une box avec debian

- Objet : Faire une box maison avec sa distribution.
- Niveau requis :
  débutant
- Commentaires : *Une box maison, avec unbound , isc-dhcp-server, isc-dhcp-client, iptables et surtout votre debian*
- Débutant, à savoir : Utiliser GNU/Linux en ligne de commande, tout commence là !.
- Suivi :
  en-chantier
  - Création par LaFouine 27/11/2018
  - Testé par <...> le <...> Fix Me!
- Commentaires sur le forum : en cours de redaction [1] Fix Me!

Nota :

Contributeurs, les Fix Me! sont là pour vous aider, supprimez-les une fois le problème corrigé ou le champ rempli !

Introduction

L'objectif de ce tutoriel est de combler un vide qui est le suivant :
Les tutoriels pour

- unbound,
- isc-dhcp-server,
- isc-dhcp-client,
- iptables,
- hostapd

sont souvent là, mais isolés, pour un débutant c'est difficile de savoir par quoi commencer.

l'idée de ce tuto c'est d'avoir quelque chose de fonctionnel pour démarrer et donc de savoir par quoi commencer.
Les conseils [conseil] sous cette clause sont facultatifs mais peuvent faire gagner du temps.

Installation

1. isc-dhcp-client et iptable sont en principe installés par défaut.
2. kernel: :quand vous voulez mais sans cela ça ne marchera pas ;)
3. iptables :en premier
4. isc-dhcp-server :en second
5. unbound :en troisième
6. hostapd :en quatrième
7. net-tools :quand vous voulez
8. ulogd2 :je l'utilise, mais ce n'est pas indispensable

9. matériel possédant aux moins 2 prises rj45 et du wifi.

kernel

nano /etc/sysctl.conf

```
net.ipv4.ip_forward=1
```

mettre a jour avec un sysctl -p

Iptables

Note, ce tutoriel est en cours de rédaction donc ne pas s'en servir pour le moment.

J'ai tenu à ce que ce soit fait avec debian , plutôt que d'autres distributions, les raisons sont multiples, mais en voici quelques-unes. Une distribution que je connais bien et donc les outils. Un deuxième pc qui peut dépanner. Apprendre, et pouvoir contrôler son réseau chez soi. etc etc.

Le schéma est le suivant:

[la box du FAI] ↔ [la box maison] ↔ vos machines on ne s'ocuppe pas de l'ipv6, j'ai malheureusement un FAI qui ne fournit pas ce type de prestation :(la configuration ipv6 n'est pas abordée, je vous recommande de fermer ipv6 si comme moi rien ne peux passer, l'ipv6 est en principe une norme qui devrait être acceptée.

iptables en premier pourquoi ? Parce que c'est aussi la sécurité, ensuite parce que cela peut loguer,

les lignes suivantes sont à adapter, car le nom de l'interface peut changer. la cible MASQUERADE indique de faire du nat, ce qui sera utilisé dans ce tutoriel, il est possible de faire autrement avec un pont/bridge

Requis :

```
iptables -t nat -A POSTROUTING -o enp1s0 -j MASQUERADE

iptables -A FORWARD -i enp1s0 -o wlanwifi -j ACCEPT
iptables -A FORWARD -i wlanwifi -o enp1s0 -j ACCEPT
```

Facultatif :

nom.sh

```
Limit=30
Burst=10
iptables -t nat -A POSTROUTING  -m limit --limit $Limit/h --limit-burst
$Burst -j NFLOG --nflog-group 0 --nflog-prefix  NAT_POSTROUTING
iptables -t nat -A PREROUTING  -m limit --limit $Limit/h --limit-burst
$Burst -j NFLOG --nflog-group 0 --nflog-prefix  NAT_PREROUTING
iptables -t nat -A INPUT  -m limit --limit $Limit/h --limit-burst
```

```
$Burst -j NFLOG --nflog-group 0 --nflog-prefix NAT_INPUT
iptables -t nat -A OUTPUT -m limit --limit $Limit/h --limit-burst
$Burst -j NFLOG --nflog-group 0 --nflog-prefix  "NAT_OUTPUT
```

Note : Il faut savoir que ces règles disparaissent au reboot. Comme il y beaucoup de tutoriels sur iptables. je vais plutôt vous donner les liens sur la documentation (ça chargerait trop le tutoriel). Sur Debian-Facilehttps://debian-facile.org/doc:reseau:iptables-pare-feu-pour-une-passerelle Lien externe plus complet: https://www.inetdoc.net/guides/iptables-tutorial/

isc-dhcp-server

isc-dhcp-server. Important.!

