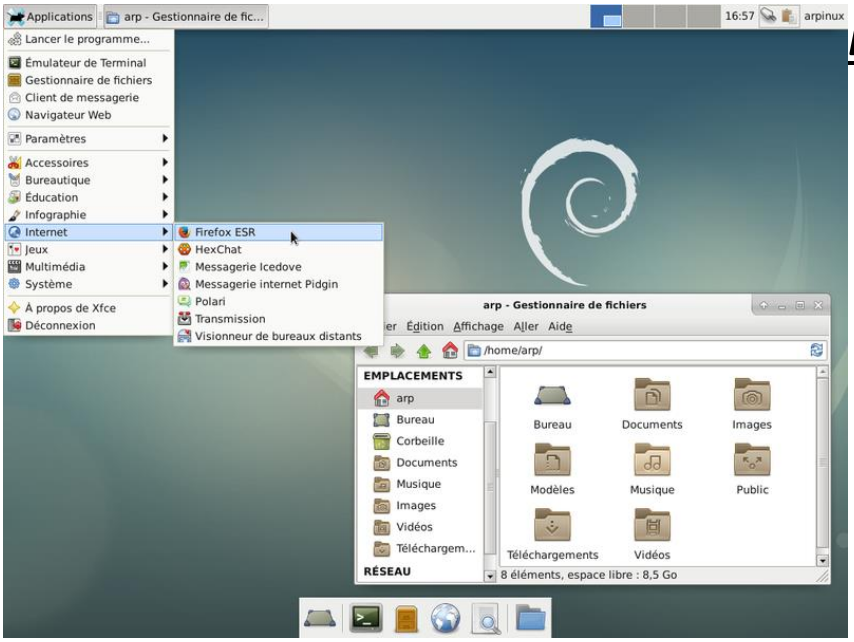
Documentation projet INFRA SI B1

La configuration du système est un outil permettant d'identifier les problèmes susceptible d'empêcher Windows et Linux de démarrer correctement. Nous pouvons utiliser pour cela Ubuntu, Debian ou CentOS.

- Ubuntu, qui est un système d'exploitation Linux basé sur la distribution Debian. Il est libre, gratuit, et simple d'utilisation. Comme pour n'importe quel logiciel et système d'exploitation, Ubuntu et ses variantes nécessitent des systèmes performants, répondant aux exigences minimales ci-dessous, afin de proposer une expérience d'utilisation agréable.



- Debian est un système d'exploitation Linux composée exclusivement de logiciels libres, développé par le Debian Project, Debian est aussi très largement utilisée par les développeurs de logiciels et de matériels parce qu'elle fonctionne sur de nombreux périphériques et architectures, et elle fournit un système de suivi de bogues public ainsi que d'autres outils pour les développeurs.



B1

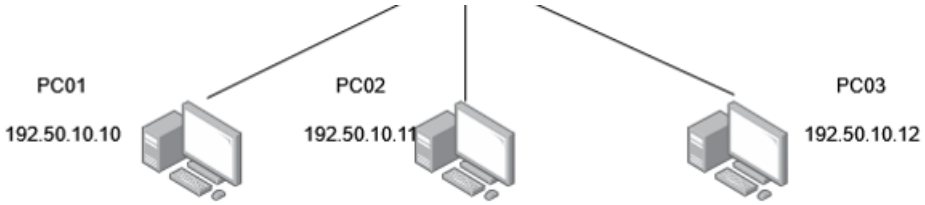
- CentOS est une distribution GNU/Linux destinée aux serveurs. À l'instar de son modèle RHEL, CentOS est une plateforme Entreprise principalement adaptée aux entreprises et aux grandes organisations. En principe, la distribution Linux peut aussi être utilisée pour un usage domestique, bien que ce ne soit pas le but des développeurs.

Configuration d'un réseau :

La configuration réseau est l'ensemble des caractéristiques d'un réseau donné.

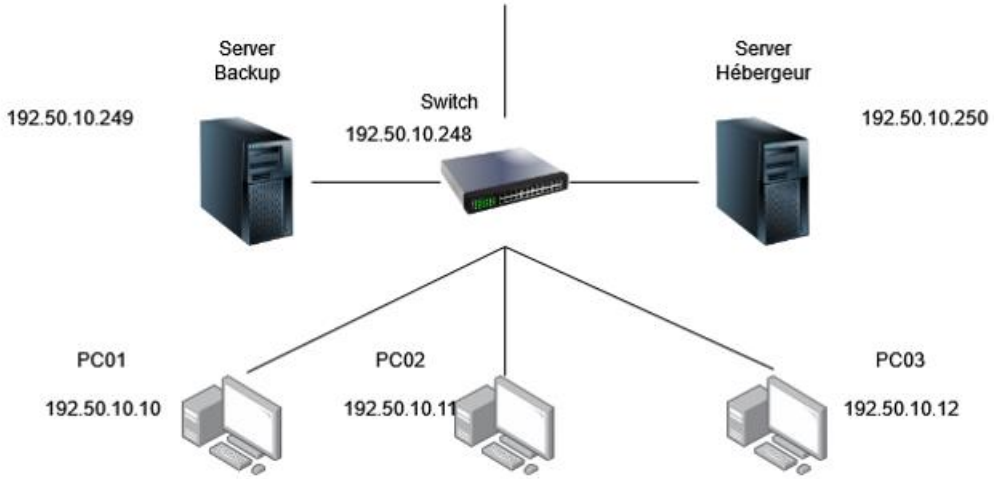
Documentation projet INFRA SI B1

- Nous prenons d'abord plusieurs PC qui vont nous permettre de nous connecter à notre réseau, ils ont chacun une adresse IP

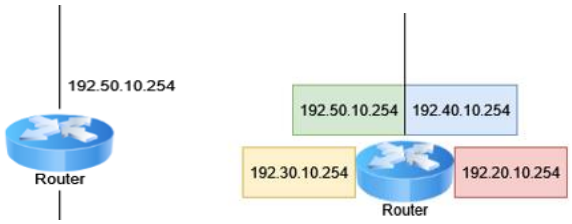


- Ces PC sont connecté sur un switch possédant son adresse IP

- Ensuite nous avons le serveur d'hébergeur et le serveur backup qui serons aussi relié au même switch que les pc pour la communication entre eux avec leur propre adresse IP

