

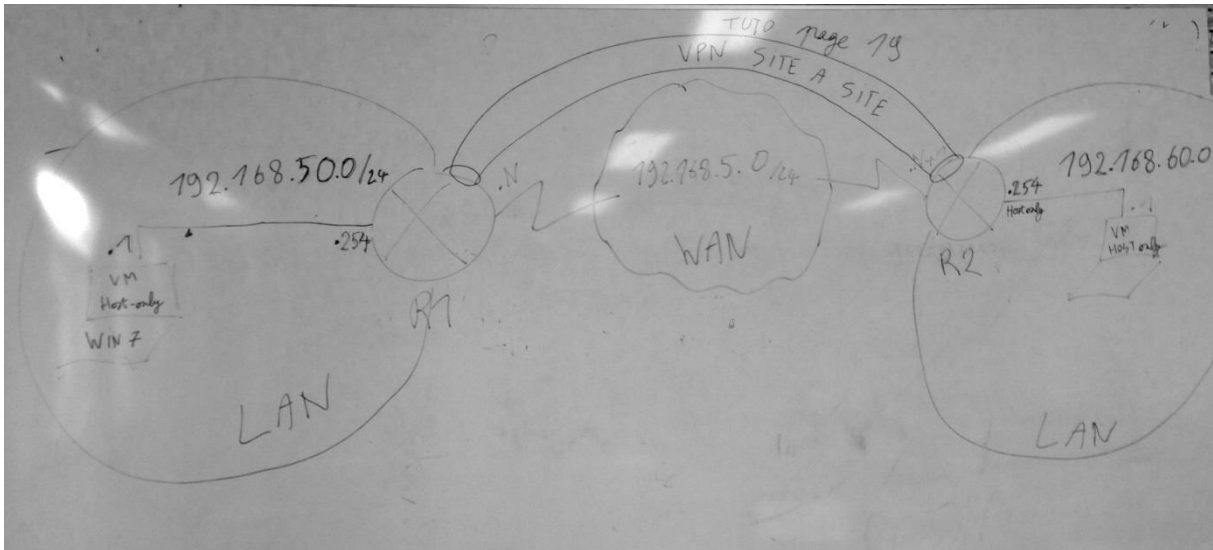
Configuration d'un OpenVPN de site à site

Contenu

1. Objectif	2
1.1. Schéma du réseau	2
1.2. Tutorial: Trad_FR_pfsense_OVPN.pdf.....	2
2. vmware Workstation : la configuration des cartes réseau	3
2.1. Réinitialisation des paramètres réseau : Si rien ne fonctionne au niveau du réseau	3
2.2. Configuration du mode bridged	4
3. Configuration réseau du routeur R1	7
4. Configuration d'un poste client P1 du LAN du routeur R1	12
4.1. Exemple d'un poste sous Linux (préférez un poste sous Windows 7)	12
4.2. Sauvegarder la configuration du routeur R1.....	16
5. Configuration routeur R2	18
5.1. Arrêter le routeur R1 avant de le cloner	18
5.2. Cloner R1 en R2	19
Une fois R1 arrêté, cloner le (current state , Full clone).....	19
6. Configuration du poste P2 cote R2.....	21
7. Créer le VPN site à site	21
7.1. Configurer openvpn de R2.....	21
7.2. Configurer openvpn de R1.....	26
8. Configuration des pare feu.....	30
9. Sauvegardes et Tests	36
9.1. Sauvegarde des configurations des routeurs	36
9.2. Arrêt des routeurs	36
10. Consultation des log (notamment en cas de problèmes)	37
10.1. LOG du pare feu.....	37
10.2. Problème des adresses privées	39
10.3. LOG openVPN	42
11. TEST du VPN	44
11.1. Test de ping	44
11.2. Capture de trame	45

1. Objectif

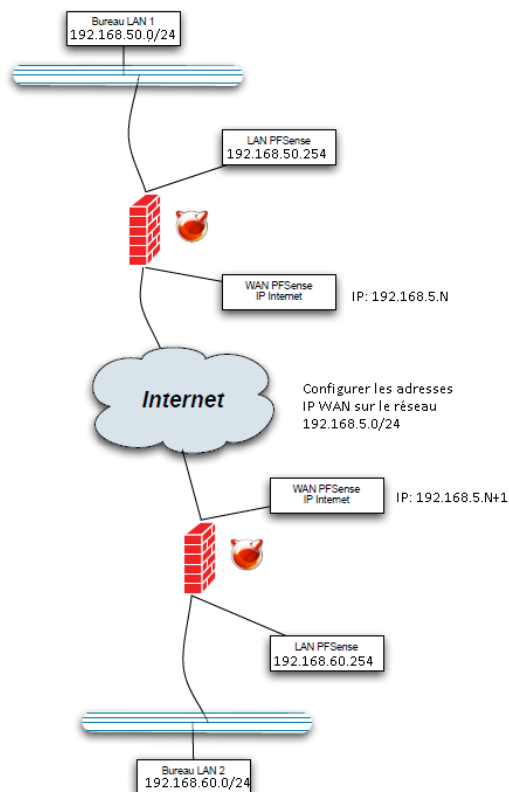
1.1. Schéma du réseau



L'idée est de configurer 2 réseaux LAN distants (192.168.50.0/24 et 192.168.60.0/24) et de configurer les routeurs R1 et R2 pour créer un tunnel VPN site à site.

1.2. Tutorial: Trad_FR_pfsense_OVPN.pdf

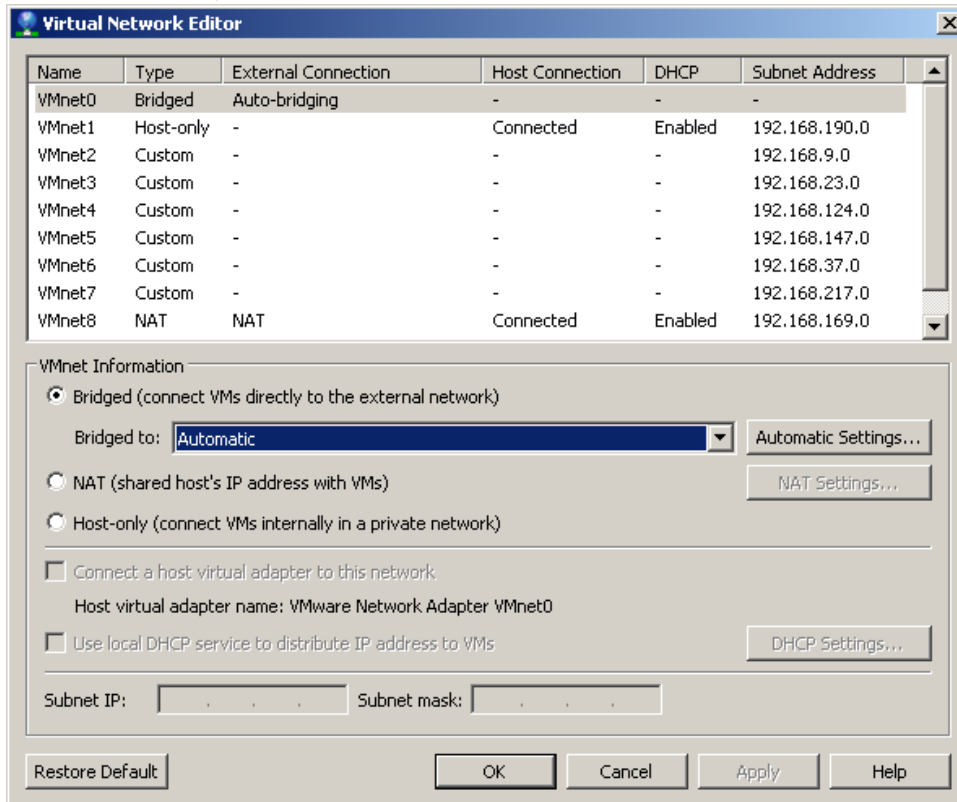
Tutorial: Trad_FR_pfsense_OVPN.pdf page 19 Configuration d'un OpenVPN de site à site mais en utilisant les adresses IP suivantes:



2. vmware Workstation : la configuration des cartes réseau

2.1. Réinitialisation des paramètres réseau : Si rien ne fonctionne au niveau du réseau

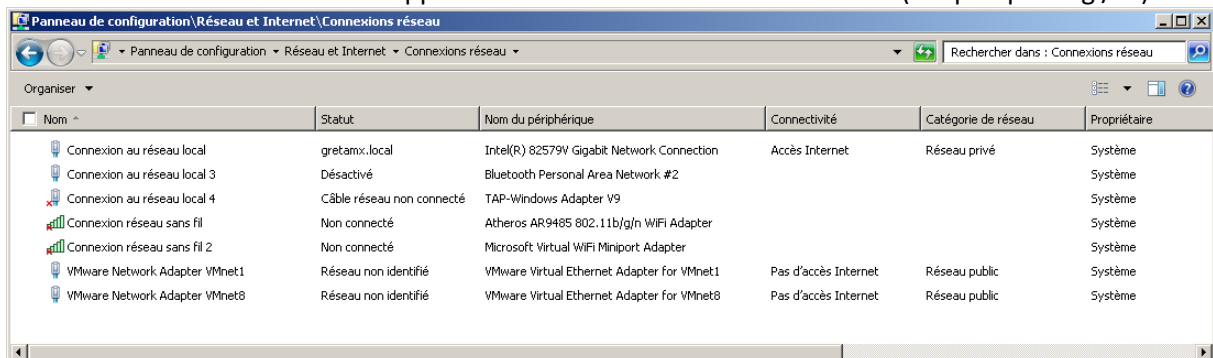
Dans workstation, menu "edit" → "virtual network editor"



Bouton "restaure default" (attention cela peut avoir une incidence sur vos Machines virtuelles)

Cela restaure les paramètres des cartes virtuelles réseau nommées VMnet0,1,...8

Les cartes virtuelles connectées apparaissent dans les connexions réseaux. (ou par ipconfig /all)



Extrait ipconfig /all

Carte Ethernet VMware Network Adapter VMnet1 :

```
Suffixe DNS propre ... la connexion. . . :
Description. . . . . : VMware Virtual Ethernet Adapter for VMnet1
Adresse physique . . . . . : 00-50-56-C0-00-01
DHCP activ,. . . . . : Non
Configuration automatique activ,e. . . : Oui
Adresse IPv6 de liaison locale. . . . : fe80::850:b0dd:f9ec:6b99%22(pr,f,r,)
Adresse IPv4. . . . . : 192.168.190.1(pr,f,r,)
Masque de sous-r,seau. . . . . : 255.255.255.0
Passerelle par d,faut. . . . . :
IAID DHCPv6 . . . . . : 369119318
DUID de client DHCPv6. . . . . : 00-01-00-01-1B-9A-24-50-10-60-4B-4A-FB-D9
Serveurs DNS. . . . . : fec0:0:0:ffff::1%1
                        fec0:0:0:ffff::2%1
                        fec0:0:0:ffff::3%1
NetBIOS sur Tcip. . . . . : Activ,
```

Carte Ethernet VMware Network Adapter **VMnet8** :

```
Suffixe DNS propre ... la connexion. . . :
Description. . . . . : VMware Virtual Ethernet Adapter for VMnet8
Adresse physique . . . . . : 00-50-56-C0-00-08
DHCP activ,. . . . . : Non
Configuration automatique activ,e. . . : Oui
Adresse IPv6 de liaison locale. . . . : fe80::45e3:82d9:a5f6:6066%23(pr,f,r,)
Adresse IPv4. . . . . : 192.168.169.1(pr,f,r,)
Masque de sous-r,seau. . . . . : 255.255.255.0
Passerelle par d,faut. . . . . :
IAID DHCPv6 . . . . . : 385896534
DUID de client DHCPv6. . . . . : 00-01-00-01-1B-9A-24-50-10-60-4B-4A-FB-D9
Serveurs DNS. . . . . : fec0:0:0:ffff::1%1
                        fec0:0:0:ffff::2%1
                        fec0:0:0:ffff::3%1
NetBIOS sur Tcip. . . . . : Activ,
```

2.2. Configuration du mode bridged

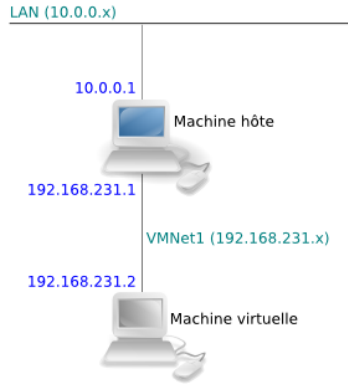
Source: <http://www.commentcamarche.net/faq/3759-vmware-et-virtualbox-les-differents-types-de-reseau>

Quand on crée une machine virtuelle dans VMWare, nous avons le choix entre 3 types de connectivité : Host-only, [NAT](#) ou Bridged.

Le schéma suivant vous explique la différence entre ces 3 modes:

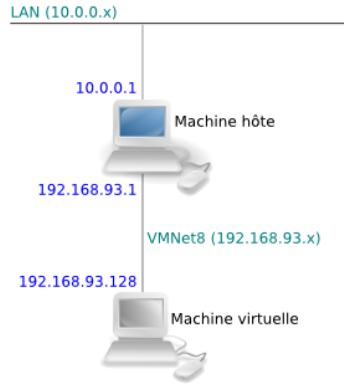
Les types de réseau VMWare

	Machine virtuelle	
	Accès au LAN	Adresse IP de LAN
Host-only	NON	NON
NAT	OUI	NON
Bridged	OUI	OUI



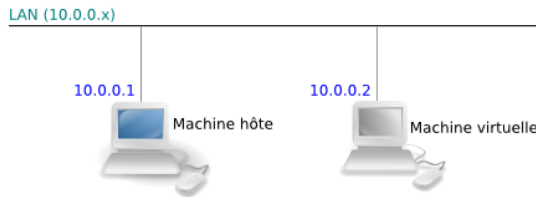
Host-only

La machine virtuelle a accès uniquement à la machine hôte sur un réseau privé virtuel (VMNetX).
Vu du LAN, il n'y a aucune nouvelle machine.
La machine hôte fait office de serveur DHCP pour le réseau VMNet1.



