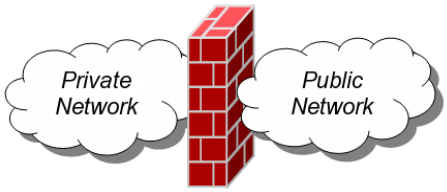
PPE Architecture réseau
Pare-feu IPFIRE

Version LICPGI

Mise en place d'un pare-feu
avec zone démilitarisée

Préambule

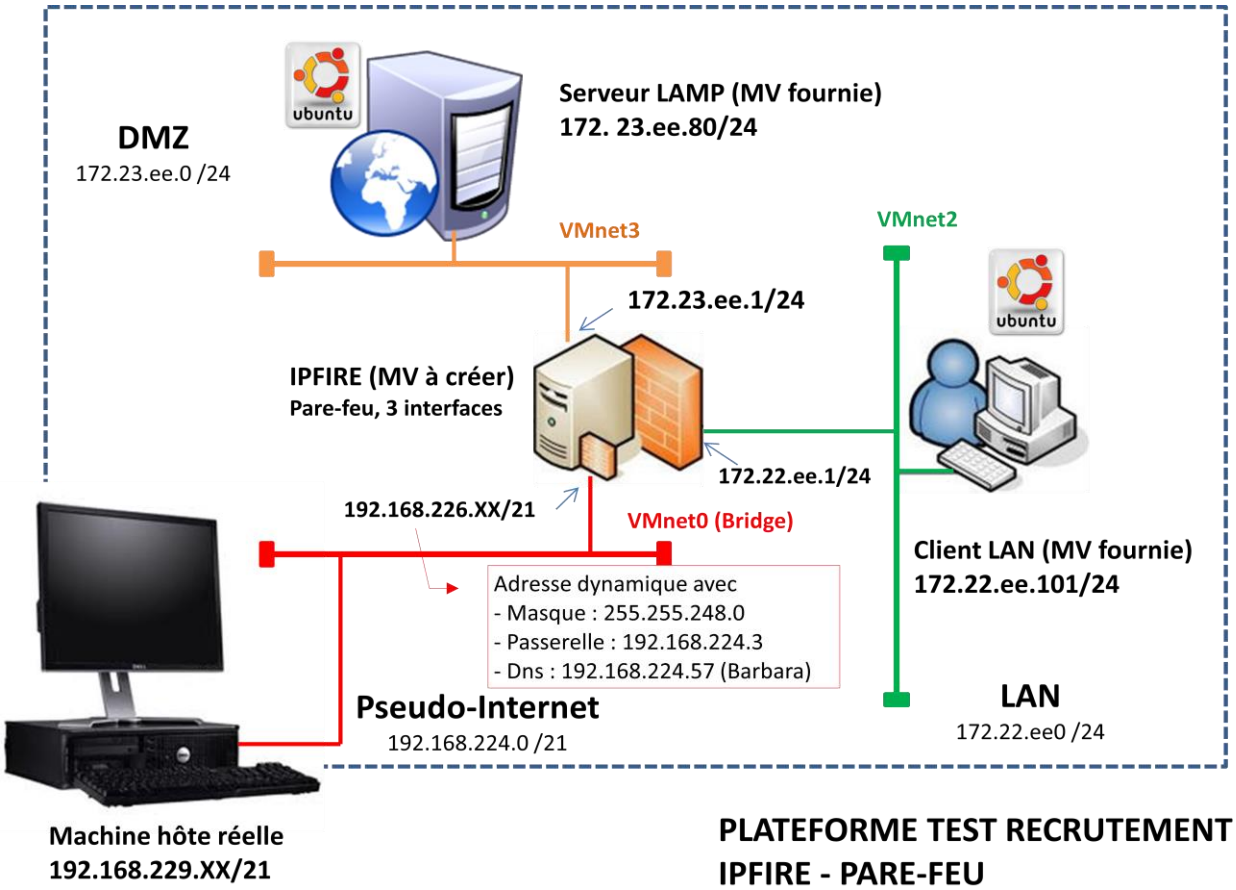


Dans ce PPE nous allons découvrir le rôle d'un pare-feu, qui consiste généralement à protéger une zone privée (Réseau local ou LAN) par rapport à une zone publique (Internet).

Il peut permettre également de filtrer l'accès à des zones qui doivent être accessibles du public, généralement appelées DMZ (zones démilitarisées).

Dans la configuration que nous allons mettre en place, nous souhaitons protéger le réseau local (représenté par une machine virtuelle Ubuntu), mais rendre accessible le serveur Web de notre entreprise, serveur que nous placerons donc dans un réseau distinct du réseau local.

La plateforme que l'on souhaite obtenir est représentée dans le schéma ci-dessous. Votre rôle consiste à installer le pare-feu (IPFIRE), permettant de protéger votre réseau local, tout en en permettant l'accès à un serveur WEB depuis l'internet. L'internet sera représenté dans notre configuration par le réseau local du lycée, pour des questions de facilité de mise en œuvre et de test.



PREPARATION DE VOTRE PLATEFORME

Copier/coller le répertoire MAQUETTE-IPFIRE-BASE (situé dans la partition LOGICIELS) dans la partition MACHINES. Renommer ensuite le répertoire dans MACHINES de la manière suivante : **MAQUETTE-IPFIRE-VOTRENOM**.

Créer un sous-répertoire supplémentaire dans ce dossier, que vous nommerez IpFire-NN (ou NN sont vos initiales.