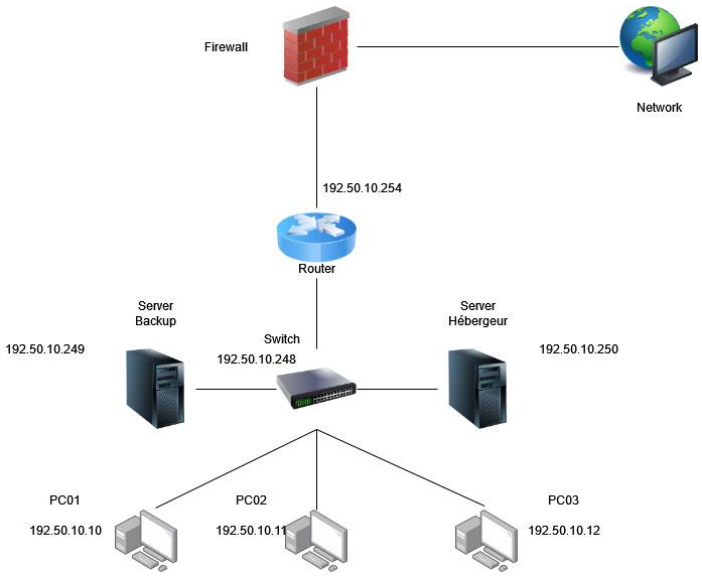


- Puis nous avons le routeur qui permet à un ou plusieurs switch de passer sur internet, il possède son adresse IP et peut aussi traiter des serveurs et utilisateurs qui n'ont pas le même numéro VLAN

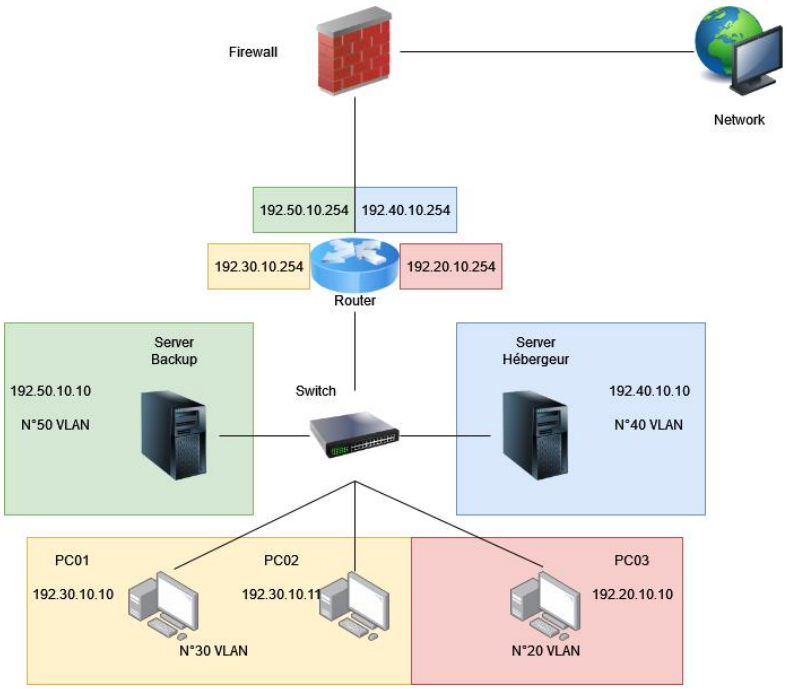


Documentation projet INFRA SI B1

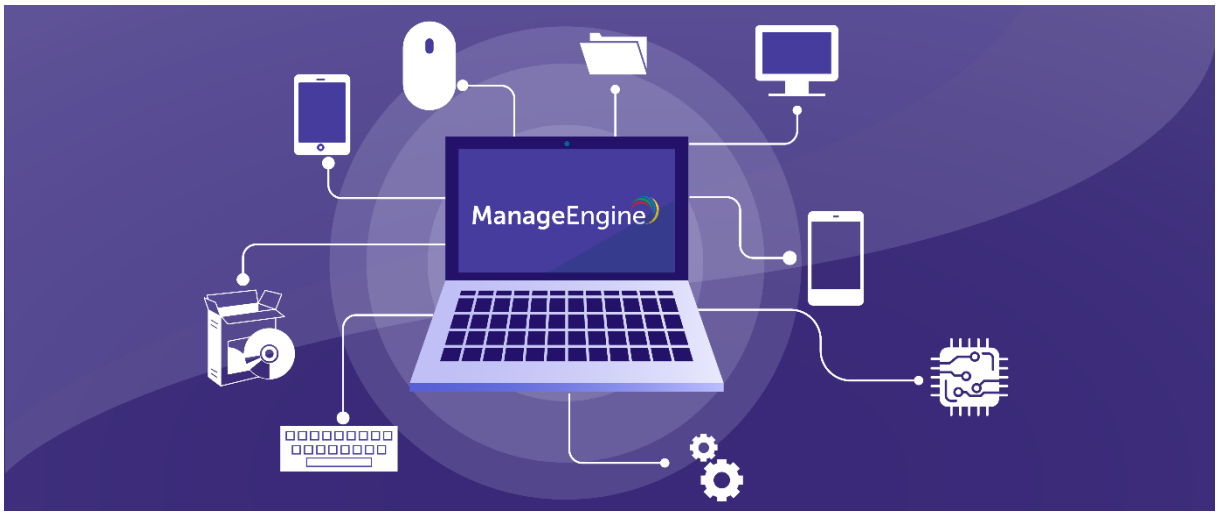
- Enfin le routeur va passer par un pare-feu pour respecter la sécurité d'un réseau et les données privées pour enfin se connecter à internet



Nous pouvons aussi traiter le cas ou les PC et les serveurs n'ont pas le même numéro VLAN, dans ce cas le routeur aura des adresses IP qui ne sont pas propre à lui mais qui le redirigera vers les différents numéro VLAN



Configuration des services :



Les services de Linux offriront diverses fonctionnalités à vos utilisateurs et aux autres machines de votre réseau. Avant toute chose, essayons de préciser ce que sont exactement ces services. Pour rappel, sous Linux, chaque programme qui s'exécute prend la forme d'un processus. Vous pouvez utiliser la commande ps pour voir les processus qui tournent sur votre système. L'option -o précise les champs que vous souhaitez voir apparaître