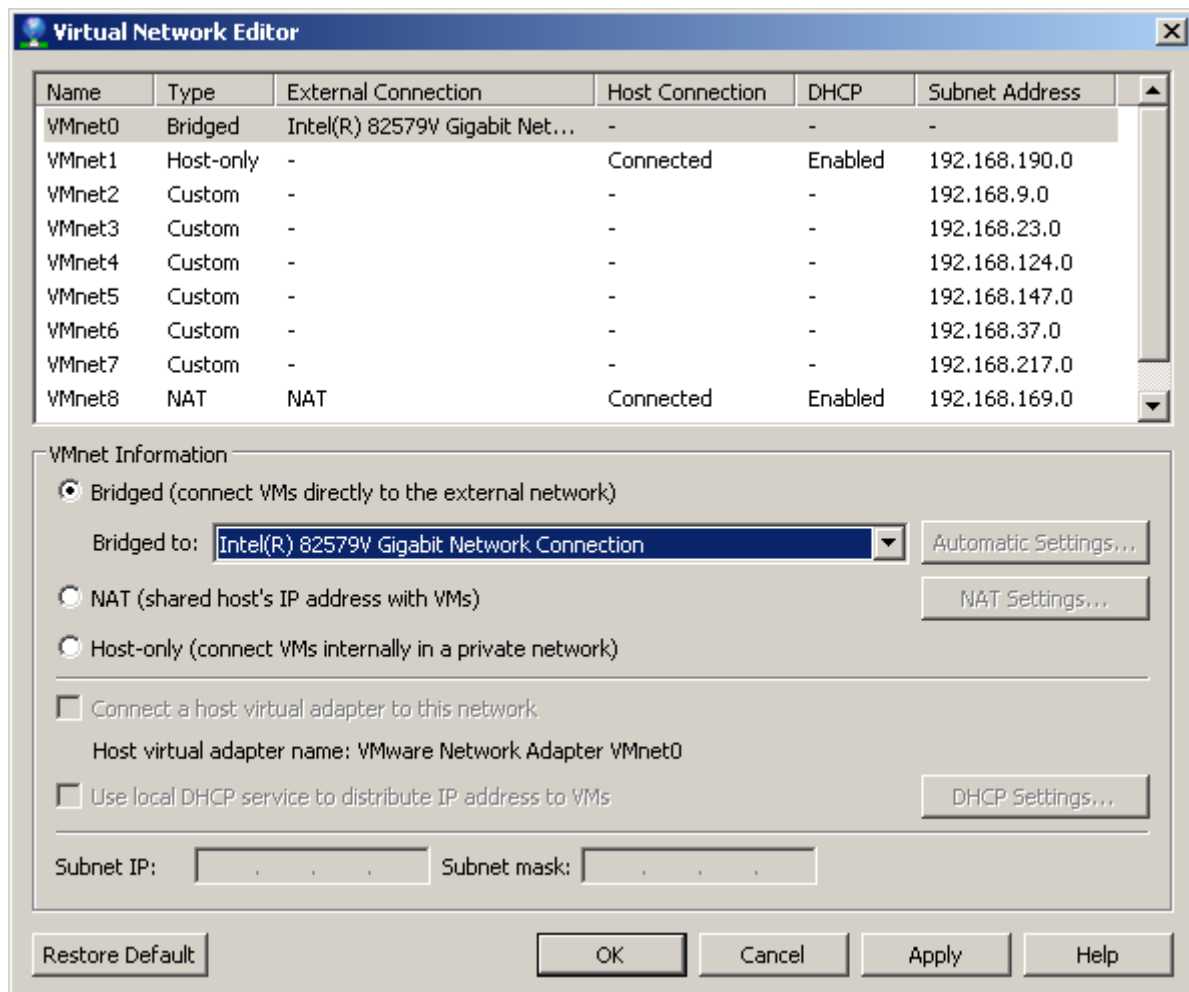
NAT

La machine virtuelle a accès au LAN à travers la machine hôte par un routage de type NAT (Network Address Translation).
Vu du LAN, il n'y a aucune nouvelle machine.
La machine virtuelle envoie ses requêtes sur le LAN en utilisant l'adresse IP de la machine hôte.
Nécessite un LAN opérationnel et connecté.
La machine hôte fait office de serveur DHCP pour le réseau VMNet8.



Bridged

La machine virtuelle a accès direct au LAN.
Vu du LAN, il y a une nouvelle machine avec sa propre adresse IP.
Nécessite un LAN opérationnel et connecté.
La machine virtuelle utilise le serveur DHCP du LAN (si présent).



Configurez pour la carte réseau virtuelle "VMnet0" le mode "bridged" en sélectionnant la carte réseau plutôt que de laisser le mode auto . Cela n'est pas obligatoire mais cela permet parfois d'éviter certains problèmes (surtout pour des PC qui ont plusieurs cartes réseau physiques filaires ou sans fil).

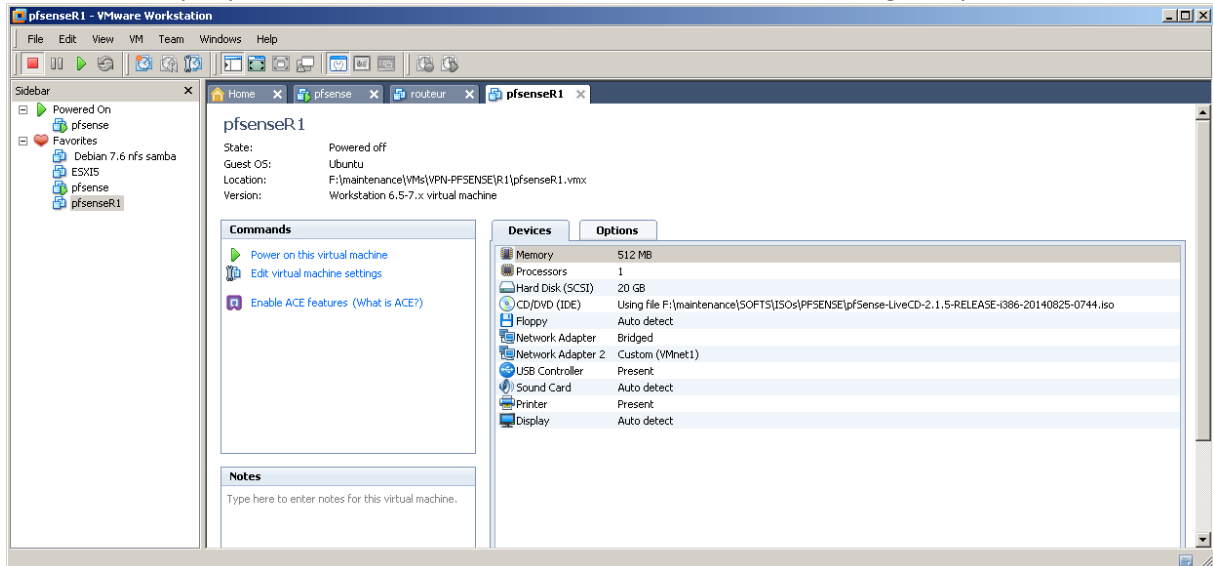
3. Configuration réseau du routeur R1

https://doc.pfsense.org/index.php/Installing_pfsense_in_VMware_under_Windows

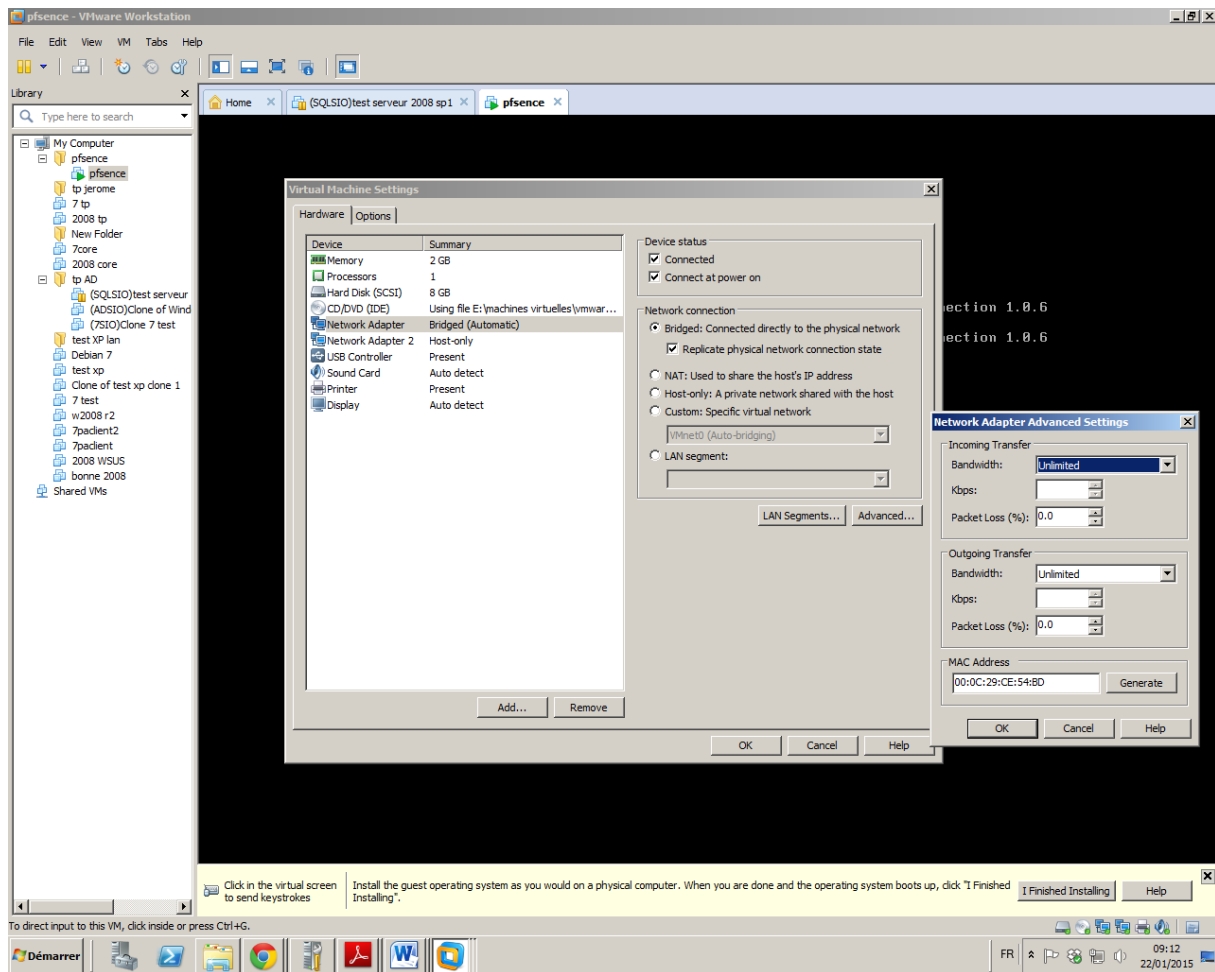
D'après cette documentation il apparaît préférable d'avoir plusieurs cartes réseau filaire.

Si vous n'avez pas plusieurs cartes réseau : suivre la méthode suivante :

Configurer la VM avec une carte réseau en bridge + une carte réseau supplémentaire en "host only". Utiliser comme CDROM (connecté et connecté au démarrage) l'image iso i386 (ou 64 bits à tester , ne fonctionne pas pour moi, EN out cas il vaut mieux utiliser la même image iso pour les 2 routeurs !)



Repérer les adresses MAC des cartes réseau par vmware workstation dans le mode avancé des cartes réseau) soit par un `ipconfig /all` comme ci-dessous un extrait qui permet de repérer l'adresse MAC (physique) de VMnet1 (utilisée pour la connexion Host-Only que l'on va utiliser pour notre routeur côté LAN).



Exemple ci-dessus dans la salle BTS: la carte WAN du routeur en mode bridged (connecté au réseau de la salle) a pour adresse MAC 00:0C:29:CE:54:BD

Booter

- "Do you want to set up VLAN" Pas de configuration de VLAN
- PAS d'Autodetection de l'interface WAN :
- "Enter the WAN interface Name" nommer l'interface le0 (ou me0 si ça ne fonctionne pas) comme interface WAN .

Remarque1 : en auto cela semble ne pas fonctionner (sans doute dû à VMWARE)

Remarque2: les noms d'interface semblent être soit le0,le1 soit em0,em1

- "Enter The LAN interface NAME" nommer l'interface le1 comme interface LAN

A ce moment là pfsence affiche le menu général comme ci-dessous (avec éventuellement des adresses IP pour les 2 Cartes s'il y a un DHCP sur le réseau ou non)


```

WAN -> le0
LAN -> le1

Do you want to proceed [y!n]?y

Writing configuration...done.
One moment while we reload the settings... done!
*** Welcome to pfSense 2.1.5-RELEASE-cdrom (i386) on pfSense ***

WAN (wan)      -> le0      ->
LAN (lan)      -> le1      -> v4: 192.168.50.254/24

0) Logout (SSH only)          8) Shell
1) Assign Interfaces          9) pfTop
2) Set interface(s) IP address 10) Filter Logs
3) Reset webConfigurator password 11) Restart webConfigurator
4) Reset to factory defaults  12) pfSense Developer Shell
5) Reboot system              13) Upgrade from console
6) Halt system                 14) Enable Secure Shell (sshd)
7) Ping host                    15) Restore recent configuration

99) Install pfSense to a hard drive, etc.

Enter an option: █

```

- Assign Interface : (on assigne à nouveau les cartes réseau pour bien vérifier les adresses MAC et faire en sorte que notre carte réseau en bridged soit pour la carte WAN du routeur et la carte en host-only soit pour le côté LAN du routeur.)

- Salle BTS : choisir em0 comme care réseau WAN et em1 pour le LAN

```

em0  00:0c:29:ce:54:bd  (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.6
em1  00:0c:29:ce:54:c7  (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.6
usb10 (up)

Do you want to set up VLANs first?

If you are not going to use VLANs, or only for optional interfaces, you should
say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y!n]? n

*NOTE*  pfSense requires *AT LEAST* 1 assigned interface(s) to function.
        If you do not have *AT LEAST* 1 interfaces you CANNOT continue.

        If you do not have at least 1 *REAL* network interface card(s)
        or one interface with multiple VLANs then pfSense
        *WILL NOT* function correctly.

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: em0 █

```

- Verifier dans vmware les adresses MAC . em0 (ou le0) correspond bien à la carte en bridged.

Ici l'adresse MAC ... correspond bien à la carte WAN

"Enter the WAN interface": em0 (ou le0)

"Enter the WAN interface": em1 (ou le1)

"Enter the optional ... (or nothing if finished)" // entrée (c'est fini)

"Do you want to proceed ?" // yes

```
Configuring firewall.....done.
Generating RRD graphs...done.
Starting syslog...done.
Starting CRON... done.
Bootup complete

FreeBSD/i386 (pfSense.localdomain) (ttyv0)

*** Welcome to pfSense 2.1.5-RELEASE-cdrom (i386) on pfSense ***

WAN (wan)      -> le0      -> v4/DHCP4: 192.168.1.17/24
LAN (lan)     -> le1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          8) Shell
1) Assign Interfaces          9) pfTop
2) Set interface(s) IP address 10) Filter Logs
3) Reset webConfigurator password 11) Restart webConfigurator
4) Reset to factory defaults    12) pfSense Developer Shell
5) Reboot system              13) Upgrade from console
6) Halt system                14) Enable Secure Shell (sshd)
7) Ping host                  15) Restore recent configuration

99) Install pfSense to a hard drive, etc.

Enter an option: █
```

- menu "Set Interface(s) IP address" : Configurer l'IP WAN en 192.168.5.N

```
Enter an option: 2

Available interfaces:

1 - WAN (le0 - dhcp, dhcp6)
2 - LAN (le1 - static)

Enter the number of the interface you wish to configure: 1
Configure IPv4 address WAN interface via DHCP? [y!n]
> n

Enter the new WAN IPv4 address. Press <ENTER> for none:
> 192.168.5.27

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0    = 8

Enter the new WAN IPv4 subnet bit count:
> 24

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> █
```

```

Enter the new WAN IPv4 subnet bit count:
> 24

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address WAN interface via DHCP6? [y/n]
> n

Enter the new WAN IPv6 address. Press <ENTER> for none:
>
Disabling DHCPD...Done!
Disabling DHCPD...Done!

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to WAN... Reloading filter...
DHCPD...

The IPv4 WAN address has been set to 192.168.5.27/24
You can now access the webConfigurator by opening the following URL in your web
browser:
        https://192.168.5.27/

Press <ENTER> to continue.

```

A la question "Do you want to revert to http as the webconfigurator protocol [y/n] ?" -> n
Par précaution, répondre « n » pour garder l'accès sécurisé (https).

- Configurer l'IP LAN en 192.168.50.254 (192.168.60.254 pour R2) pas de serveur DHCP pour l'instant côté LAN non plus.