Ne démarre pas si le fichier /etc/network/interfaces n'est pas en relation parfaite, j'explique:

Il faut que l'interface soit opérationnelle/active et donc bien paramétrée , sinon isc-dhcp-server ne démarrera pas . si ce dernier ne démarre pas unbound en fera de même.

Si vous utilisez un client windows pour tester, je vous recommande de le redémarrer, Windows à du mal avec le réseau à se mettre à jour correctement avec une reconnexion >–> reconnexion, de même pour la box, certains paramètres peuvent changer, /etc/resolv.conf est un classique. Parfois ce sont certaines interfaces qui ne s'activent pas.

L'ordre de démarrage peut jouer un rôle, je vous conseille de faire votre propre service ou de modifier la configuration de Debian pour que cela démarre comme cité plus haut.

Petite parenthèse pour les débutants et aussi facultative :

Je conseille d'utiliser les alias pour éditer les fichiers cela va grandement vous faciliter la tâche, comme cela se passe sous root. Soyez vigilants à ne pas faire n'importe quoi sous Debian. Si vous voulez que cela soit pour tous les utilisateurs ça ce passe dans ce fichier :

```
/etc/bash.bashrc
```

```
Editeur="nano"
alias ndhcp=$Editeur' /etc/dhcp/dhcpd.conf'
alias ndhcps=$Editeur' /etc/default/isc-dhcp-server'
alias ndhcp=$Editeur' /etc/dhcp/dhcpd.conf'
```

Ce fichier est en root mais vous pouvez aussi le placer au niveau utilisateur. Cela va vous éviter de taper chaque fois le chemin et de devoir en plus savoir où il se trouve: un oubli ? : **alias** vous le montrera.

isc-dhcp-server choisir les interfaces

Ces fichiers sont sous **root** Donc penser à faire une sauvegarde avant toute chose ! éditer le fichier **/etc/default/isc-dhcp-server**

nom.sh

```
#ipv4
INTERFACESv4="enp2s0 enp3s0 enp4s0 wlx64f06d883452"
#ipv6 si vide pas d'interface donc pas d'ipv6
INTERFACESv6=""
```

Vous remarquez qu'il manque l'interface enp1s0, car c'est celle qui a un câble relié à la box du FAI , donc en dhcp ou en static, regardez dans la doc de votre box du fournisseur pour y mettre une ip fixe c'est quand même plus pratique.

isc-dhcp-server configuration dhcp

éditer le fichier : **/etc/dhcp/dhcpd.conf**

```
authoritative;

option domain-name "domroxlan.dom";

default-lease-time 600;
max-lease-time 7200;
ddns-update-style none;
log-facility local7;
option subnet-mask 255.255.255.0;

subnet 192.168.2.0 netmask 255.255.255.0 {
        range  192.168.2.20  192.168.2.29;
        option routers 192.168.2.21;
        option broadcast-address 192.168.2.255;
        option domain-name-servers 192.168.2.21;
}

subnet 192.168.3.0 netmask 255.255.255.0 {
        range  192.168.3.20  192.168.3.29;
        option routers 192.168.3.21;
        option broadcast-address 192.168.3.255;
        option domain-name-servers 192.168.3.21;
}

subnet 192.168.4.0 netmask 255.255.255.0 {
        range  192.168.4.20  192.168.4.29;
        option routers 192.168.4.21;
        option broadcast-address 192.168.4.255;
        option domain-name-servers 192.168.4.21;
}


subnet 192.168.50.0 netmask 255.255.255.0
{
```

```
        range  192.168.50.50  192.168.50.60;
        option routers 192.168.50.51;
        option broadcast-address 192.168.50.255;
        option domain-name-servers 192.168.50.51;
}
```

Ici soyez précis dans la syntaxe car si vous vous trompez d'un chiffre cela ne vous donnera pas la moindre info.