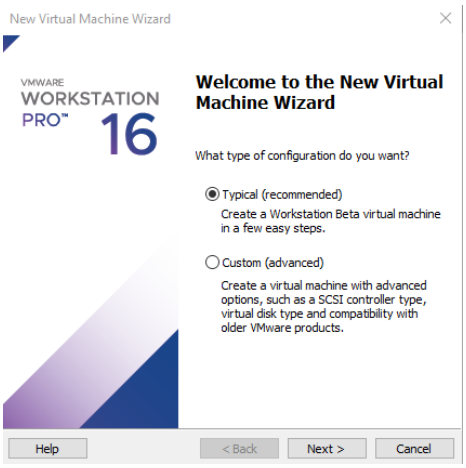
- **Exigences générales :**
  Pour les déploiements initiaux de Linux, ainsi que pour les mises à niveau, veuillez laisser suffisamment d'espace disque disponible pour la distribution des fichiers d'installation de Linux. Pour installer Linux, il suffit de démarrer votre ordinateur avec le DVD d'installation dans le lecteur ou en téléchargeant VM Ware. Le programme se lance automatiquement et il vous suffira de vous laisser guider par les différents écrans, tout comme le feriez pour une installation Windows.
- **Comment l'installer :**

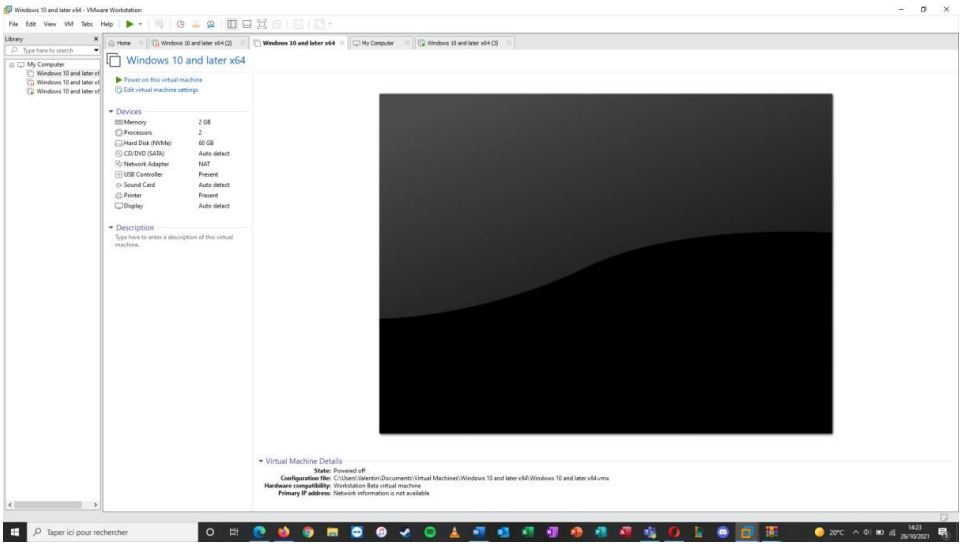
  Tout d'abord un outil de virtualisation (nous utiliserons Vmware) :

  vmware

Documentation projet INFRA SI B1

Après être entré dans l'application on va aller dans file en haut, puis dans new virtual machin, ou CTRLN + N,

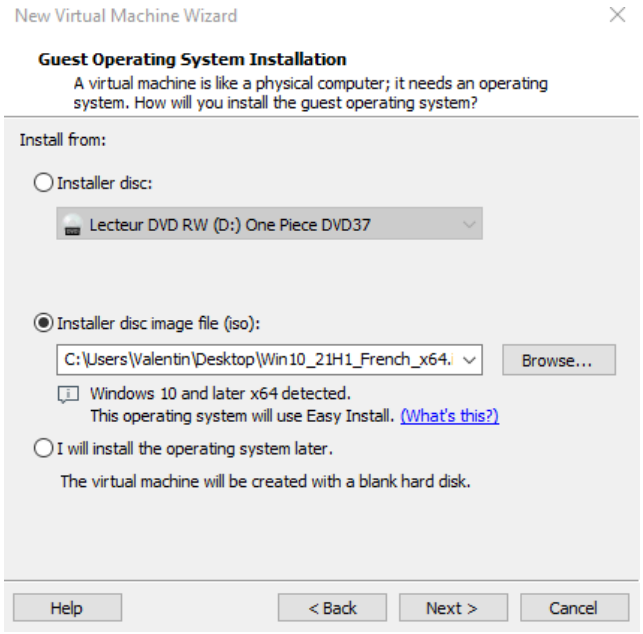




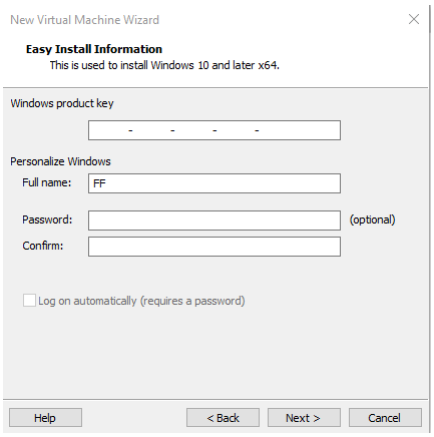
Ensuite on coche la case typical qui est recommandé pour créer une version workstation beta de notre machine virtuelle, appuyer sur next.

Documentation projet INFRA SI B1

Vous cochez ensuite la cochez la case installer disc image pour pouvoir créer le fichier, appuyer sur next.

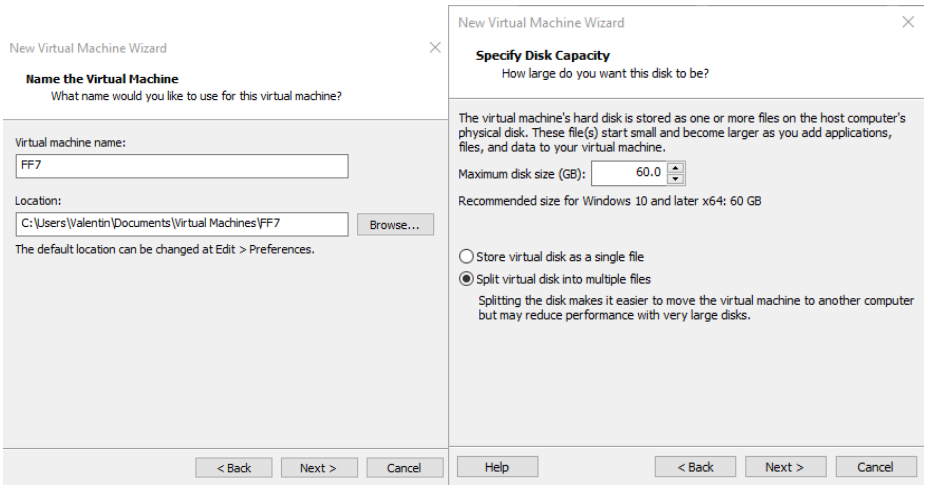


Après, dans la page suivante nous pouvons créer une clé (mais c'est payant donc on ne le fera pas) donner un nom à votre dossier et si vous le désirez, un mot de passe, appuyer sur next quand cela sera fait.