Installer pfsense sur le disque dur (menu 99)

Accéder à a configuration de R2 , sauvegarder la config du routeur (quick/easy sauvegarde , standard kernel)

Déconnecter le CDROM

Menu 5 : reboot system

Au reboot , les IP ont bien été sauvegardées

```
Starting DHCPv6 service...done.
Configuring firewall.....done.
Generating RRD graphs...done.
Starting syslog...done.
Starting CRON... done.
Bootup complete

FreeBSD/i386 (pfSense.localdomain) (ttyv0)

*** Welcome to pfSense 2.1.5-RELEASE-pfSense (i386) on pfSense ***

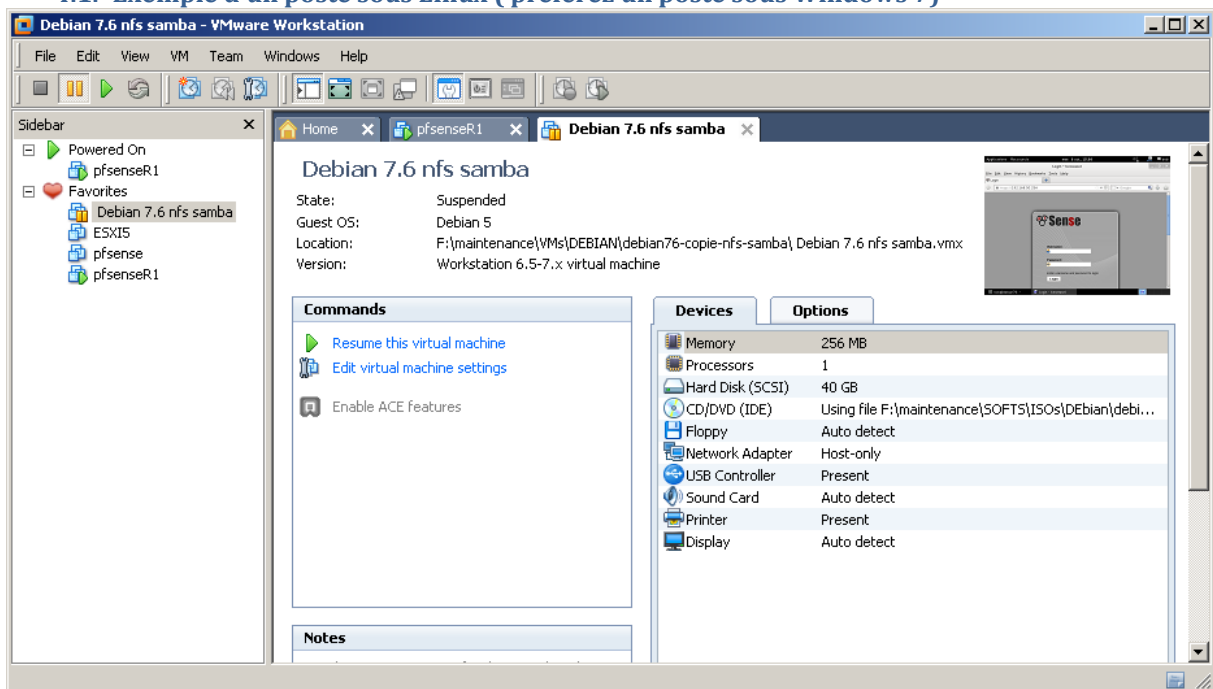
WAN (wan)      -> le0          -> v4: 192.168.5.27/24
LAN (lan)      -> le1          -> v4: 192.168.50.254/24

0) Logout (SSH only)          8) Shell
1) Assign Interfaces          9) pfTop
2) Set interface(s) IP address 10) Filter Logs
3) Reset webConfigurator password 11) Restart webConfigurator
4) Reset to factory defaults  12) pfSense Developer Shell
5) Reboot system              13) Upgrade from console
6) Halt system                 14) Enable Secure Shell (sshd)
7) Ping host                    15) Restore recent configuration

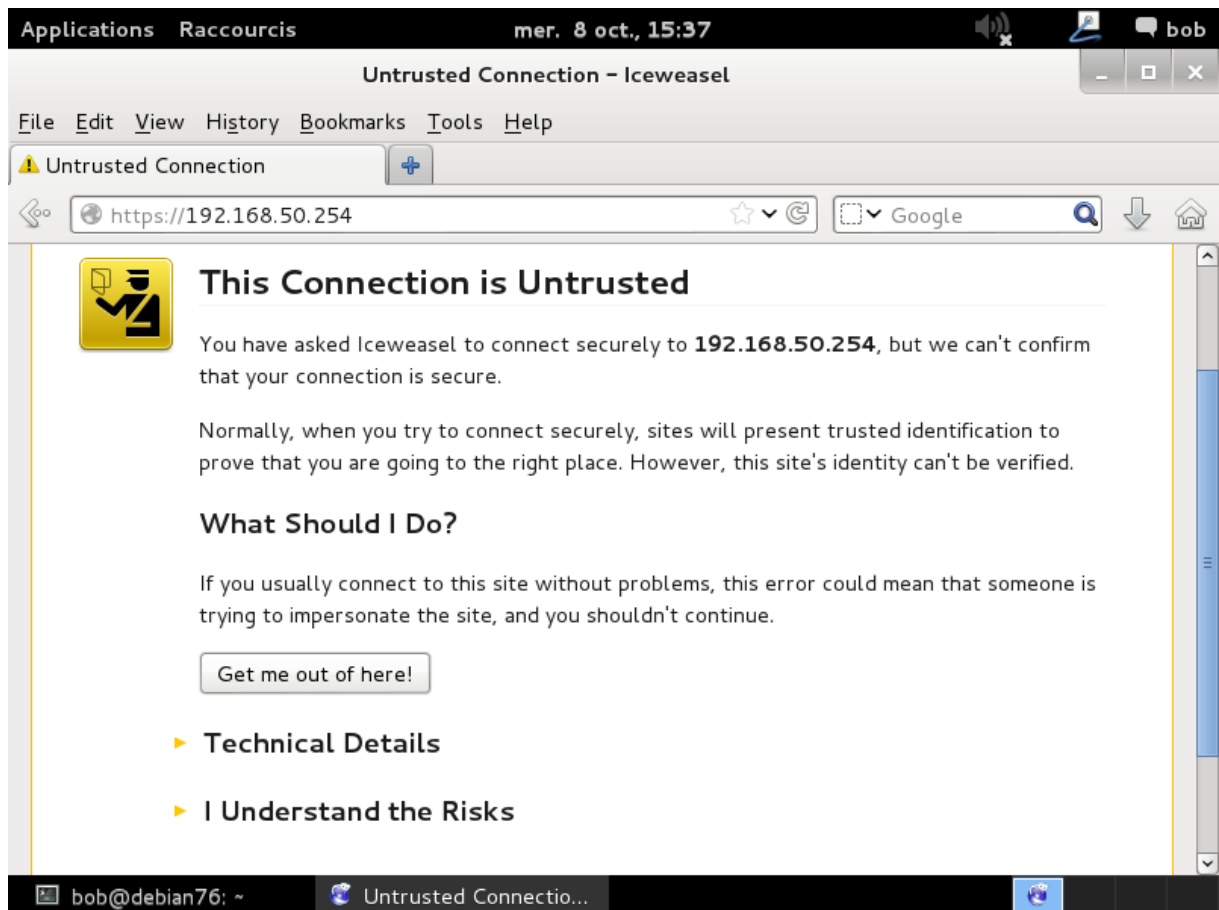
Enter an option: |
```

4. Configuration d'un poste client P1 du LAN du routeur R1

4.1. Exemple d'un poste sous Linux (préférez un poste sous Windows 7)

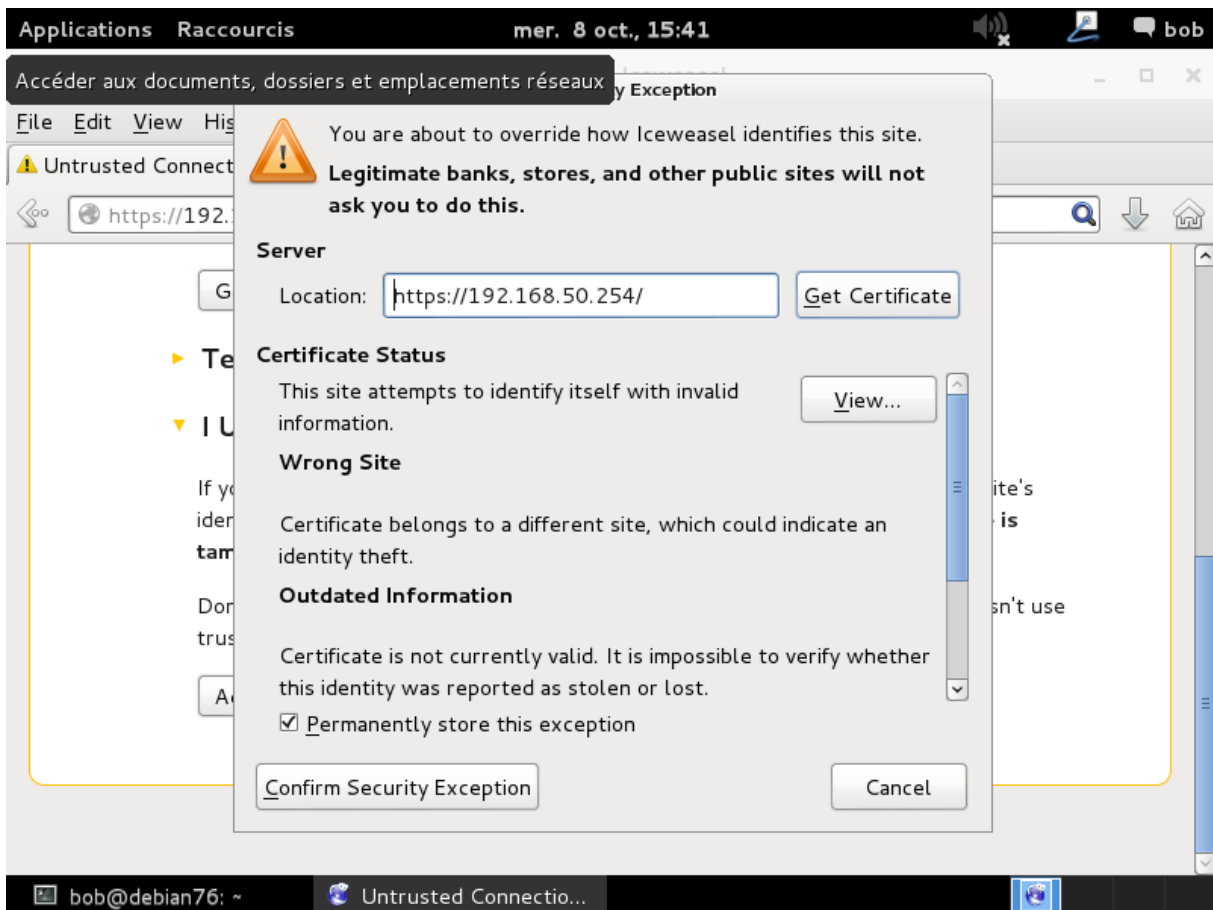


Configurer l'IP du poste en 192.168.50.1

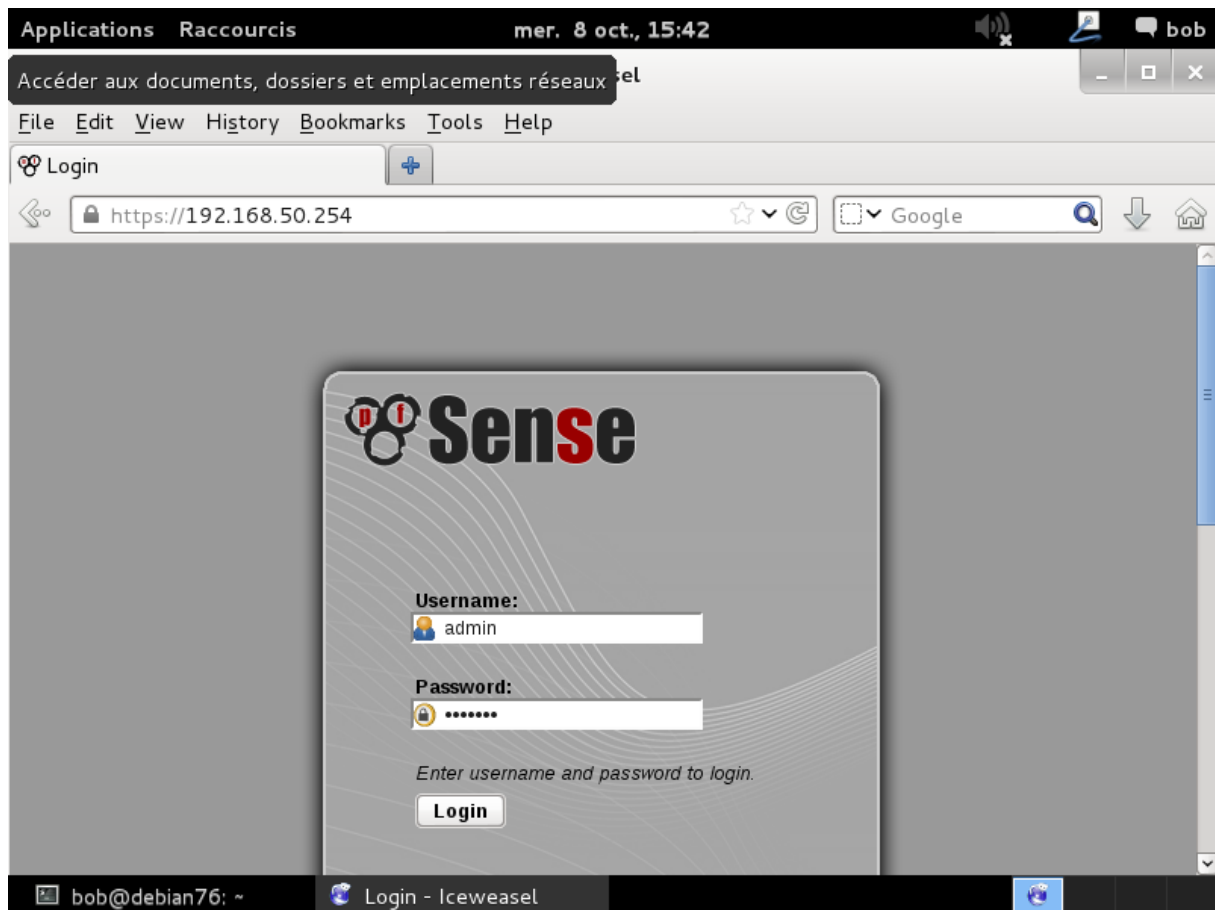


L'interface de pfsense se fait du côté LAN (si l'interface LAN du routeur pfsense est configurée) Routeur R2.

"I understand the risks" pour obtenir le certificat du site interne et l'installer malgré le fait qu'il ne viennent pas d'une autorité certifiée



Confirm exception



Username admin
Mot de passe pfsense

L'assistant "wizzard" se lance: changer l'URL par <https://192.168.60.254> pour annuler l'assistant.