IMPORTANT: une fois que tout fonctionne changer ces valeurs pour des raison de sécurité évidentes, Pour les raisons qui m'ont poussé à faire cette documentation c'est le manque de wiki à fournir une ip complète... en gros une configuration qui fonctionne .

Configuration des interfaces

sujet : Le fichier /etc/network/interfaces

Conseil:

J'ai rencontré un bug à un moment donné en changeant la configuration de ce fichier. Je recommande donc d'arrêter le service AVANT de le modifier! Profitez de faire de même, et donc ce qui l'utilise.

Pas la peine de dire que la connexion est coupée si vous faites cela :)

```
source /etc/network/interfaces.d/*

auto lo
iface lo inet loopback
#============== wifi =============
allow-hotplug wlx234f0432556912
iface wlx234f0432556912inet static
        address 192.168.50.51
        netmask 255.255.255.0
        network 192.168.50.0
        wireless-power off
#============= rj45 ==============
allow-hotplug enp1s0
iface enp1s0 inet static
        address 192.168.0.11/24
        gateway 192.168.0.1
        # dns-* options are implemented by the resolvconf package, if
installed
        #dpkg -l |grep  resolvconf = null
        #dns-nameservers 192.168.0.1
#       dns-search domroxlan.dom

allow-hotplug enp2s0
iface enp2s0 inet static
        address 192.168.2.21
        netmask 255.255.255.0
```

```
        network 192.168.2.0

allow-hotplug enp3s0
iface enp3s0 inet static
        address 192.168.3.21
        netmask 255.255.255.0
        network 192.168.3.0

allow-hotplug enp4s0
iface enp4s0 inet static
        address 192.168.4.21
        netmask 255.255.255.0
        network 192.168.4.0
```

À ce stade les connexions filaires ne marcheront pas car unbound n'est pas présent donc il faut faire la suite si vous voulez que cela marche ainsi utilisez le dns de la box à ce moment là :)

Je remercie Mikl et raleur dans cette démarche car sans leur aide j'aurais bien plus galéré

Serveur Unbound pour un dns local

Soyez particulièrement prudent car ce service est sensible aux vulnérabilités.