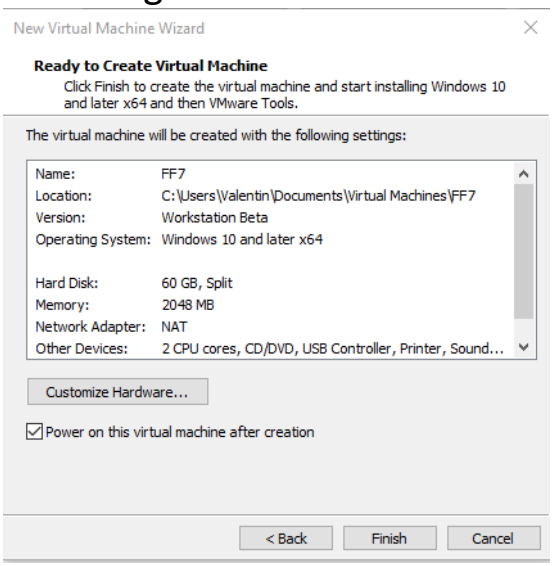


Puis le nom de votre machine ainsi que sa taille maximale, appuyer sur next.

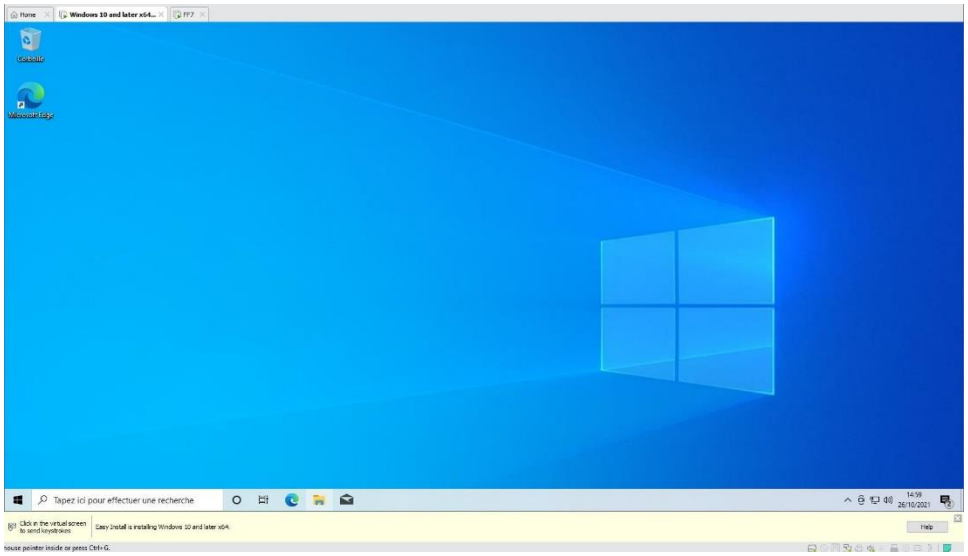
Documentation projet INFRA SI B1



Enfin validez vos options en appuyant sur finish et attendez la fin du téléchargement



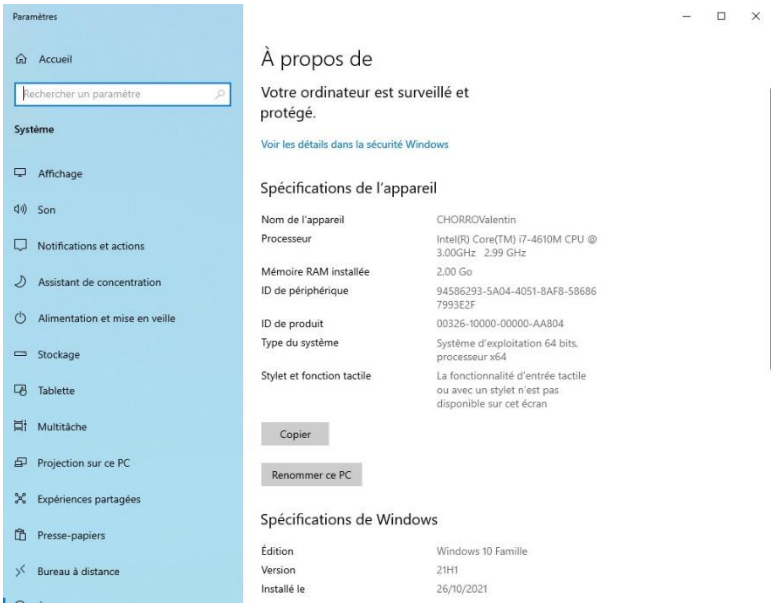
Vous devez normalement arriver sur cette page :

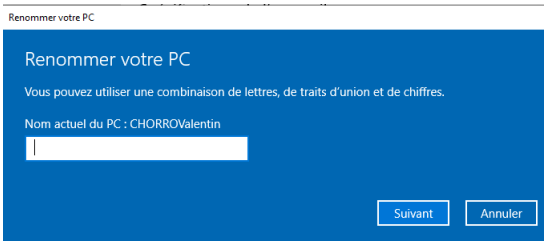


Documentation projet INFRA SI B1

Il faut maintenant le renommer : aller dans la barre de recherche en bas à droite et taper pc,