Applications Raccourcis mer. 8 oct., 15:44 bob

Parcourir et lancer les applications installées - Status: Dashboard - Iceweasel

File Edit View History Bookmarks Tools Help

pfSense.localdomain - Status: ...

https://192.168.50.254

Google

pfSense

System Interfaces Firewall Services VPN Status Diagnostics Gold

Status: Dashboard

System Information

Name	pfSense.localdomain
Version	2.1.5-RELEASE (i386) built on Mon Aug 25 07:44:26 EDT 2014 FreeBSD 8.3-RELEASE-p16
	Unable to check for updates.
Platform	cdrom
CPU Type	Intel(R) Core(TM) i3-2370M CPU @ 2.40GHz
Uptime	02 Hours 00 Minute 47 Second
Current date/time	Mon Jan 26 21:02:17 UTC 2015
DNS server(s)	127.0.0.1 192.168.1.254

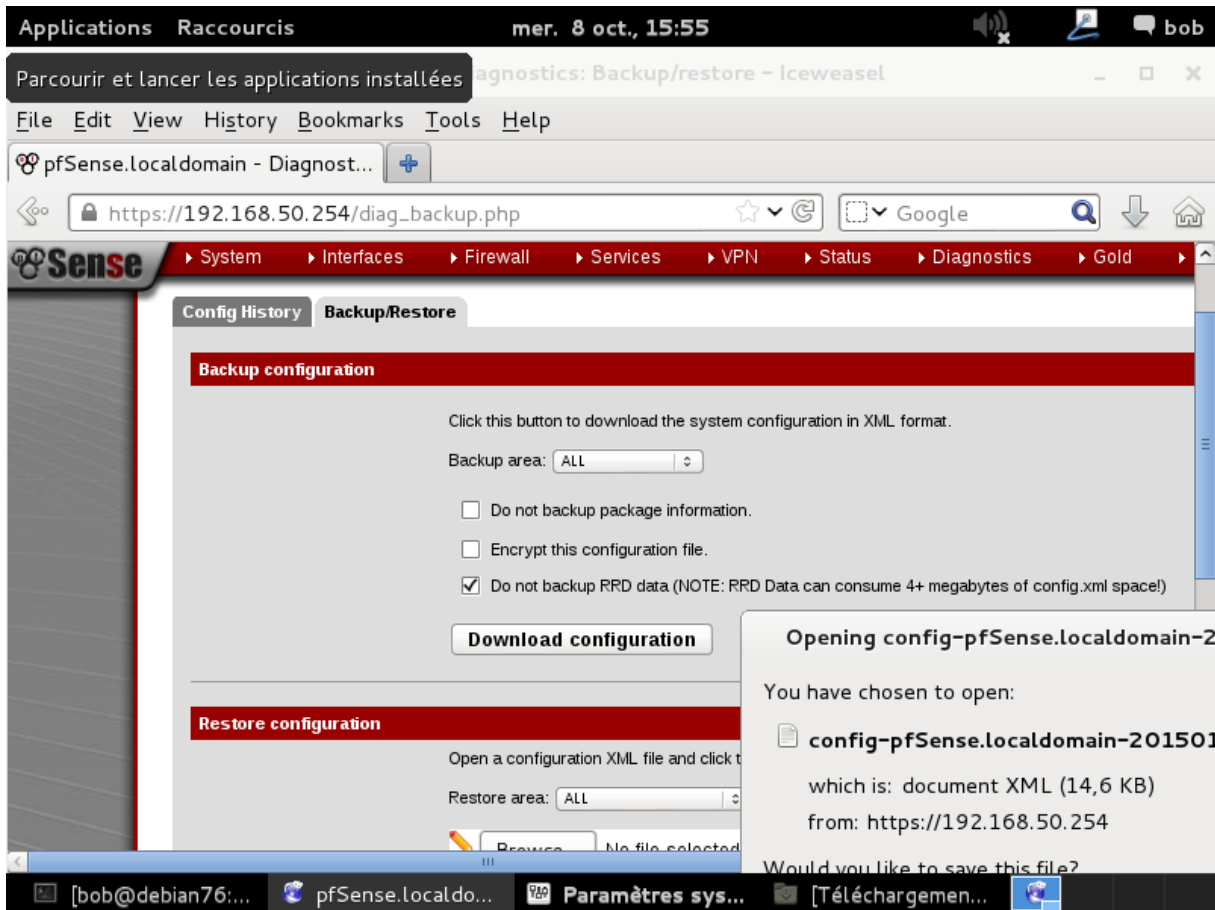
Interfaces

WAN	↑ autoselect 192.168.5.27
LAN	↑ autoselect 192.168.50.254

bob@debian76: ~ pfSense.localdomain ...

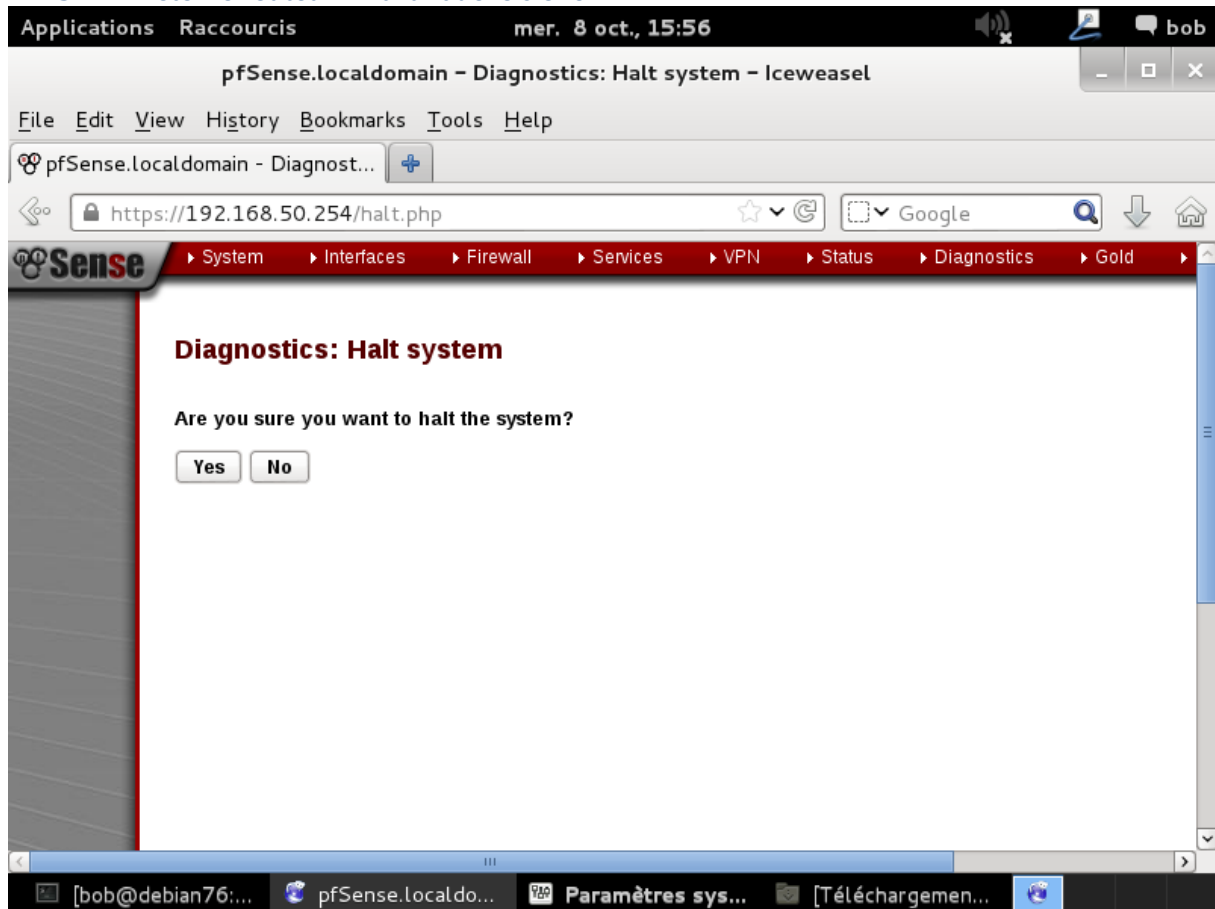
4.2. Sauvegarder la configuration du routeur R1

pfSense keeps its configuration in one convenient XML document. A backup of this document can be saved by going to **Diagnostics > Backup/Restore**, and clicking **Download Configuration**.



5. Configuration routeur R2

5.1. Arrêter le routeur R1 avant de le cloner



YES

```
7) Ping host 15) Restore recent configuration
99) Install pfSense to a hard drive, etc.
Enter an option:
Message from syslogd@pfSense at Jan 26 21:00:57 ...
pfSense php: /index.php: Successful login for user 'admin' from: 192.168.50.25
*** FINAL System shutdown message from root@pfSense.localdomain ***
System going down IMMEDIATELY

pfSense is now shutting down ...
Jan 26 21:15:01 lighttpd[25469]: (server.c.1558) server stopped by UID = 0 PID =
1
Waiting (max 60 seconds) for system process 'vnru' to stop...done
Waiting (max 60 seconds) for system process 'bufdaemon' to stop...done
Waiting (max 60 seconds) for system process 'syncer' to stop...
Syncing disks, vnodes remaining...0 0 0 0 done
All buffers synced.
Uptime: 2h13m47s
```

5.2. Cloner R1 en R2

Une fois R1 arrêté, cloner le (current state , Full clone)

Clone Virtual Machine Wizard

Clone Type
How do you want to clone this virtual machine?

Clone method

- Create a linked clone
A linked clone is a reference to the original virtual machine and requires less disk space to store. However, it cannot run without access to the original virtual machine.
- Create a full clone
A full clone is a complete copy of the original virtual machine at its current state. This virtual machine is fully independent, but requires more disk space to store.

< Précédent Suivant > Annuler

Clone Virtual Machine Wizard

Name of the New Virtual Machine
What name would you like to use for this virtual machine?

Virtual machine name
R2

Location
F:\maintenance\VMs\VPN-PFSENSE\R2 Browse...

< Précédent Terminer Annuler

Spécifier le nom et l'emplacement (pas forcément identique à la capture ce dessus)

Assigner au routeur R2 l'adresse IP WAN 192.168.5.N+1 LAN 192.168.60.254

Installer pfsense sur le disque dur (menu 99)

```
Starting DHCPv6 service...done.  
Configuring firewall.....done.  
Generating RRD graphs...done.  
Starting syslog...done.  
Starting CRON... done.  
Bootup complete
```

```
FreeBSD/i386 (pfSense.localdomain) (ttyv0)
```

```
*** Welcome to pfSense 2.1.5-RELEASE-pfSense (i386) on pfSense ***
```

```
WAN (wan)      -> le0      -> v4: 192.168.5.28/24  
LAN (lan)     -> le1      -> v4: 192.168.60.254/24
```

- | | |
|-----------------------------------|----------------------------------|
| 0) Logout (SSH only) | 8) Shell |
| 1) Assign Interfaces | 9) pfTop |
| 2) Set interface(s) IP address | 10) Filter Logs |
| 3) Reset webConfigurator password | 11) Restart webConfigurator |
| 4) Reset to factory defaults | 12) pfSense Developer Shell |
| 5) Reboot system | 13) Upgrade from console |
| 6) Halt system | 14) Enable Secure Shell (sshd) |
| 7) Ping host | 15) Restore recent configuration |

```
Enter an option: █
```

6. Configuration du poste P2 cote R2

Cloner le poste coté R1 et lui assigner l'IP 192.168.60.1

7. Créer le VPN site à site

Explication des paramètres lors de la création du VPN:

https://doc.pfsense.org/index.php/OpenVPN_Site_To_Site

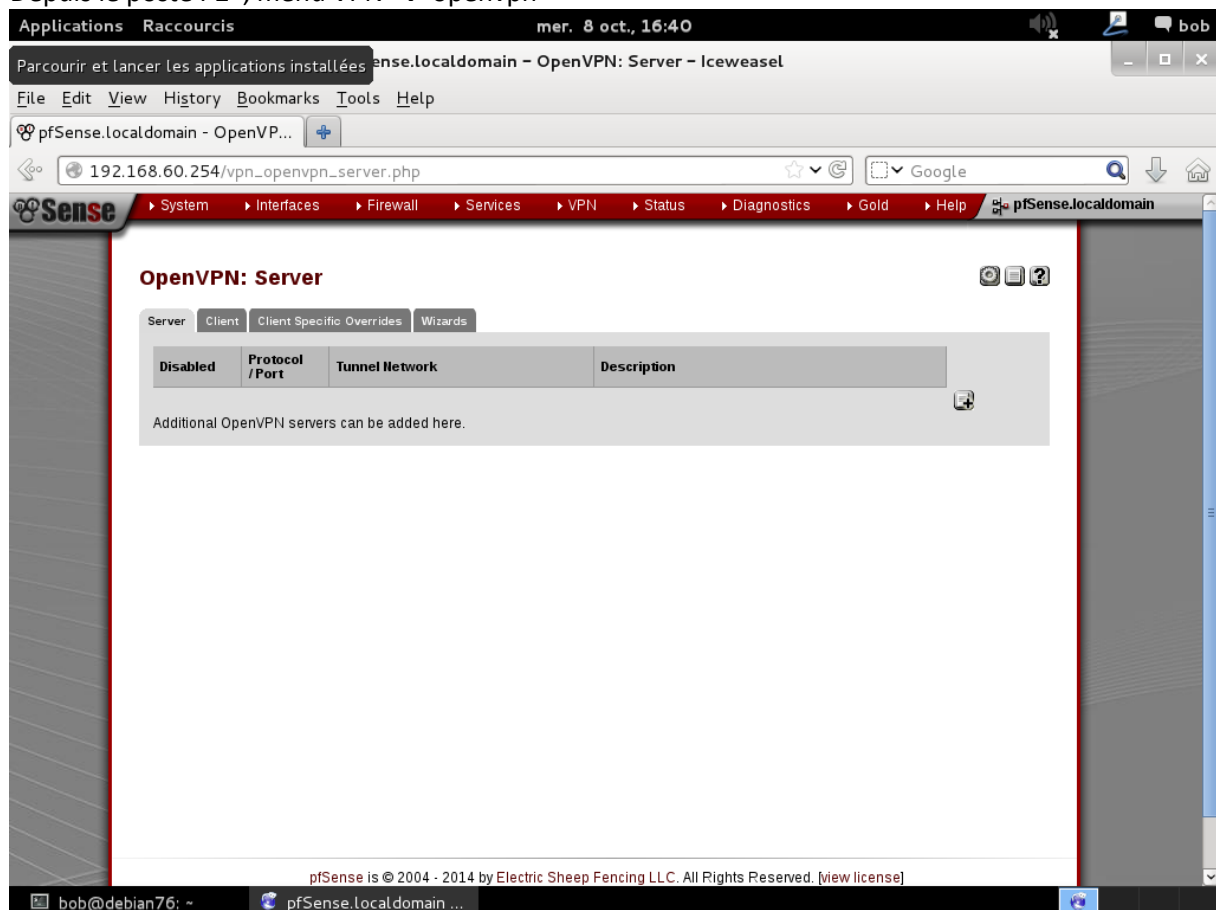
Capture d'écran de pfsense lors de la création du VPN:

https://doc.pfsense.org/index.php/Routing_internet_traffic_through_a_site-to-site_OpenVPN-connection_in_PfSense_2.1

7.1. Configurer openvpn de R2

Source https://doc.pfsense.org/index.php/Routing_internet_traffic_through_a_site-to-site_OpenVPN-connection_in_PfSense_2.1

Depuis le poste P2 , menu VPN → openvpn



+Configuration du serveur openvpn:

The image shows two screenshots of the pfSense OpenVPN server configuration interface. The top screenshot displays the 'General information' section, and the bottom screenshot displays the 'Tunnel Settings' section.

General information

- Disabled:** Disable this server. Set this option to disable this server without removing it from the list.
- Server Mode:** Peer to Peer (Shared Key)
- Protocol:** UDP
- Device Mode:** tun
- Interface:** WAN
- Local port:** 1194
- Description:** You may enter a description here for your reference (not parsed).