Note. Je ne suis pas parvenu a trouver une traduction en français des paramètres, les valeurs sont à adapter selon vos besoins. j'ai donc juste indiqué les valeurs que j'utilise.

```
nano  /etc/unbound/unbound.conf
```

```
cat /etc/unbound/unbound.conf
# Unbound configuration file for Debian.
#
# See the unbound.conf(5) man page.
#
# See /usr/share/doc/unbound/examples/unbound.conf for a commented
# reference config file.
#
# The following line includes additional configuration files from the
# /etc/unbound/unbound.conf.d directory.
include: "/etc/unbound/unbound.conf.d/*.conf"

#server:
port:                   53                              #port d'écoute
do-ip4:                 yes                             #
do-ip6:                 yes                             #
do-udp:                 yes                             #protocole autorisé
do-tcp:                 yes                             #indique de
communiquer sur le protocole TCP
#interface: 0.0.0.0
access-control:         192.168.50.0/24 allow
```

```
interface:              192.168.50.51                   #requis wifi
interface:              192.168.4.21                    #requis rj45
interface:              192.168.3.21                    #requis rj45
interface:              192.168.2.21                    #requis rj45
interface:              127.0.0.1                       #?
access-control:         127.0.0.1       allow           #?
access-control:         192.168.0.0/24  allow           #requis rj45
access-control:         192.168.2.0/24  allow           #requis rj45
access-control:         192.168.3.0/24  allow           #requis rj45
access-control:         192.168.4.0/24  allow           #requis rj45
access-control:         192.168.50.0/24 allow           #requis wifi (pas en
service)
private-address:        192.168.0.0/24                  #renforce le coté
privé et  protège de la technique des "Relais DNS"
unwanted-reply-threshold: 10000000                      #eviter
l'empoisonnement DNS
aggressive-nsec: yes
harden-algo-downgrade:  no                              #l algorithme le
plus faible est exclut no
hide-identity:          yes                             #
hide-version:           yes
harden-glue:            yes
#ssl-upstream:          yes                             # oblige à
communiquer sur le protocole TLS.                      :yes:erreur :debug: tcp
error for address 8.8.8.8 port 53
#ssl-port:              853
prefetch:               yes                             # garde en cache les
bons résultats
prefetch-key:           yes                             #
cache-min-ttl:          100000                          #durée minimale
cache-max-ttl:          200000                          #durée max
key-cache-size:         50m
infra-cache-numhosts:   1000000                         #nombre d'hôtes qui
peuvent être mis en cache
do-ip6:                 no                              #desactive les
requêtes ipv6
tcp-idle-timeout:       15000                           #delai avant de
signaler un timeout sur la connextion

harden-below-nxdomain:  yes
harden-dnssec-stripped: yes                             #DNSSEC pour les
zones de confiance
val-clean-additional:   no                              #toutes les données
DNS non sécurisées son effacées
do-not-query-localhost: yes                             #permet d'interroger
localhost
so-reuseport:           yes                             #{linux seulement}
améliore les performance udp
#serve-expired: <yes or no>                             # tester
num-threads: 4
key-cache-slabs: 8
```

```
infra-cache-slabs: 8
msg-cache-slabs: 8
rrset-cache-slabs: 8
key-cache-size:         100m
key-cache-slabs:        2m
harden-short-bufsize:   yes                             #contre les très
petites tailles de mémoire tampon EDNS.
harden-large-queries:   yes                             #contre les requêtes
volumineuses
num-queries-per-thread: 100

val-log-level:          2                               #log
verbosity:              5                               #plage de 1 à 5 , 5
permet le plus parlant
log-time-ascii:         yes                             #valable sur un
autre fichier que syslog
log-queries:            yes                             #affiche une ligne
par requête
log-replies:            yes                             #affiche une ligne
par requête,(réponse)
log-local-actions:      yes                             #affiche les info de
la zone local
log-servfail:           yes                             #afficher pourquoi
les requêtes renvoient SERVFAIL Ref doc

logfile:                /var/log/unbound.log            #chemin d'accès

#private-domain:                "domroxlan.dom"                 #domaine
local

forward-zone:
        name: "."
#forward-addr: 192.168.0.1@53
forward-addr: 1.1.1.1@53
forward-addr: 1.0.0.1@53
forward-addr: 65.2.17.60@53
forward-addr: 65.2.17.61@53
forward-addr: 66.2.24.158@53
forward-addr: 67.2.24.162@53
forward-addr: 8.8.8.8@53
```

Bug connu : Si dans le fichier /var/log/syslog vous avez ceci

```
Jan 16 14:10:11 box kernel: [ 1352.364742] audit: type=1400
audit(1579180211.005:13): apparmor="DENIED" operation="open"
profile="/usr/sbin/unbound" name="/var/log/unbound/unbound.log" pid=1000
comm="unbound" requested_mask="ac" denied_mask="ac" fsuid=106 ouid=0
Jan 16 14:10:11 box unbound[1000]: Jan 16 14:10:11 unbound[1000:0] debug:
switching log to /var/log/unbound/unbound.log
Jan 16 14:10:11 box unbound[1000]: Jan 16 14:10:11 unbound[1000:0] error:
Could not open logfile /var/log/unbound/unbound.log: Permission denied
```

unbound ne peux pas écrire dans le log que vous lui avez fourni, cela est lié à apparmor il y a peu de documentation en français:

la solution est celle-ci

```
Mettre ceci
/{,var/}run/systemd/notify w,
Dans le fichier
/etc/apparmor.d/usr.sbin.unbound
```

Ensuite ceci ne devrai rien renvoyer (donc tout va bien)

```
apparmor_parser -r /etc/apparmor.d/usr.sbin.unbound
```

Vérifier les droits sur le fichier au besoin pour tester 0777 mais en principe un 0770 devrai suffire. Relancer le service unbound et regarder si le log est pris en compte

il peux être nécessaire de changer le fichier

```
/etc/resolv.conf
```

de façon à ce qu'il contienne :

```
nameserver 127.0.0.1
```

Rappelle: Ce fichier a la fâcheuse tendance à se modifier. Vous pouvez donc le verrouiller avec la commande **chattr**, **Attention** c'est pas anodin car le système ne peux plus mettre a jour le fichier. Par exemple, si vous supprimez le paquet unbound, l'ip ne pourra plus se mettre à jour. (c'est un exemple parmi les nombreuse autres mauvaises surprises qui en découlent.)