Appuyer sur propriété

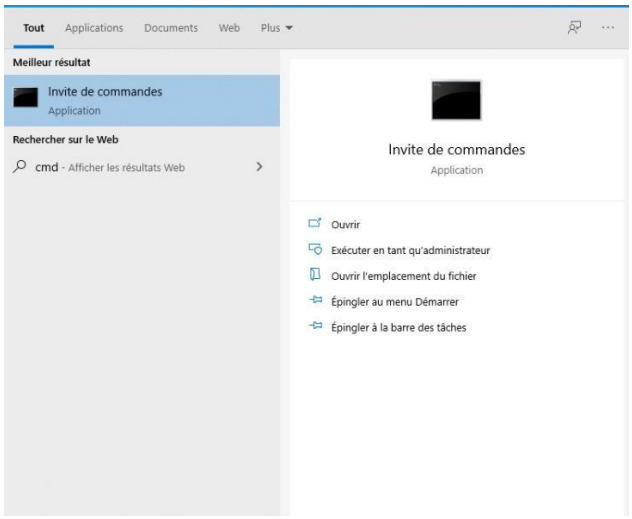


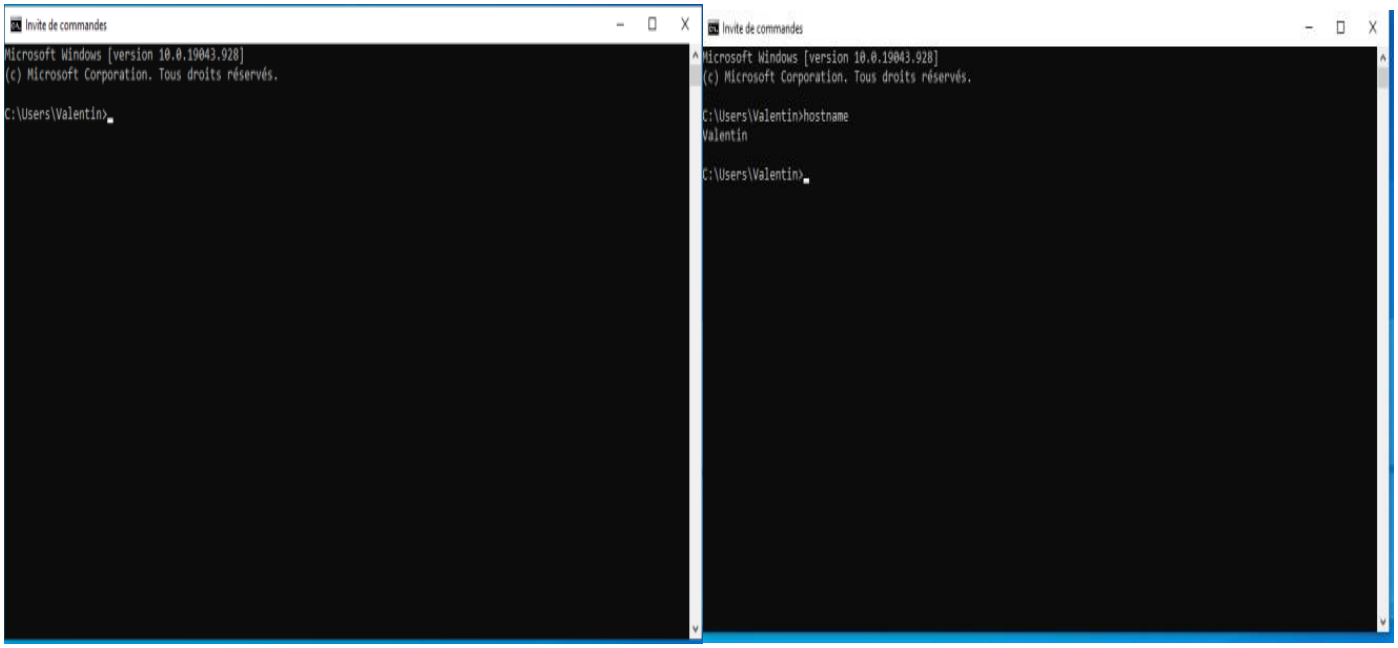


Documentation projet INFRA SI B1

Aller dans renommer ce PC, puis renommer le comme vous le voulez

Vous devrez ensuit le redémarrer, reveiner dans la barre de recherche puis taper cmd et allez dans invite de commande





Vous arrivez sur cette page et taper hostname pour pouvoir afficher le nom de votre dossier.

Documentation projet INFRA SI B1

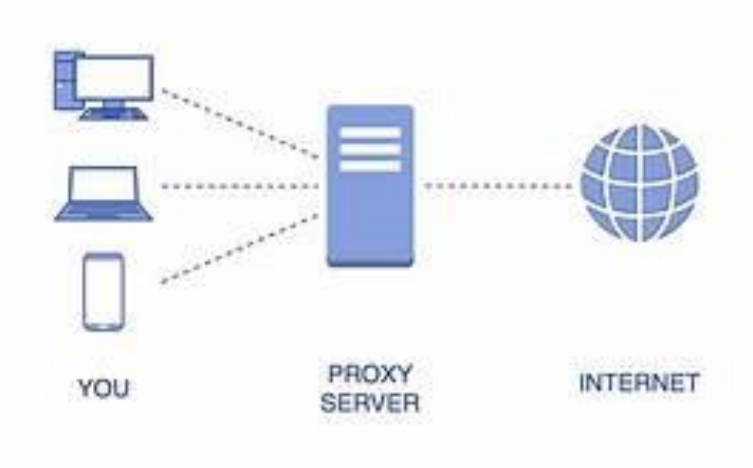
Vous voici enfin arrivé à la partie documentation d'exploitation, ici nous allons traiter des services mis en place et les outils permettant la création de votre serveur web « Ngnix ».

NGINX

Depuis le début de la documentation vous aurez pu constater de voir apparaître plusieurs fois le mot « Nginx », sans pour autant comprendre ce que là cela signifier. Et bien tout d'abord Nginx est un serveur web open source, donc un logiciel est libre de droit, qui utilise le protocole http, ainsi qu'un proxy inversé.

Mais qu'est-ce qu'un proxy inversé ?

Proxy inversé et tout d'abord un proxy, vous ne le savez peut-être pas mais quand vous vous connectez à internet, via un moteur de recherche tel que Google, et bien Google vous prête un proxy pour vous connecter à internet, voici la schématisation de cette infrastructure, qui est votre PC, le proxy, puis internet.

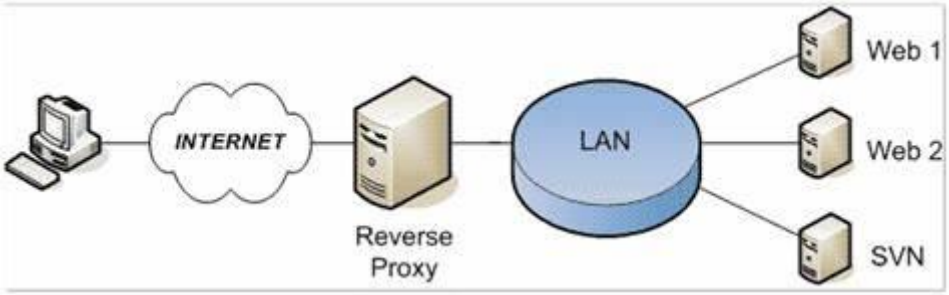


En somme comme nous pouvons le constater, un proxy est un dispositif, un outil informatique servant d'intermédiaire entre les ordinateurs d'un réseau privé et internet, il fait notamment office de pare-feu et de cache, pour vous protéger de tout type de malware, dans la mesure du possible bien évidemment.