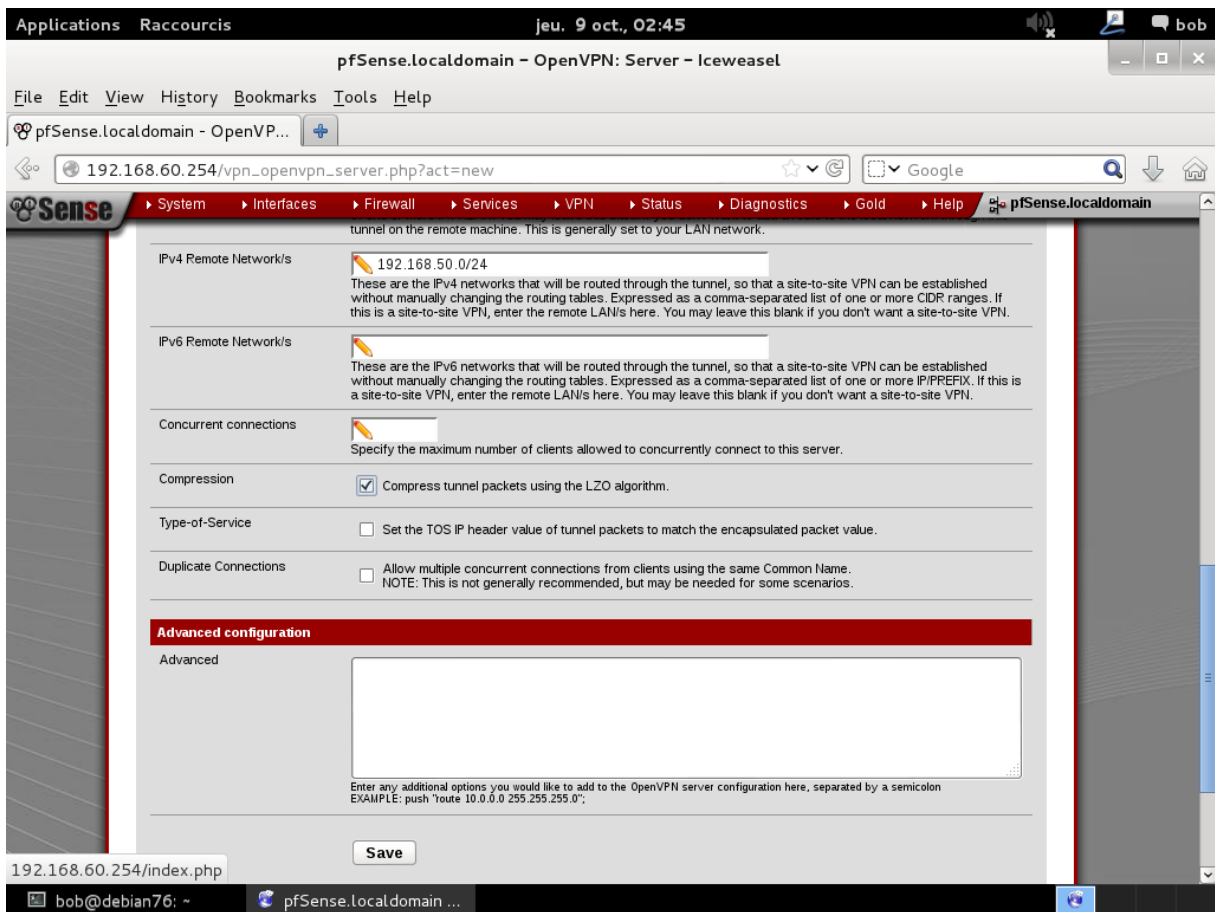
Cryptographic Settings

- Shared Key:** Automatically generate a shared key.
- Encryption algorithm:** AES-128-CBC (128-bit)
- Hardware Crypto:** No Hardware Crypto Acceleration

Tunnel Settings

- IPv4 Tunnel Network:** 192.168.10.0/24
This is the IPv4 virtual network used for private communications between this server and client hosts expressed using CIDR (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses can optionally be assigned to connecting clients. (see Address Pool)
- IPv6 Tunnel Network:** [Empty field]
- IPv4 Local Network/s:** 192.168.60.0/24
These are the IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges. You may leave this blank if you don't want to add a route to the local network through this tunnel on the remote machine. This is generally set to your LAN network.
- IPv6 Local Network/s:** [Empty field]
- IPv4 Remote Network/s:** 192.168.50.0/24
These are the IPv4 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more CIDR ranges. If this is a site-to-site VPN, enter the remote LAN/s here. You may leave this blank if you don't want a site-to-site VPN.
- IPv6 Remote Network/s:** [Empty field]
- Concurrent connections:** [Empty field]
Specify the maximum number of clients allowed to concurrently connect to this server.
- Compression:** Compress tunnel packets using the LZO algorithm.
- Type-of-Service:** Set the TOS IP header value of tunnel packets to match the encapsulated packet value.

Les données dans le tunnel seront transportés sur le réseau IP 192.168.10.0/24
Le réseau distant est bien 192.168.50.0/24 (permet d'ajouter une route sur le routeur)
Le réseau local est bien 192.168.60.0/24



La compression permet d'utiliser une bande passante réduite

Bouton SAVE

Applications Raccourcis | jeu. 9 oct., 02:46 | bob

pfSense.localdomain - OpenVPN: Server - Iceweasel

File Edit View History Bookmarks Tools Help

192.168.60.254/vpn_openvpn_server.php

System Interfaces Firewall Services VPN Status Diagnostics Gold Help

OpenVPN: Server

Server Client Client Specific Overrides Wizards

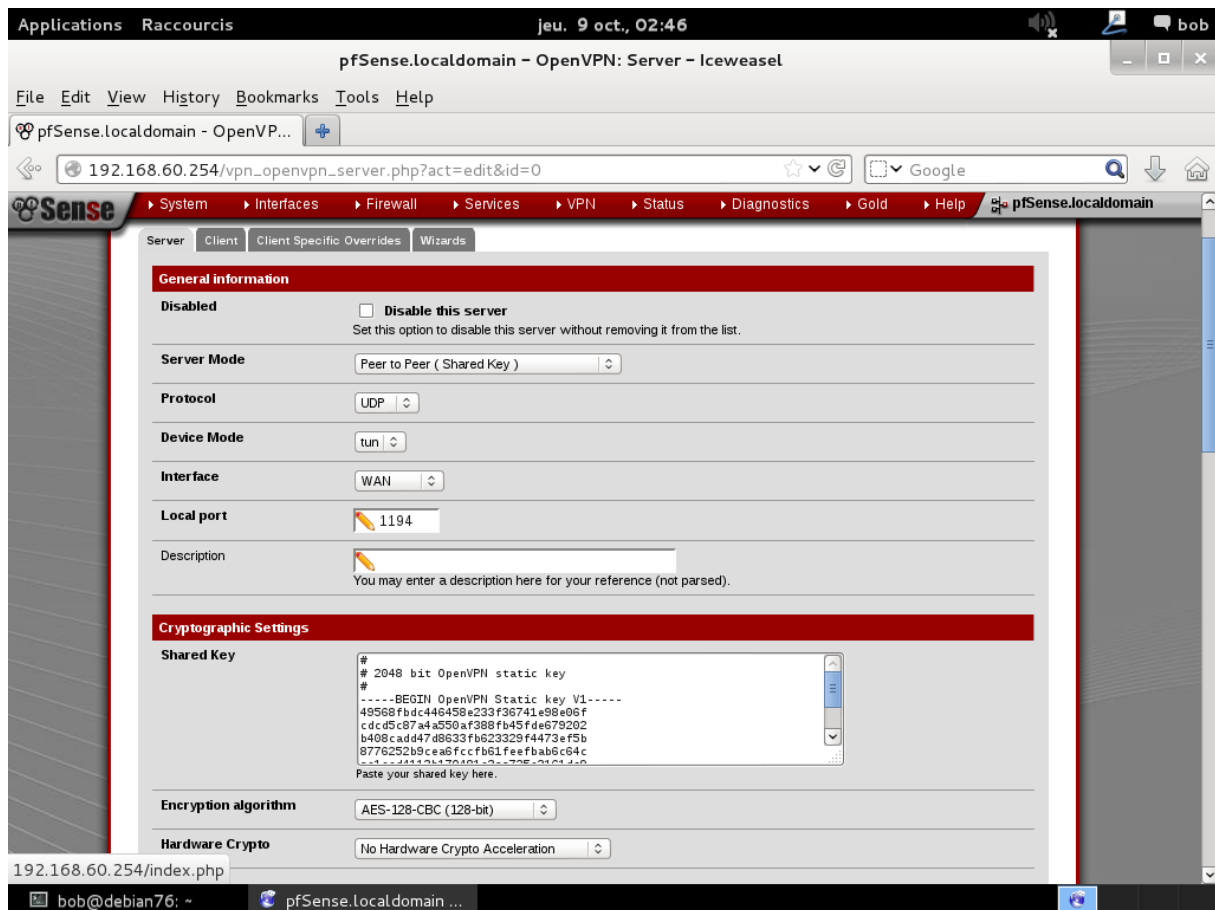
Disabled	Protocol / Port	Tunnel Network	Description
NO	UDP / 1194	192.168.10.0/24	

Additional OpenVPN servers can be added here.

pfSense is © 2004 - 2014 by Electric Sheep Fencing LLC. All Rights Reserved. [view license]

bob@debian76: ~ | pfSense.localdomain ...

Bouton "edit server"





Peer to peer (shared key).

Shared key : The keys can be made in the GUI. Check "Automatically generate a shared key.", and when the settings are saved, a key will be generated. Then copy/paste the key into the client

Il faut copier cette clé pour la partie client d'openVPN.

Le plus simple est d'utiliser une clé USB pour y créer un fichier keyvpn.txt avec cette clé "shared key".

La clé USB est visible dans la machine virtuelle si elle est connectée, voir  en bas à droite de la fenêtre de VMWARE.

Une fois la clé copiée, utilisez le même  pour déconnecter la clé de cette machine virtuelle.

7.2. Configurer openvpn de R1

Applications Raccourcis jeu. 9 oct., 02:56 bob

pfSense.localdomain - OpenVPN: Client - Iceweasel

File Edit View History Bookmarks Tools Help

pfSense.localdomain - OpenVP... +

https://192.168.50.254/vpn-openvpn_client.php

Sense System Interfaces Firewall Services VPN Status Diagnostics Gold Help pfSense.localdomain

OpenVPN: Client

Server Client Client Specific Overrides Wizards

Disabled	Protocol	Server	Description
----------	----------	--------	-------------

Additional OpenVPN clients can be added here.

pfSense is © 2004 - 2014 by Electric Sheep Fencing LLC. All Rights Reserved. [view license]

bob@debian76: ~ pfSense.localdomain ...

Côté client

Applications Raccourcis | jeu. 9 oct., 02:59 | bob

pfSense.localdomain - OpenVPN: Client - Iceweasel

File Edit View History Bookmarks Tools Help

pfSense.localdomain - OpenVP... | Google

https://192.168.50.254/vpn_openvpn_client.php?act=new

Sense | System | Interfaces | Firewall | Services | VPN | Status | Diagnostics | Gold | Help | .. 01 unread notice ..

OpenVPN: Client

Server Client Client Specific Overrides Wizards

General information

Disabled **Disable this client**
Set this option to disable this client without removing it from the list.

Server Mode Peer to Peer (Shared Key)

Protocol UDP

Device mode tun

Interface WAN

Local port
Set this option if you would like to bind to a specific port. Leave this blank or enter 0 for a random dynamic port.

Server host or address

Server port

Proxy host or address

Proxy port

Proxy authentication extra options Authentication method : none

Server host name resolution Infinitely resolve server

bob@debian76: ~ | pfSense.localdomain ...

Peer to peer (shared key)

192.168.5.28 est l'adresse IP WAN du routeur distant ou est configure le serveur openvpn

Applications Raccourcis jeu. 9 oct., 03:01 bob

pfSense.localdomain - OpenVPN: Client - Iceweasel

File Edit View History Bookmarks Tools Help

pfSense.localdomain - OpenVP... +

https://192.168.50.254/vpn_openvpn_client.php?act=new

Sense System Interfaces Firewall Services VPN Status Diagnostics Gold Help .. 01 unread notice ..

Tunnel Settings

IPv4 Tunnel Network
This is the virtual network used for private communications between this client and the server expressed using CIDR (eg. 10.0.0/24). The first network address is assumed to be the server address and the second network address will be assigned to the client virtual interface.

IPv6 Tunnel Network
This is the IPv6 virtual network used for private communications between this client and the server expressed using CIDR (eg. fe80::/64). The first network address is assumed to be the server address and the second network address will be assigned to the client virtual interface.

IPv4 Remote Network/s
These are the IPv4 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more CIDR ranges. If this is a site-to-site VPN, enter the remote LAN/s here. You may leave this blank to only communicate with other clients.

IPv6 Remote Network/s
These are the IPv6 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more IP/PREFIX. If this is a site-to-site VPN, enter the remote LAN/s here. You may leave this blank to only communicate with other clients.

Limit outgoing bandwidth
Maximum outgoing bandwidth for this tunnel. Leave empty for no limit. The input value has to be something between 100 bytes/sec and 100 Mbytes/sec (entered as bytes per second).

Compression Compress tunnel packets using the LZO algorithm.

Type-of-Service Set the TOS IP header value of tunnel packets to match the encapsulated packet value.

Advanced configuration

Advanced

bob@debian76: ~ pfSense.localdomain ...

SAVE

Applications Raccourcis | jeu. 9 oct., 03:01 | bob

pfSense.localdomain - OpenVPN: Client - Iceweasel

File Edit View History Bookmarks Tools Help

pfSense.localdomain - OpenVP... | https://192.168.50.254/vpn_openvpn_client.php | Google

Sense | System | Interfaces | Firewall | Services | VPN | Status | Diagnostics | Gold | Help | .. 01 unread notice ..

OpenVPN: Client

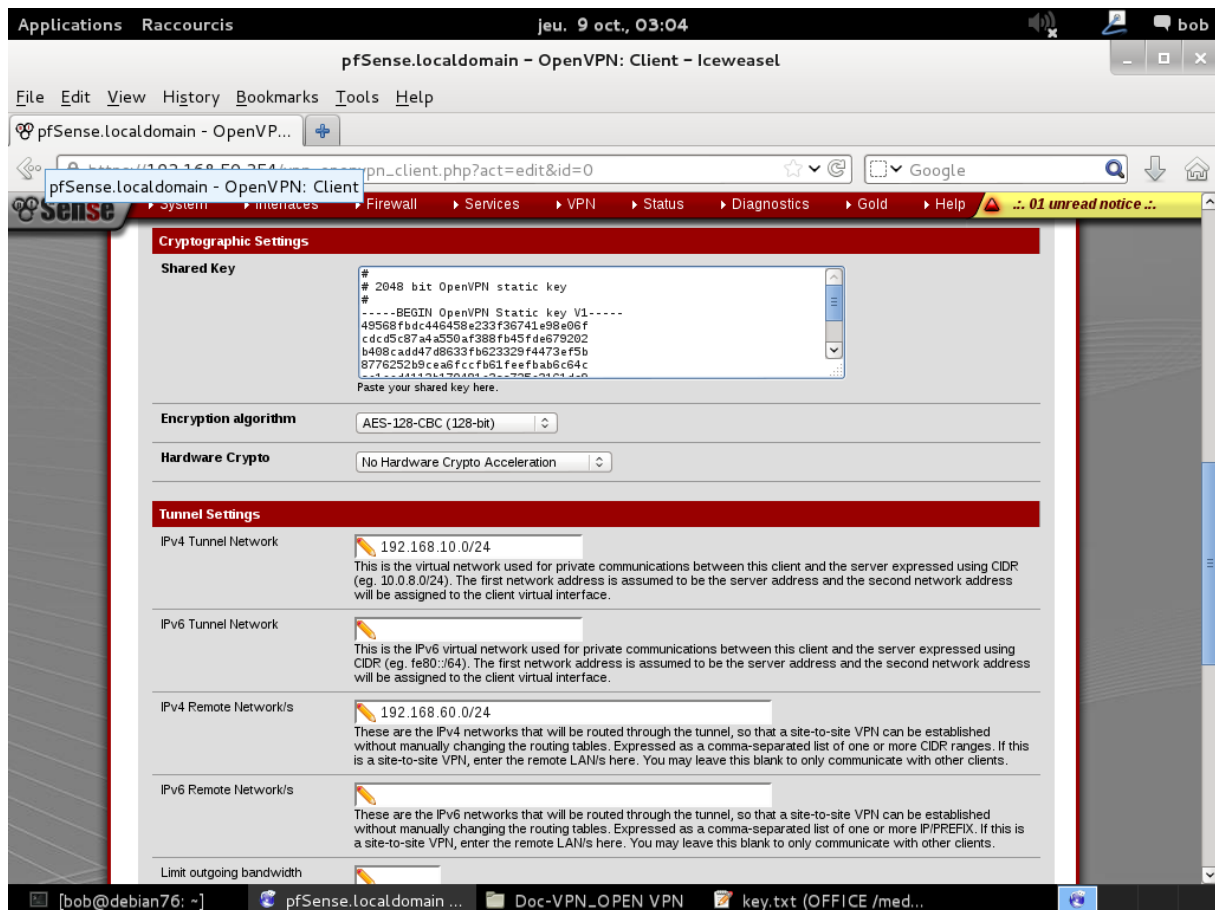
Server Client Client Specific Overrides Wizards

Disabled	Protocol	Server	Description
NO	UDP	192.168.5.28:1194	

Additional OpenVPN clients can be added here.

pfSense is © 2004 - 2014 by Electric Sheep Fencing LLC. All Rights Reserved. [view license]

bob@debian76: ~ | pfSense.localdomain ...