EXPLICATIONS COMPLEMENTAIRES (à lire pendant la copie des machines)

Le tableau ci-dessous résume la fonction de chaque machine virtuelle appartenant à la maquette du TP, maquette qui vise à comprendre le fonctionnement d'un pare-feu.

	**MACHINE CLIENTE SUR LE LAN** La machine virtuelle qui vous est fournie pour faire office de client sur le LAN est une machine Linux basée sur la distribution Ubuntu 12.04 LTS, baptisée « Precise Pangolin ». L'utilisateur créé sur cette machine est « **BTS SIO** » (login : « **pangolin** »), avec comme mot de passe « **mdp** ».
	**SEVEUR LAMP DANS LA DMZ** La machine virtuelle qui vous est fournie pour faire office de serveur LAMP (Linux Apache MySql Php), autrement dit de serveur web, est une machine Ubuntu serveur, sans interface graphique. Cette machine devra être accessible de puis l'internet, comme le serait par exemple le serveur web qu'une entreprise hébergerait pour son catalogue en ligne. L'utilisateur créé sur cette machine est « **ubuntu** » avec comme mot de passe « **PASSWORD** », mais vous n'en aurez pas vraiment besoin si tout se passe bien.
	**PARE-FEU IPFIRE** C'est la machine virtuelle que vous devez installer, et qui ne permettra que les communications autorisées, les flux autorisés. Vous utiliserez la documentation d'installation fournie sous forme de PDF. Respectez bien les consignes et les éléments de configuration pour limiter les soucis, et notamment le plan d'adressage, car le client ubuntu et le serveur ubuntu sont pré-configurés pour s'insérer dans une plateforme ainsi configurée. Mot de passe **root** : **PASSWORD** – Mot de passe **admin** : **ADMIN**

IPFIRE

IPFire est une distribution Linux basée sur Linux From Scratch : « Le système de base utilise LFS (Linux from Scratch) », faisant office de pare-feu.

IPFire est basée sur Linux From Scratch, et est aussi à l'origine un spin-off de IPCop, mais dans la version 2, seule l'interface web d'IPCop a été utilisée.

La conception modulaire permet aux utilisateurs de créer un système adapté à ses besoins. Cela peut être un petit système très ancien, comme un processeur Intel Pentium 4 ou encore un processeur multi-cœur.

[extrait de wikipedia]

INSTALLATION d'IPFIRE

Utilisez l'Annexe A du Doc_Installation_IpFire_v.21docx pour installer IPFIRE, en respectant bien le plan d'adressage, de manière à pouvoir utiliser les machines virtuelles fournies pour :

- Le poste client situé dans le LAN : Ubuntu-Clt-Lan
- Le serveur LAMP situé dans la DMZ : Ubuntu-Srv-Dmz

Vérifiez que vous pouvez le « pinguer » depuis la machine hôte (la machine réelle sur laquelle vous travaillez).

DEMARRAGE des MACHINES VIRTUELLES

Dans VMWARE, **ouvrir** les deux machines virtuelles que vous avez copiées (donc depuis la partition MACHINES, répertoire X:\Maquette-IpFire-VOTRENOM) :

- ⇨ X:\Maquette-IpFire-VOTRENOM\Ubuntu-CltLan\Ubuntu-CltLAN.vmx pour le client
- ⇨ X:\Maquette-IpFire-VOTRENOM\Ubuntu-SrvDmz\Ubuntu-SrvDMZ.vmx pour le client
- ⇨ NB : X: est le lecteur correspondant à la partition MACHINES, en principe M: ou D: (suivant les salles).

Lorsque VMWARE demande si vous les avez copiées ou déplacées, CHOISIR « **Copied** » pour changer les adresses MAC de la machine de base. Sinon la configuration initiale des cartes sera conservée, car UBUNTU pensera qu'il s'agit des mêmes cartes installées.

FONCTIONNEMENT PAR DEFAUT DU PARE-FEU

Vous allez vérifier le fonctionnement par défaut du pare-feu :

- Depuis le LAN, on accède à la DMZ, donc au serveur WEB (172.23.ee.80)
  - Lancer le navigateur sur le client UBUNTU et taper l'adresse du serveur LAMP comme URL
- Depuis le LAN, on accède à Internet normalement :
  - Nous utilisons : 192.168.224.3
  - Normalement, vous devriez également avoir accès au véritable internet, par une astuce qu'il serait trop long d'expliquer ici (en gros un double nat/pat successif pour information).

  Utiliser le navigateur du client UBUNTU pour vérifier
- Depuis l'extérieur (le pseudo-internet = votre machine réelle), vous ne pouvez en aucun cas accéder au LAN même si vous mettez comme passerelle l'adresse IPFire en 192.168.226.XX
- Depuis l'extérieur (le pseudo-internet), vous ne pouvez en aucun cas accéder à le DMZ (pour l'instant) même si vous mettez comme passerelle l'adresse IPFire en 192.168.226.XX
- Vérifier également que vous accéder, depuis le LAN, à la configuration de l'IPFIRE en https :
  - Utiliser le navigateur du client Ubuntu, avec l'URL https://172.22.ee.1:444

Utiliser **l'annexe B** pour visualiser comment effectuer les différents tests.

ACCES A LA DMZ

Utilisez **l'annexe C** pour effectuer une redirection du port 80. Et accéder ainsi au serveur via l'adresse « publique » de votre routeur/pare-feu, à savoir 192.168.226.XX1. (Taper http://192.168.226.XX1 dans le navigateur de votre machine réelle.

FIN DU TP

Prendre le temps d'arrêter proprement les machines virtuelles.