Documentation projet INFRA SI B1

Mais alors quelle est la différence entre un proxy lambda et un proxy inversé. Un proxy inverse fait apparaître différents serveurs et services comme s'ils étaient une seule unité. Il vous permet de masquer la présence de plusieurs serveurs distincts derrière le même nom.

Pour rappel dans un réseau informatique, un proxy inverse de base sert d'intermédiaire entre un groupe de serveurs et les clients qui souhaitent les utiliser. Un client est un matériel ou un logiciel qui peut envoyer des demandes à un serveur. Le proxy inverse envoie toutes les demandes des clients aux serveurs et envoie également toutes les réponses et services des serveurs aux clients. Du point de vue du client, tout semble venir d'un même endroit.



Maintenant que vous avez compris ce qu'est un proxy, et qu'est-ce qu'apporte vraiment le reverse-proxy, fourni avec Nginx (attention un reverse-proxy est aussi fourni avec Apache, mais il est quand même important de le souligner, car il peut être intéressant de le mettre en place dans votre infrastructure).

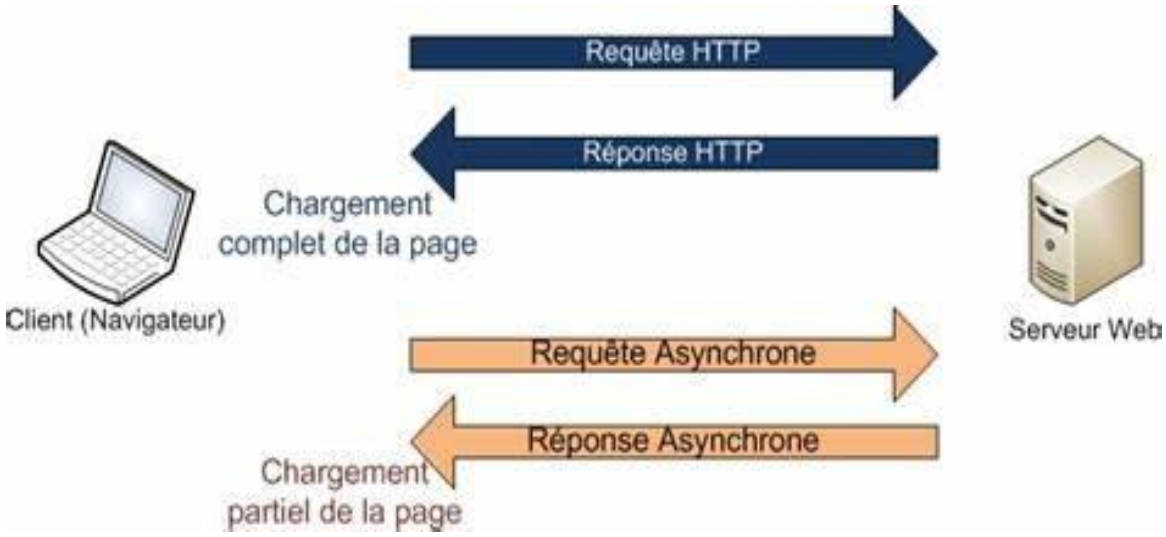
Pour votre culture, comme tout logiciel Ngnix, a été développé par un groupe, une entreprise ou bien une personne, ici c'est une personne Ngnix a été écrit par Igor Sysoev, dont le développement a débuté en 2002 pour les besoins d'un site russe à très fort trafic.

Fonctionnalités :

Documentation projet INFRA SI B1

Serveur asynchrone

Nginx est un serveur asynchrone par opposition aux serveurs synchrones où chaque requête est traitée par un processus dédié. Au lieu d'exploiter une architecture parallèle et un multiplexage temporel des tâches par le système d'exploitation, Nginx utilise les changements d'état pour gérer plusieurs connexions en même temps, le traitement de chaque requête est découpé en de nombreuses mini-tâches et permet ainsi de réaliser un multiplexage efficace entre les connexions. Afin de tirer parti des ordinateurs multiprocesseurs, plusieurs processus peuvent être démarrés. Ce choix d'architecture se traduit par des performances très élevées, mais également par une charge et une consommation de mémoire particulièrement faibles comparativement aux serveurs HTTP classiques, tels qu'Apache ou bien Ajax.



Modularité

Nginx est très modulaire : un noyau minimal et des modules, nombreux, venant compléter les fonctions de base. Chaque module peut agir comme un filtre sur le contenu en entrée, en sortie ou intermédiaire (proxy) par le biais de nombreuses callbacks. Ainsi, à titre d'exemple, un contenu

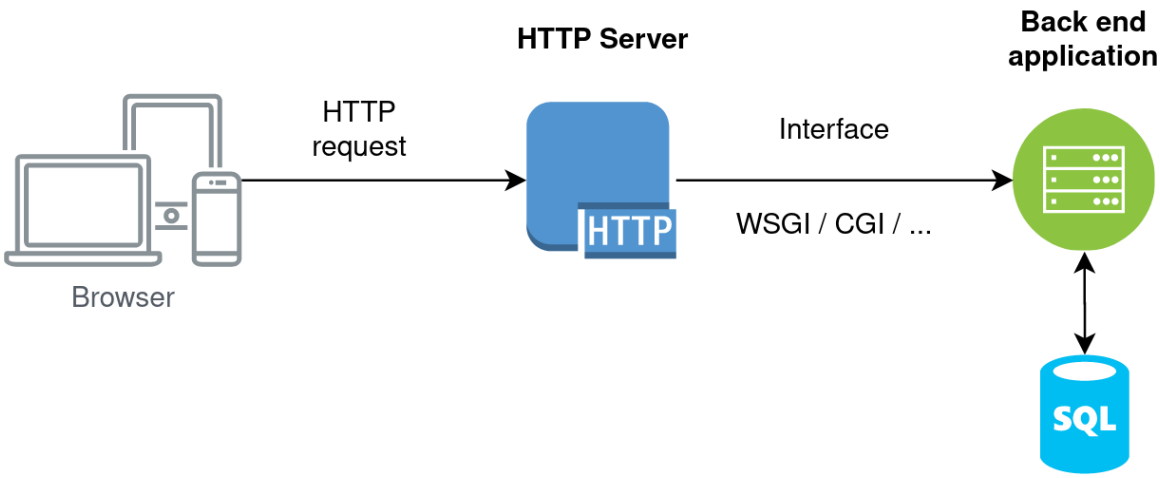
dynamique peut être compressé à la volée par le module « gzip » avant envoi.