Coller la clé depuis le fichier sur a clé usb. Il faut que ce soit la même clé sur le client et le serveur.

8. Configuration des pare feu

SITE avec routeur R2:

From the **Firewall** menu, choose **Rules**. Open the **WAN** tab, unless using a different interface for the VPN connection. Click on the **+** button to add a new rule.

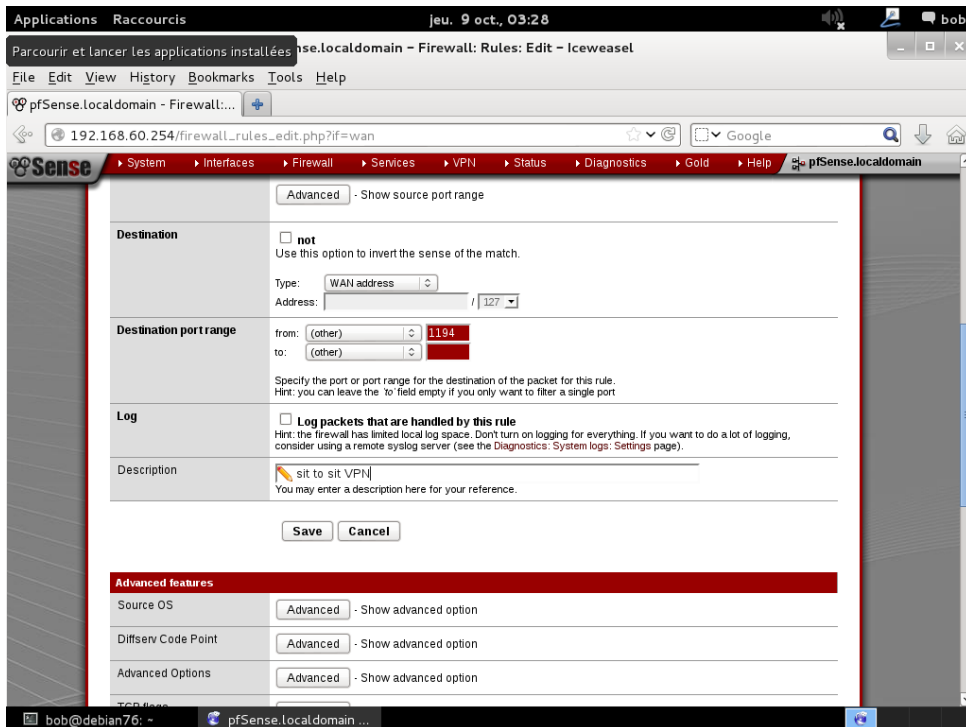
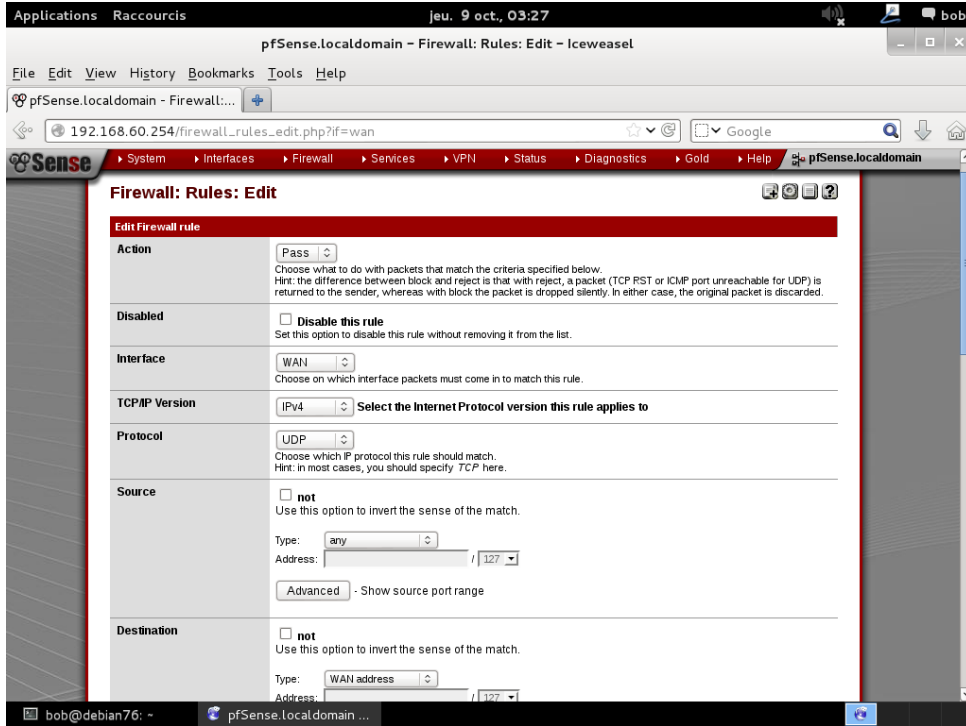
Le port utilisé par le serveur et le client openvpn est le 1194

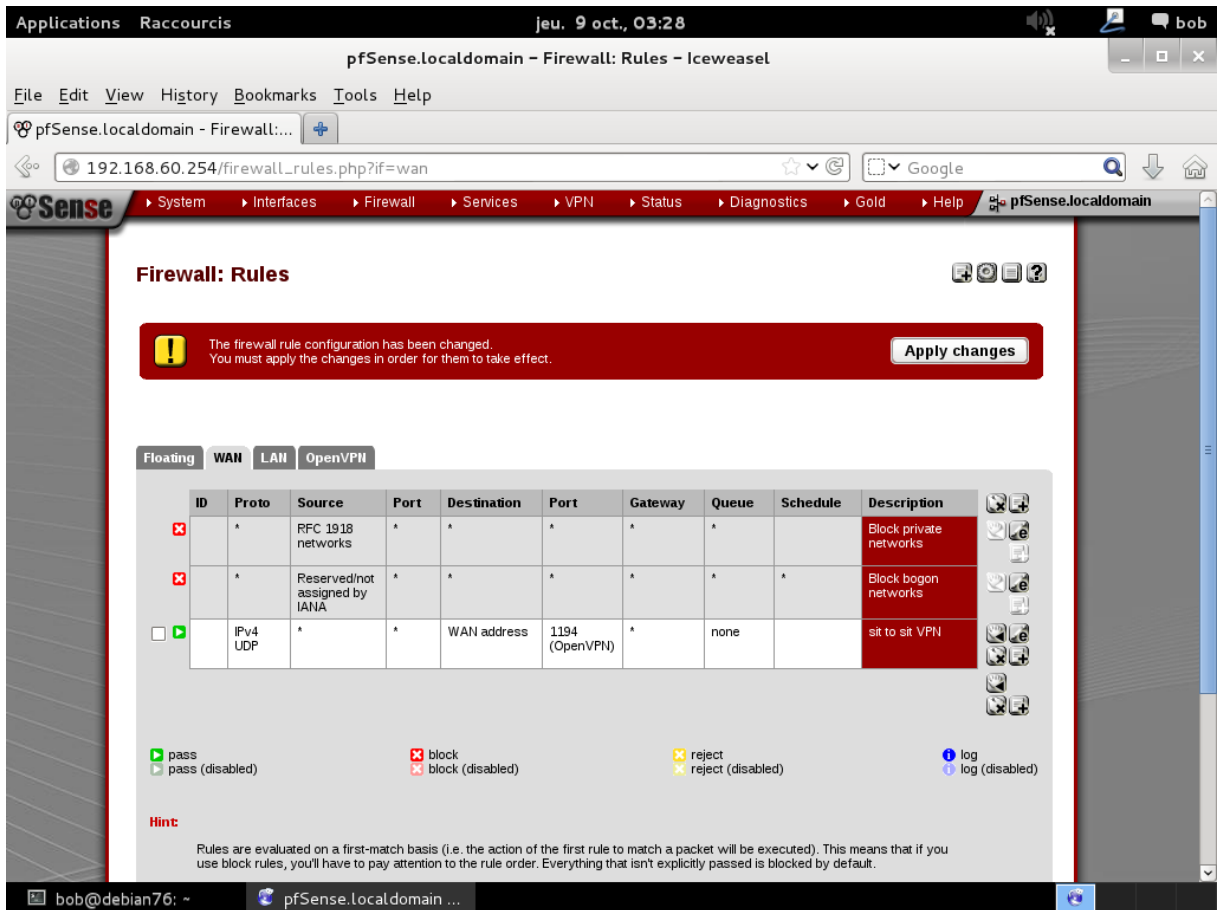
Il faut donc débloquer tout le trafic sur ce port.

Enter these values:

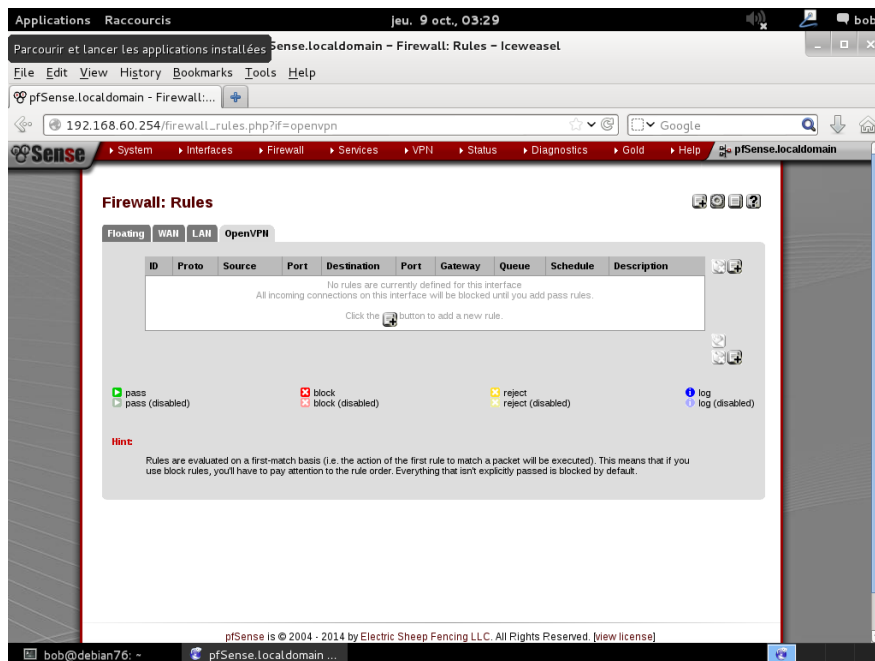
Action	Pass
Interface	WAN
TCP/IP Version	IPv4
Protocol	UDP
Source	any
Destination	Type: WAN address
Destination port range	from: (other) 1194

	to: (other)
Log	not checked
Description	Site-to-site VPN





Bouton apply changes



Onglet openvpn rajouter un role por openvpn

Enter these values:

Action	Pass
Disabled	not checked
Interface	OpenVPN
TCP/IP Version	IPv4
Protocol	any
Source	any
Destination	any
Log	not checked
Description	Allow everything through OpenVPN

Applications Raccourcis jeu. 9 oct., 03:31 bob

pfSense.localdomain - Firewall: Rules: Edit - Iceweasel

File Edit View History Bookmarks Tools Help

192.168.60.254/firewall_rules_edit.php?f=openvpn

System Interfaces Firewall Services VPN Status Diagnostics Gold Help pfSense.localdomain

Firewall: Rules: Edit

Edit Firewall rule

Action
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled **Disable this rule**
Set this option to disable this rule without removing it from the list.

Interface
Choose on which interface packets must come in to match this rule.

TCP/IP Version **Select the Internet Protocol version this rule applies to**

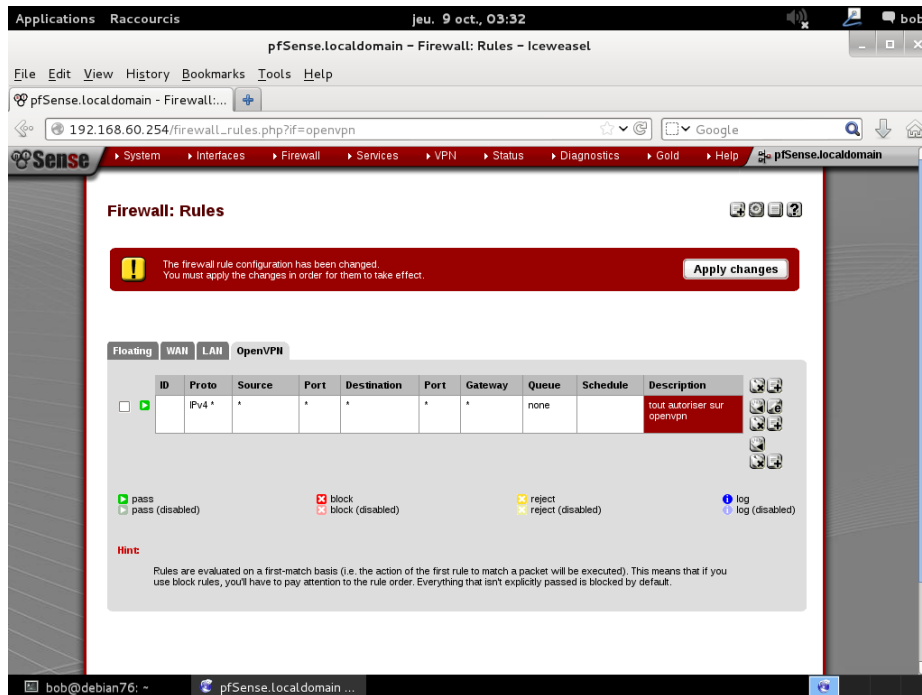
Protocol
Choose which IP protocol this rule should match.
Hint: in most cases, you should specify *TCP* here.