Attention l'utilisation peut empêcher le système d'écrire du coup le répertoire **/etc** est utiliseé à la place. vous aurez alors quelque chose de semblable

```
ls /etc |grep resolv.conf.dhclient
-rw-r--r-- 1 root root      47 mai 25 03:31 resolv.conf.dhclient-new.12784
-rw-r--r-- 1 root root      47 mai 25 12:06 resolv.conf.dhclient-new.13099
-rw-r--r-- 1 root root      47 mai 25 20:57 resolv.conf.dhclient-new.13271
```

il est peut être possible de passer par le fichier /etc/dhcp/dhclient.conf en modifiant ou en l'ajoutant avec

```
supersede domain-name-servers 127.0.0.1;
```

En redémarrant (le service ou la machine) cela devrait au moins vous garder la ligne concernée, mais comme ça boxe a fond dans ce fichier il est possible qu'autre chose vienne le modifier après... bref c'est bien relou pour pas grand chose et impossible d'être certain de ne pas avoir une modification suite à une installation d'un autre logiciel etc etc.

je n’apprécie pas ce type de comportement de la part des développeurs, pour la simple et bonne raison que si un fichier est modifié par l'utilisateur on a plus le droit

de le modifier sans son accord, particulièrement quand il s'agit de la configuration du système. car en cas de problème qui est responsable, la dernière valeur ou l'utilisateur,surtout que ça peut en plus venir, aux moment du renouvellement du bail de la box du FAI !

Pour tester utiliser la commande: **dig**

Si vous êtes sur un O.S propriétaire il peux s'avérer utile d'y effacer le cache dns sur un client windows on utilisera:

```
ipconfig /flushdns
```

A partir de là cela devrait suffire pour une connexion filaire et être fonctionnel,

Le point d'accès wifi

l'installation est assez simple.

```
aptitude install hostapd
```

fichier de configuration: **/etc/hostapd/hostapd.conf**

```
interface=wlx

#interface=wlan0
driver=nl80211
# Nom du spot Wi-Fi
ssid=Rox
country_code=Ch
#hw_mode=g
channel=7
macaddr_acl=0
#wifi fermer = 1 ouver 0
auth_algs=1
ignore_broadcast_ssid=0
wpa=2
wpa_passphrase=15carracteconseillier:D
wpa_key_mgmt=WPA-PSK
wpa_pairwise=TKIP
wpa_group_rekey=86400
ieee80211n=1
# Beacon interval in kus (1.024 ms)
beacon_int=100
# mode Wi-Fi (a = IEEE 802.11a, b = IEEE 802.11b, g = IEEE 802.11g)
hw_mode=g
wme_enabled=1
# DTIM (delivery trafic information message)
dtim_period=2
```

```
# Maximum number of stations allowed in station table
max_num_sta=10
# Fragmentation threshold; 2346 = disabled (default)
fragm_threshold=2346
```

j'ai pas trouvé de documentation en français mais, il faut chercher a savoir 2 choses Si la carte/clé wifi est bien reconnue par le kernel. Le nom qui est retenu ou plutôt attribué à cette carte ici : **wlx**

Note avec iptables je vous conseille de filtrer les adresse mac, c'est pas infaillible mais ça va laisser des traces dans les logs et de compliquer la tache du pirate. Dans le cas où la clef serait craquée.

vous devriez à ce stade avoir une machine qui sert donc de “pc/box” transportable n'importe où, avec votre distribution ,un serveur dns,un point d'accès wifi.

Je remercie tous ceux qui m'ont apporté de l'aide grâce au forum.

1)

N'hésitez pas à y faire part de vos remarques, succès, améliorations ou échecs !

From:
http://debian-facile.org/ - **Documentation - Wiki**

Permanent link:
http://debian-facile.org/atelier:chantier:une-box-maison

Last update: **29/10/2022 11:39**