Optimisations

Le noyau s'appuie sur des structures de données minimales, mais optimales, visant à réduire le nombre d'appels système, en particulier pour tout ce qui a trait à l'allocation de mémoire. Différents mécanismes de signalisation peuvent être utilisés afin d'exploiter au mieux le système d'exploitation (par exemple : epoll sous Linux et kqueue sous BSD). L'architecture asynchrone soulage l'ordonnanceur du système d'exploitation et favorise l'utilisation des caches du ou des processeurs.

Utilisations

Outre le fait d'être un serveur HTTP, Nginx peut être configuré pour être un proxy inverse Web et un serveur proxy de messagerie électronique (IMAP / POP3). L'utilisation la plus fréquente de Nginx est de le configurer comme un serveur Web classique pour servir des fichiers statiques et comme un proxy pour les requêtes dynamiques typiquement acheminées en utilisant une interface FastCGI vers un ou des serveurs applicatifs avec un mécanisme de répartition de charge.



Pour la documentation des commandes pour la création de votre serveur et la mise en ligne, de ce dernier un onglet spécial sur le nôtre site est mise a disposition, rendez-vous sur la page principale et descendez jusqu'en bas jusqu'à voir la « MISE EN PLACE D'UN

Documentation projet INFRA SI B1

SERVER NGINX », vous n'aurez qu'a cliquer sur le bouton « En savoir plus -> », pour obtenir les informations nécessaires à la création de votre server web.

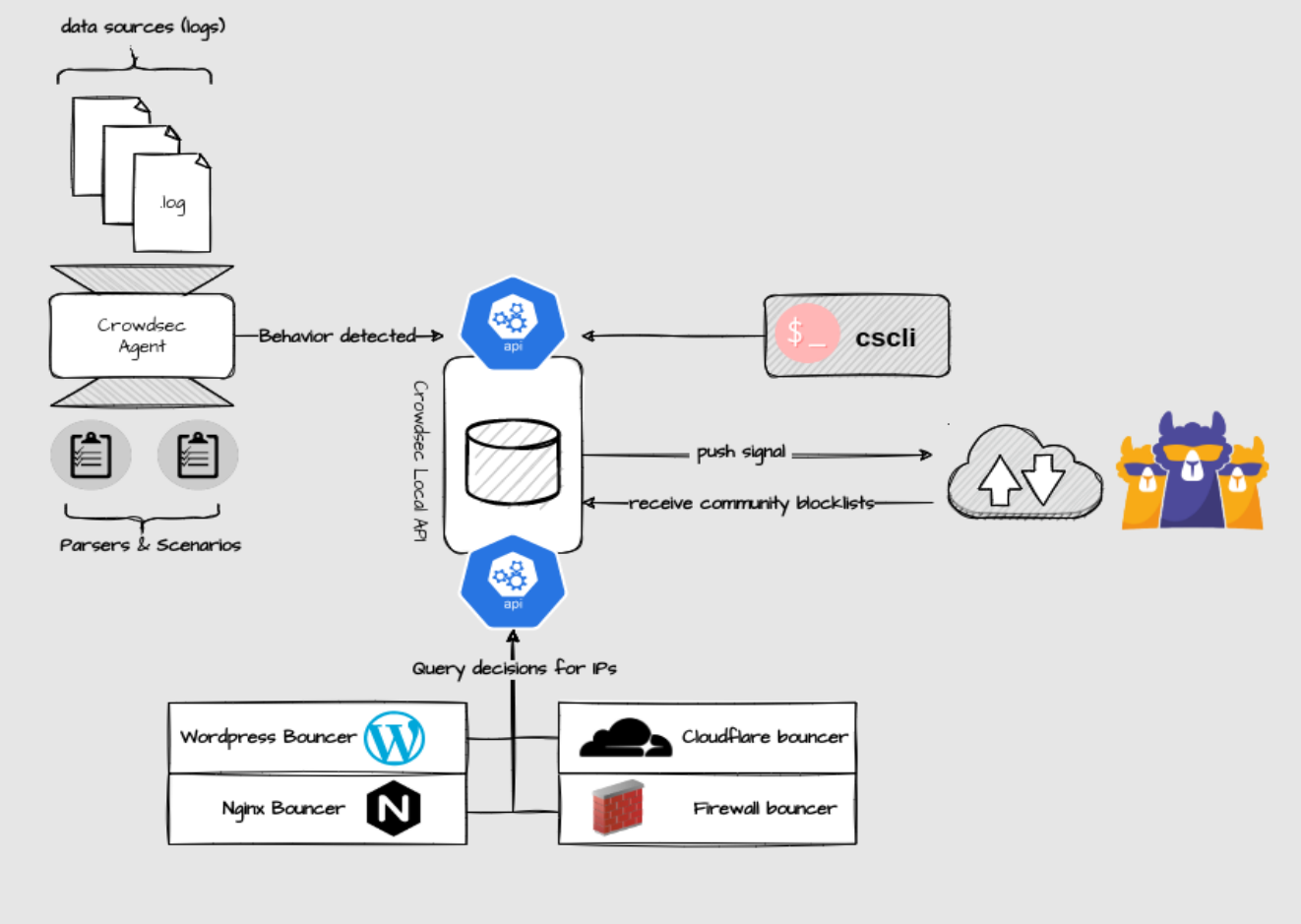
CROWDSEC

Maintenant que la partie la plus importante qui était le serveur web, et compris nous allons pouvoir rentrer dans la protection de votre héberger Web, pour cela vous pouvez utiliser un firewall, autrement dit un pare feu, nous avons vu l'exemple d'un pare-feu avec un proxy juste avant, mais il faut savoir que toute machine c'est à dire ordinateur, possède de bases un pare-feu. Personnellement je suis sur Windows et je possède

Windows Defender, qui est mon pare-feu par défaut qui me protège de tout virus reconnu comme malveillant, par Windows Defender, ma avertissant avec une notification ou en supprimant directement le malware.