Source **not**
Use this option to invert the sense of the match.
Type:
Address: /

Destination **not**
Use this option to invert the sense of the match.
Type:
Address: /

Log **Log packets that are handled by this rule**

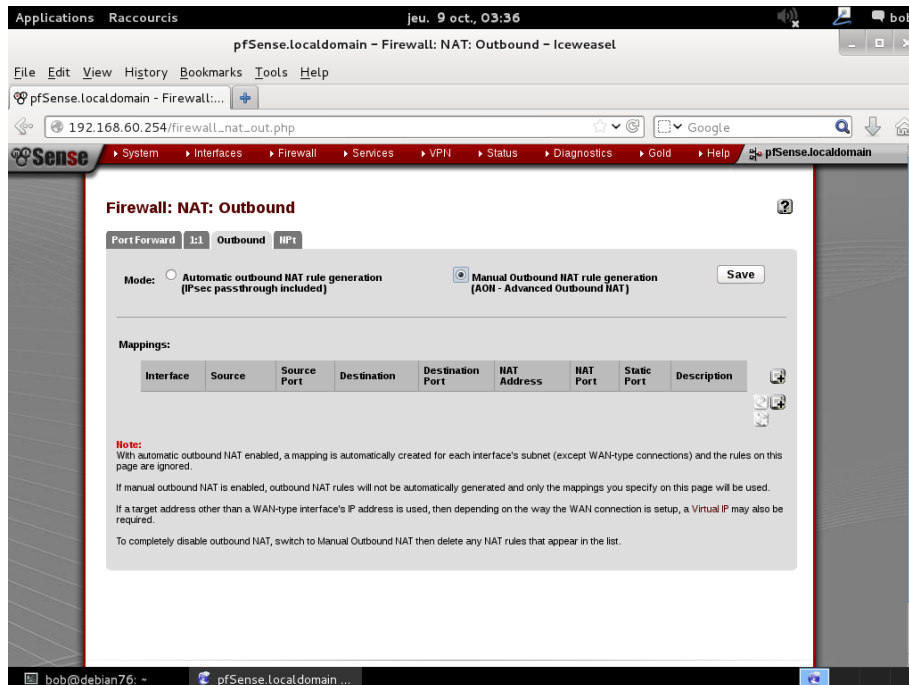
bob@debian76: ~ pfSense.localdomain ...



Bouton APPLY CHANGES

Set up outbound NAT at Site B

From the **Firewall** menu, choose **NAT** and click on the **Outbound** tab. Select **Manual Outbound NAT rule generation (AON – Advanced Outbound NAT)** and click **Save**. On the next page, click **Apply Changes**.



Save

Enter these values:

Do not NAT	not checked	
Interface	WAN	Unless using a different interface for the VPN
Protocol	any	
Source	Type: Network Address: 192.168.10.0/24 Source port: leave empty	Site A's subnet
Destination	Type: any Destination port: leave empty	
Translation	Address: Interface address Port: leave empty Static port: not checked	
No XMLRPC Sync	Leave unchecked	
Description	Site A	

Applications Raccourcis | jeu. 9 oct., 03:40 | bob

pfSense.localdomain - Firewall: NAT: Outbound: Edit - Iceweasel

File Edit View History Bookmarks Tools Help

192.168.60.254/firewall_nat_out_edit.php?after=-1

System Interfaces Firewall Services VPN Status Diagnostics Gold Help | pfSense.localdomain

Edit Advanced Outbound NAT entry

Do not NAT
Enabling this option will disable NAT for traffic matching this rule and stop processing Outbound NAT rules.
Hint: in most cases, you won't use this option.

Interface
WAN
Choose which interface this rule applies to.
Hint: in most cases, you'll want to use WAN here.

Protocol
any
Choose which protocol this rule should match.
Hint: in most cases, you should specify any here.

Source
Type: Network
Address: 192.168.10.0 / 24
Enter the source network for the outbound NAT mapping.
Source port: (leave blank for any)

not
Use this option to invert the sense of the match.

Destination
Type: any
Address: / 24
Enter the destination network for the outbound NAT mapping.
Destination port: (leave blank for any)

Translation
Address: Interface address
Packets matching this rule will be mapped to the IP address given here.
If you want this rule to apply to another IP address rather than the IP address of the interface chosen above, select it here (you will need to define Virtual IP addresses on the interface first).
Port: (leave blank for any)
Static port:

192.168.60.254/index.php | bob@debian76: ~ | pfSense.localdomain ...

9. Sauvegardes et Tests

9.1. Sauvegarde des configurations des routeurs

9.2. Arrêt des routeurs

R1 : "Halt" pour arreter R1

Reboot de R2 (c'est le serveur qui dot être en écoute quand le client va tenter de se connecter)


10. Consultation des log (notamment en cas de problèmes)

10.1. LOG du pare feu

The screenshot shows the pfSense web interface for 'Status: System logs: Firewall'. A red menu is open over the log table, highlighting 'System Logs'. The log table displays the following entries:

Act	Time	If	Source	Destination	Protocol	Quantity
✗	Jan 27 10:06:20	WAN	192.168.5.27:60464	192.168.5.28:1194	UDP	1
✗	Jan 27 10:06:21	WAN	192.168.5.27:60464	192.168.5.28:1194	UDP	1
✗	Jan 27 10:06:22	WAN	192.168.5.27:60464	192.168.5.28:1194	UDP	1
✗	Jan 27 10:06:23	WAN	192.168.5.27:60464	192.168.5.28:1194	UDP	1
✗	Jan 27 10:06:24	WAN	192.168.5.27:60464	192.168.5.28:1194	UDP	1
✗	Jan 27 10:06:25	WAN	192.168.5.27:60464	192.168.5.28:1194	UDP	1
✗	Jan 27 10:06:25	WAN	192.168.5.27:60464	192.168.5.28:1194	UDP	1
✗	Jan 27 10:06:26	WAN	192.168.5.27:60464	192.168.5.28:1194	UDP	1
✗	Jan 27 10:06:27	WAN	192.168.5.27:60464	192.168.5.28:1194	UDP	1
✗	Jan 27 10:06:28	WAN	192.168.5.27:60464	192.168.5.28:1194	UDP	1
✗	Jan 27 10:06:29	WAN	192.168.5.27:60464	192.168.5.28:1194	UDP	1
✗	Jan 27 10:06:30	WAN	192.168.5.27:60464	192.168.5.28:1194	UDP	1

Ci-dessus au niveau du pare feu du routeur R2, on voit bien que les paquets venant de 192.168.5.27 port UDP 60464 (cad R1) à destination de 192.168.5.28 port UDP 1194 (cad le serveur openVPN de R2) sont bloqués ! la connexion VPN ne peut donc pas s'établir.

On peut cliquer sur l'icône  juste avant 192.168.5.28:1194 pour créer un règle "easy Rule" :

Applications Raccourcis jeu. 9 oct., 05:06 bob

pfSense.localdomain - Firewall: Rules - Iceweasel

File Edit View History Bookmarks Tools Help

192.168.60.254/firewall_rules.php?if=wan

System Interfaces Firewall Services VPN Status Diagnostics Gold Help pfSense.localdomain

Firewall: Rules

The firewall rule configuration has been changed. You must apply the changes in order for them to take effect. **Apply changes**

Floating WAN LAN OpenVPN

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input checked="" type="checkbox"/>	*	RFC 1918 networks	*	*	*	*	*	*	Block private networks
<input checked="" type="checkbox"/>	*	Reserved/not assigned by IANA	*	*	*	*	*	*	Block bogon networks
<input type="checkbox"/>	IPv4 UDP	192.168.5.27	*	WAN address	1194 (OpenVPN)	*	none		sit to sit VPN
<input type="checkbox"/>	IPv4 UDP	192.168.5.27	*	192.168.5.28	1194 (OpenVPN)	*	none		Easy Rule: Passed from Firewall Log View

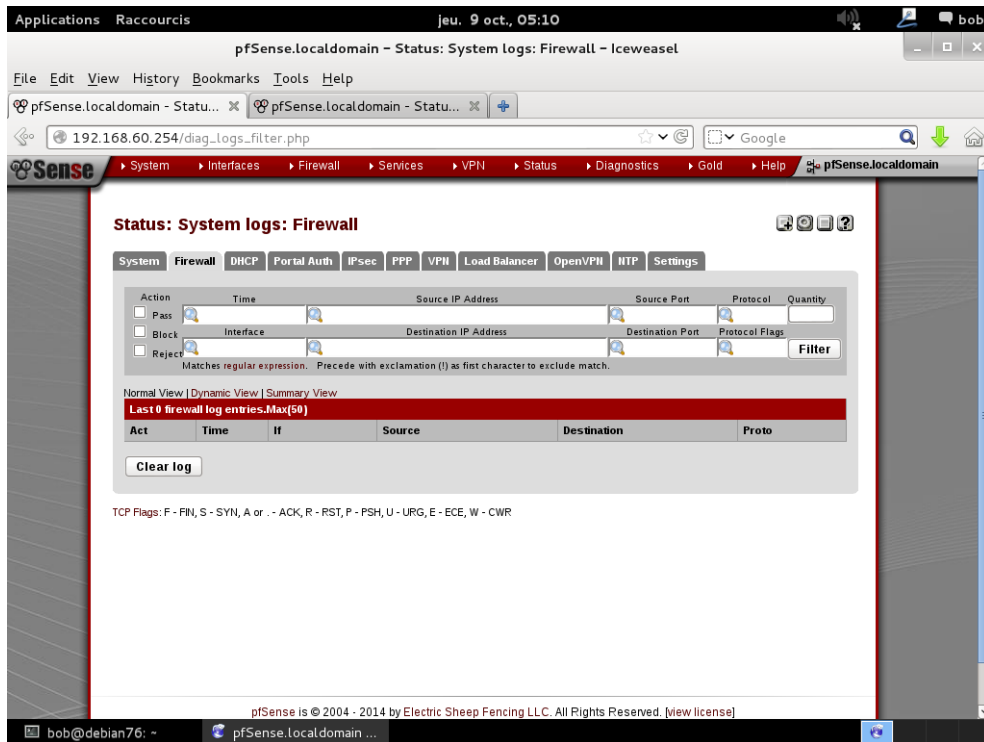
pass
 pass (disabled)
 block
 block (disabled)
 reject
 reject (disabled)
 log
 log (disabled)

bob@debian76: ~ pfSense.localdomain ...

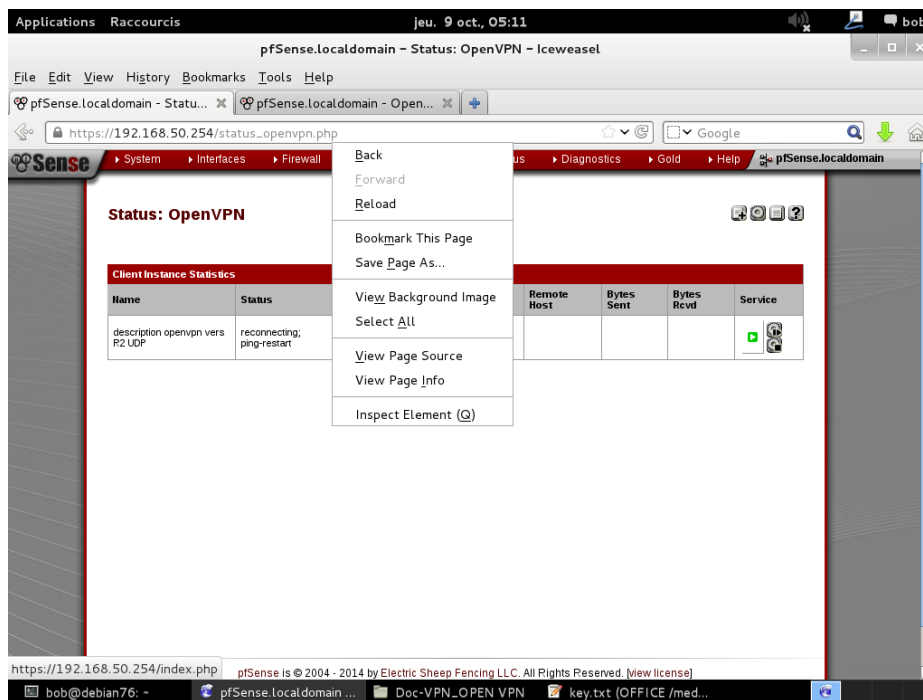
On voit bien que la nouvelle règle ainsi créée accepte tous les datagrammes UDP provenant de l'IP source 192.168.5.27 (R1) à destination de 192.168.5.28 (R2) port UDP 1194

Bouton "Apply changes"

⇒ Sur R2 faire un clear log au niveau du firewall :



⇒ Sur R1 , status d'openvpn redémarrer openvpn

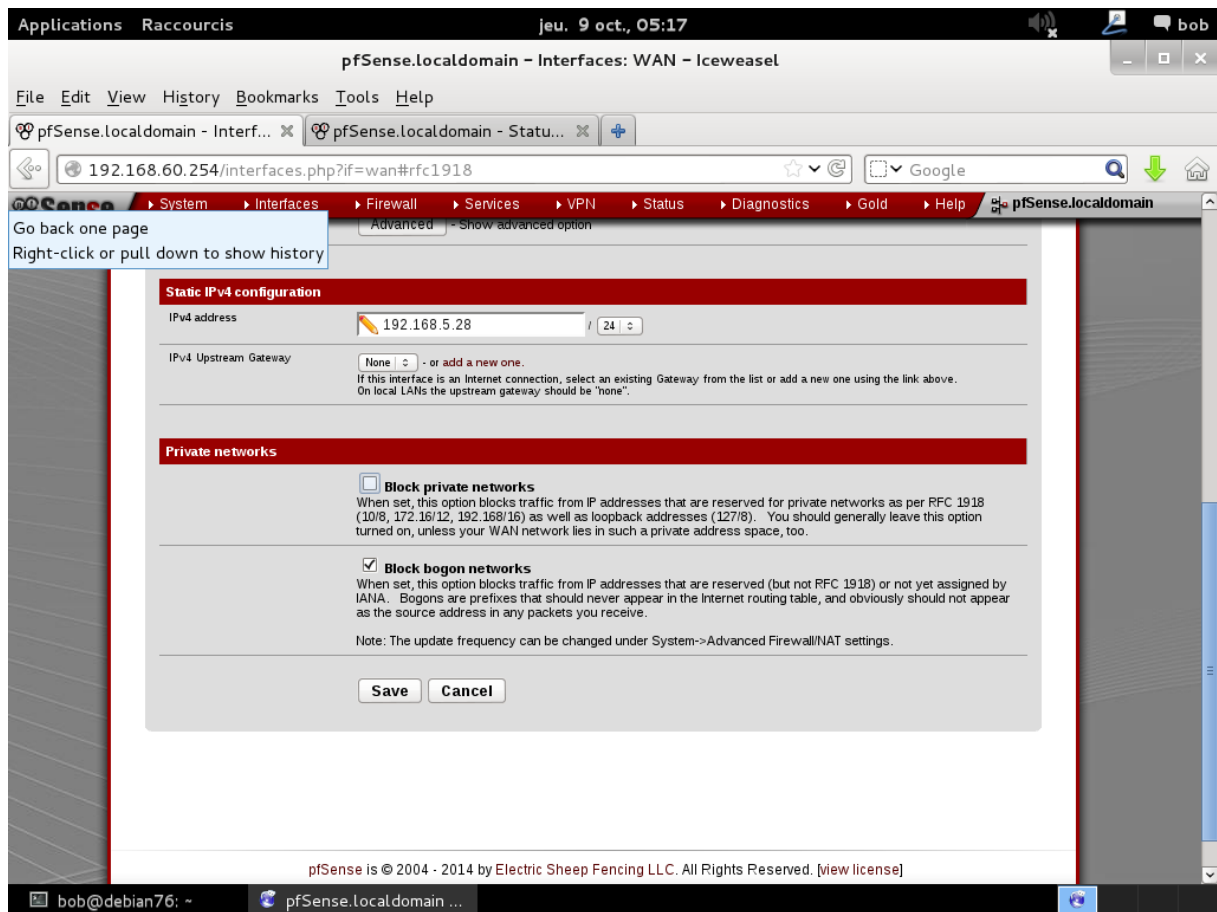


⇒ Sur R2 vérifier les lig du parefeu pour voir si ça bloque toujours ou pas.