Donc un pare-feu permet donc de protéger votre ordinateur mais aussi votre réseau local. en l'occurrence nous cette fois-ci nous souhaitons protéger notre réseau, toutes nos machines liées à notre réseau. Pour ce faire nous allons installer une défense, un firewall il y a plusieurs firewall qui peuvent être installés facilement, comme par exemple le fameux Pfsense, mais pour nous ce sera plutôt CrowdSec, étant facile d'installation et totalement open source et totalement gratuit, vous obtiendrez un accès à une interface qui vous donnera l'état de votre serveur en temps réel, permettant de le contrôler ou plutôt de le surveiller à distance, en cas de cyberattaque.

Documentation projet INFRA SI B1



RSYNC ET SSH

Une fois avoir parlé du firewall notre protection, notre mur qui nous protège des personnes malveillantes, nous allons préparer et voir, comment et avec quel outil faire un serveur de backup, car nous pouvons ne pas penser au risque d'une potentielle cyberattaque, mais aussi des bugs de corruption. Qui pourrait par mésaventure nous faire perdre notre hébergeur web étant actuellement notre VM Linux, pour se prévenir de tout ça nous allons créer un serveur de backup sur une autre VM cette fois-ci, qui nous permettra de restaurer une ancienne version de notre VM datant au plus tard pour nous donne-moi une journée.

Documentation projet INFRA SI B1

Pour ce faire nous allons utiliser l'outil est :
rsync (pour **r**emote **sync**hronization ou synchronisation à distance), est un logiciel [1)] de synchronisation de fichiers. Il est fréquemment utilisé pour mettre en place des systèmes de sauvegarde distante ou des points de restauration du système (via l'interface Timeshift).

rsync travaille de manière unidirectionnelle c'est-à-dire qu'il synchronise, copie ou actualise les données d'une source (locale ou distante) vers une destination (locale ou distante) en ne transférant que les octets des fichiers qui ont été modifiés.

Dans la documentation nous voyons le côté pratique mais nous on les commande pour la mise en œuvre de ce serveur backup, Pour ce faire comme tout à l'heure notre site met à disposition la possibilité d'obtenir une vraie documentation guider avec toutes les commandes pour la mise en place en bonne et due forme, de votre serveur backup.

Pour revenir sur la back up il vous sera nécessaire de vous munir d'un protocole, le protocole SSH pour Protocole Secure Shell

SSH signifie "*Secure Shell*", il s'agit donc d'un "*shell"* dit "*sécurisé*". Pour rappel, un shell, que l'on peut également appeler communément "terminal", est la méthode la plus courante de gestion des serveurs Linux.
Un shell va permettre de dialoguer avec une machine ou un serveur via l'exécution de différentes commandes qui retourneront des informations. Le protocole SSH a été conçu avec

Documentation projet INFRA SI B1

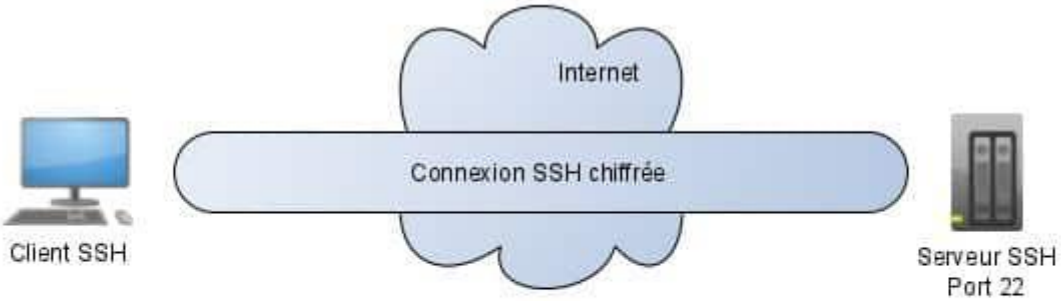
l'objectif de remplacer les différents protocoles non chiffrés comme rlogin, telnet, rcp et rsh.

La sécurité joue toujours un rôle majeur sur Internet : c'est pourquoi le protocole de sécurité SSH est fermement intégré dans la pile de protocoles TCP/IP. Le protocole SSH permet aux utilisateurs d'établir une connexion sécurisée entre deux ordinateurs.

SSH est donc un protocole de communication qui vise à rendre la communication sûre.
Généralement, un administrateur l'utilise pour prendre la main sur une machine distante.

L'établissement de la connexion SSH se fait avec le processus suivant :

- Un client SSH se connecte à serveur SSH installé sur une machine distante. Par exemple un serveur sur internet ou une autre machine du LAN. Il peut aussi s'agir d'un équipement réseau comme un routeur
- On s'authentifie soit avec une clé sécurisée, soit par mot de passe
- L'administrateur ouvre alors un shell et peut passer des commandes sur la machine distante.



Documentation projet INFRA SI B1

MYSQL

En continuant dans votre infrastructure la création de votre réseau, nous pouvons vous proposer d'autres outils qui permettraient d'obtenir une base de données. alors une base de données qu'est ce que cela pourrait vous apporter ?

et Bien, bien des choses, comme la possibilité d'administrer des droits dont votre hébergeur web, pouvoir créer la possibilité de se connecter, via identifiant ou un mot de passe, gérer tout droit administrateur un utilisateur sur le réseau, lui permet de modifier ou d'écrire certains fichiers en fonction de ses droits te son niveau à l'intérieur de la base de données. comme dit une base de données et l'endroit vous allez stocker toutes les informations liées à un utilisateur à la page au serveur, et divers autres informations qui peuvent être facultatives comme potentiellement très intéressantes. il est recommandé dans une infrastructure, de créer une base de données le mieux étant via l'outil « MYSQL ».

Pour résumer, MySQL est un système de gestion de base de données open source de type relationnel. Il fonctionne en tant que serveur et permet à plusieurs utilisateurs de gérer et de créer des bases de données. Il s'agit d'un élément central de tous les logiciels d'application Web LAMP open source utilisés pour créer des sites Web. LAMP veut dire Linux, Apache, MySQL et PHP.

Voilà ce qui conclut la partie des outils et des services utilisés, qui sont les prérequis nécessaires pour la création de votre

hébergeur web, via notre solution apportée. si vous souhaitez les documentations liées aux commandes pour cette fois-ci créez réellement votre machine virtuelle, qui vous permettra de mettre en place un server web, sur Nginx, vous pourrez retrouver toutes les documentations nécessaires sur notre site web, www.newyunniverse.net .