10.2. Problème des adresses privées

Menu "Interface WAN"

Il faut désactiver "Block private network"



Du coup il y a une règle du pare feu qui a été enlevée

Menu Firewall → rule

Applications Raccourcis | jeu. 9 oct., 05:22 | bob

pfSense.localdomain - Firewall: Rules - Iceweasel

File Edit View History Bookmarks Tools Help

192.168.60.254/firewall_rules.php

System Interfaces Firewall Services VPN Status Diagnostics Gold Help pfSense.localdomain

Firewall: Rules

Floating WAN LAN OpenVPN

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input checked="" type="checkbox"/>	*	Reserved/not assigned by IANA	*	*	*	*	*	*	Block bogon networks
<input type="checkbox"/>	IPv4 UDP	192.168.5.27	*	WAN address	1194 (OpenVPN)	*	none		sit to sit VPN

pass
 pass (disabled)

 block
 block (disabled)

 reject
 reject (disabled)

 log
 log (disabled)

Hint:
 Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.

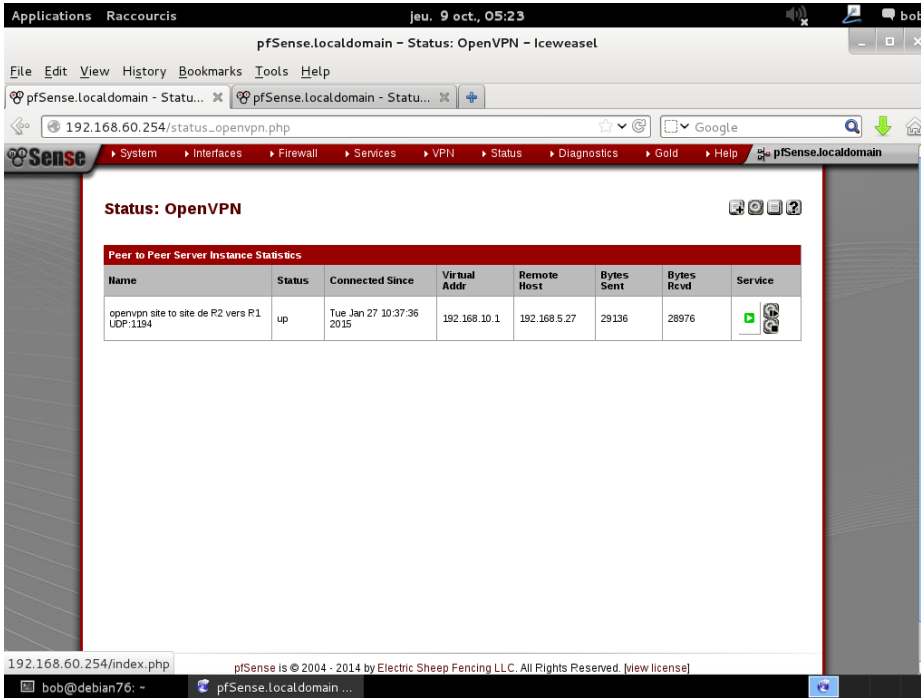
pfSense is © 2004 - 2014 by Electric Sheep Fencing LLC. All Rights Reserved. [view license]

bob@debian76: ~ | pfSense.localdomain ...

10.3. LOG openVPN

SUR R2 Menu status → openvpn

Le VPN est bien connecté !

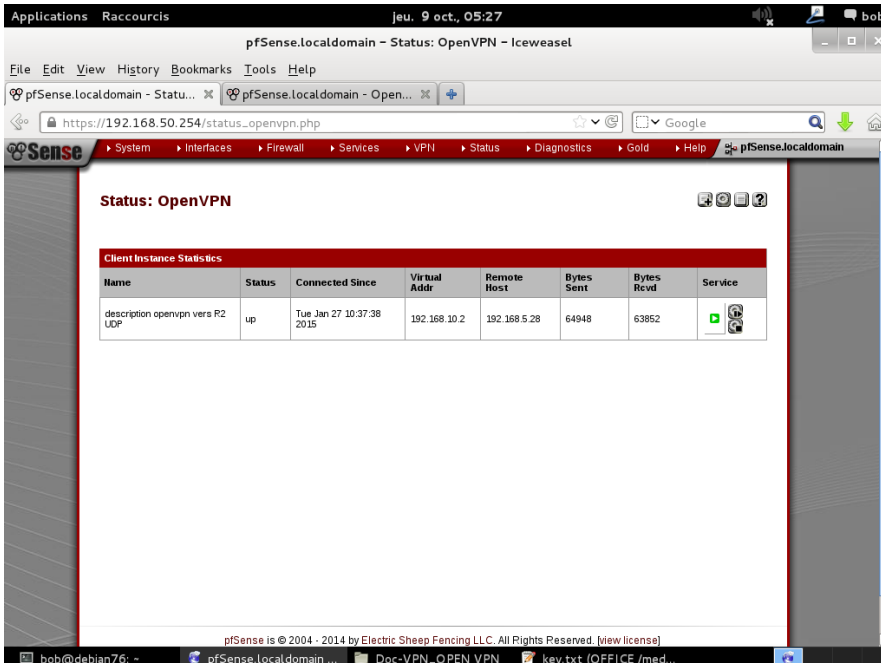


The screenshot shows the pfSense web interface for SUR R2. The browser address bar displays `192.168.60.254/status_openvpn.php`. The page title is "Status: OpenVPN". The main content area is titled "Peer to Peer Server Instance Statistics" and contains a table with the following data:

Name	Status	Connected Since	Virtual Addr	Remote Host	Bytes Sent	Bytes Rcvd	Service
openvpn site to site de R2 vers R1 UDP:1194	up	Tue Jan 27 10:37:36 2015	192.168.10.1	192.168.5.27	29136	28976	

SUR R1 menu status → openvpn

Le VPN est bien connecté !



The screenshot shows the pfSense web interface for SUR R1. The browser address bar displays `https://192.168.50.254/status_openvpn.php`. The page title is "Status: OpenVPN". The main content area is titled "Client Instance Statistics" and contains a table with the following data:

Name	Status	Connected Since	Virtual Addr	Remote Host	Bytes Sent	Bytes Rcvd	Service
description openvpn vers R2 UDP	up	Tue Jan 27 10:37:38 2015	192.168.10.2	192.168.5.28	64948	63852	

Sur R2 Menu status → system log

The screenshot shows the pfSense web interface. At the top, the system status bar indicates the date and time as 'jeu. 9 oct., 05:25'. The browser window title is 'pfSense.localdomain - Status: System logs: OpenVPN - Iceweasel'. The address bar shows the URL '192.168.60.254/diag_logs_openvpn.php'. The navigation menu includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The main content area is titled 'Status: System logs: OpenVPN' and features a tabbed interface with 'OpenVPN' selected. Below the tabs, a table displays the 'Last 50 OpenVPN log entries'. The table contains two entries for January 27, 2014, at 10:37:36, showing a peer connection initiated and the initialization sequence completed. A 'Clear log' button is located below the table. The footer of the page states 'pfSense is © 2004 - 2014 by Electric Sheep Fencing LLC. All Rights Reserved. [view license]'. The system tray at the bottom shows the user 'bob@debian76' and the local domain 'pfSense.localdomain'.

Applications Raccourcis jeu. 9 oct., 05:25 bob

pfSense.localdomain - Status: System logs: OpenVPN - Iceweasel

File Edit View History Bookmarks Tools Help

pfSense.localdomain - Statu... x pfSense.localdomain - Statu... x +

192.168.60.254/diag_logs_openvpn.php Google

pfSense

System Interfaces Firewall Services VPN Status Diagnostics Gold Help pfSense.localdomain

Status: System logs: OpenVPN

System Firewall DHCP Portal Auth IPsec PPP VPN Load Balancer **OpenVPN** NTP Settings

Last 50 OpenVPN log entries

Jan 27 10:37:36	openvpn[13972]: Peer Connection Initiated with [AF_INET]192.168.5.27:55076
Jan 27 10:37:36	openvpn[13972]: Initialization Sequence Completed

Clear log

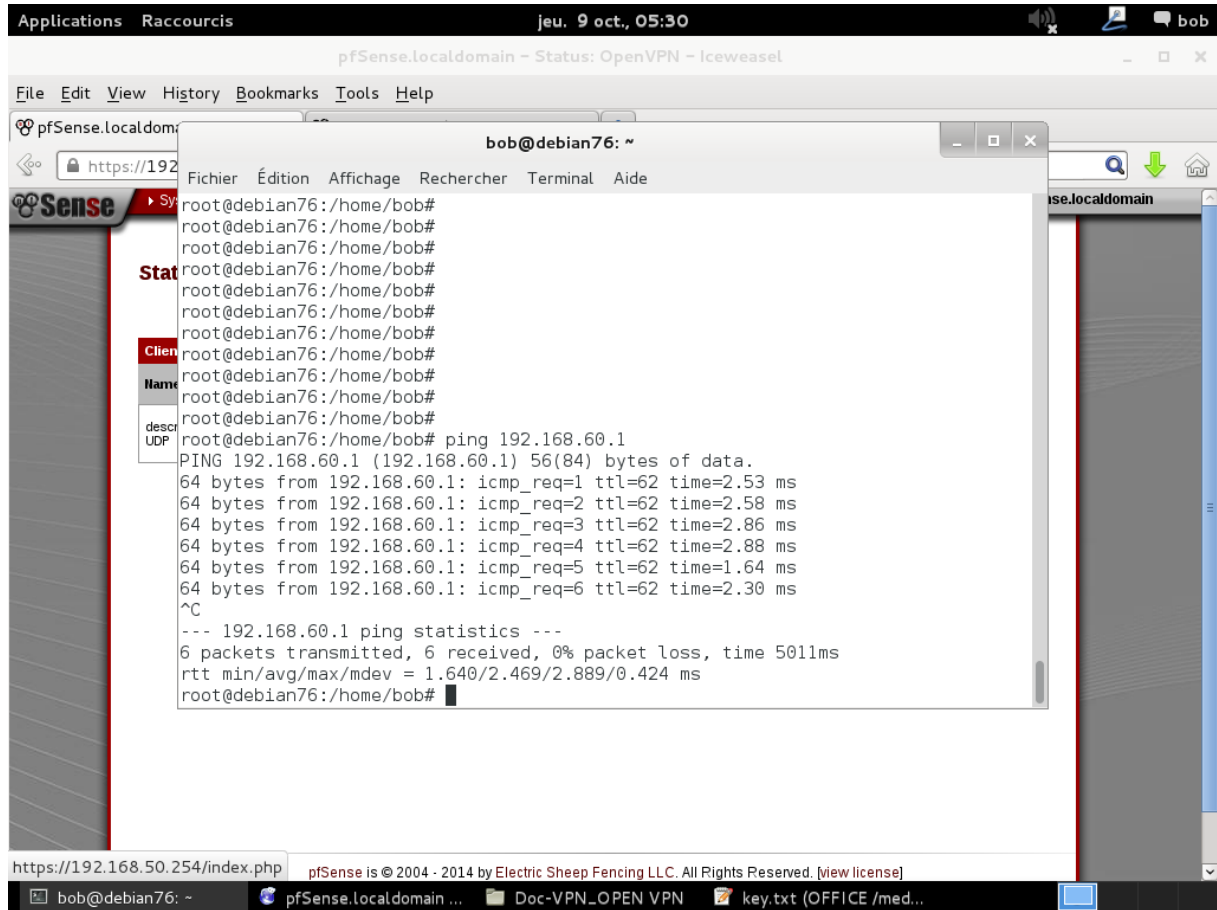
pfSense is © 2004 - 2014 by Electric Sheep Fencing LLC. All Rights Reserved. [view license]

bob@debian76: ~ pfSense.localdomain ...

11. TEST du VPN

11.1. Test de ping

Depuis le poste P1 (ip 192.168.50.1) du LAN de R1 : ping 192.168.60.1

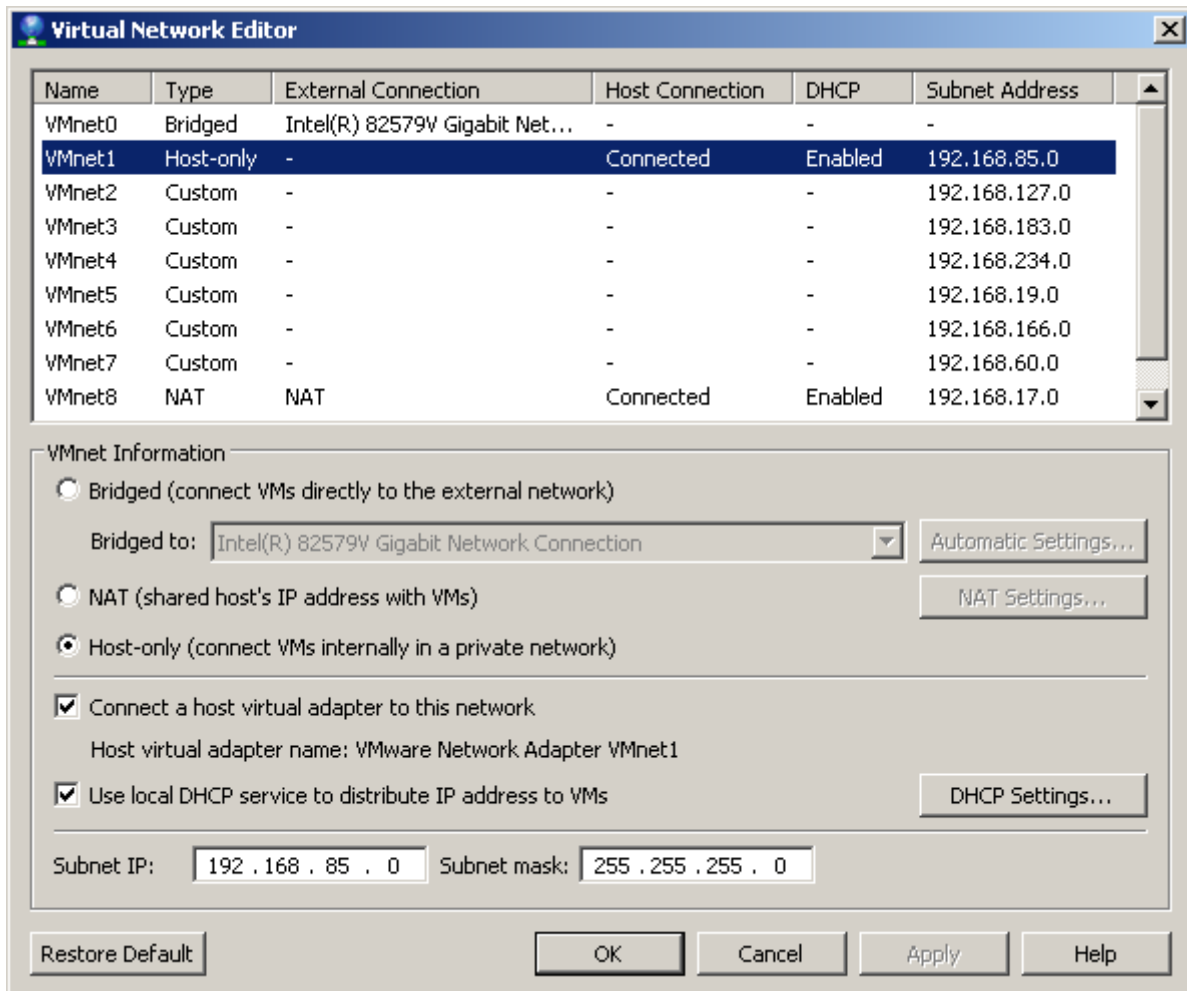


11.2. Capture de trame

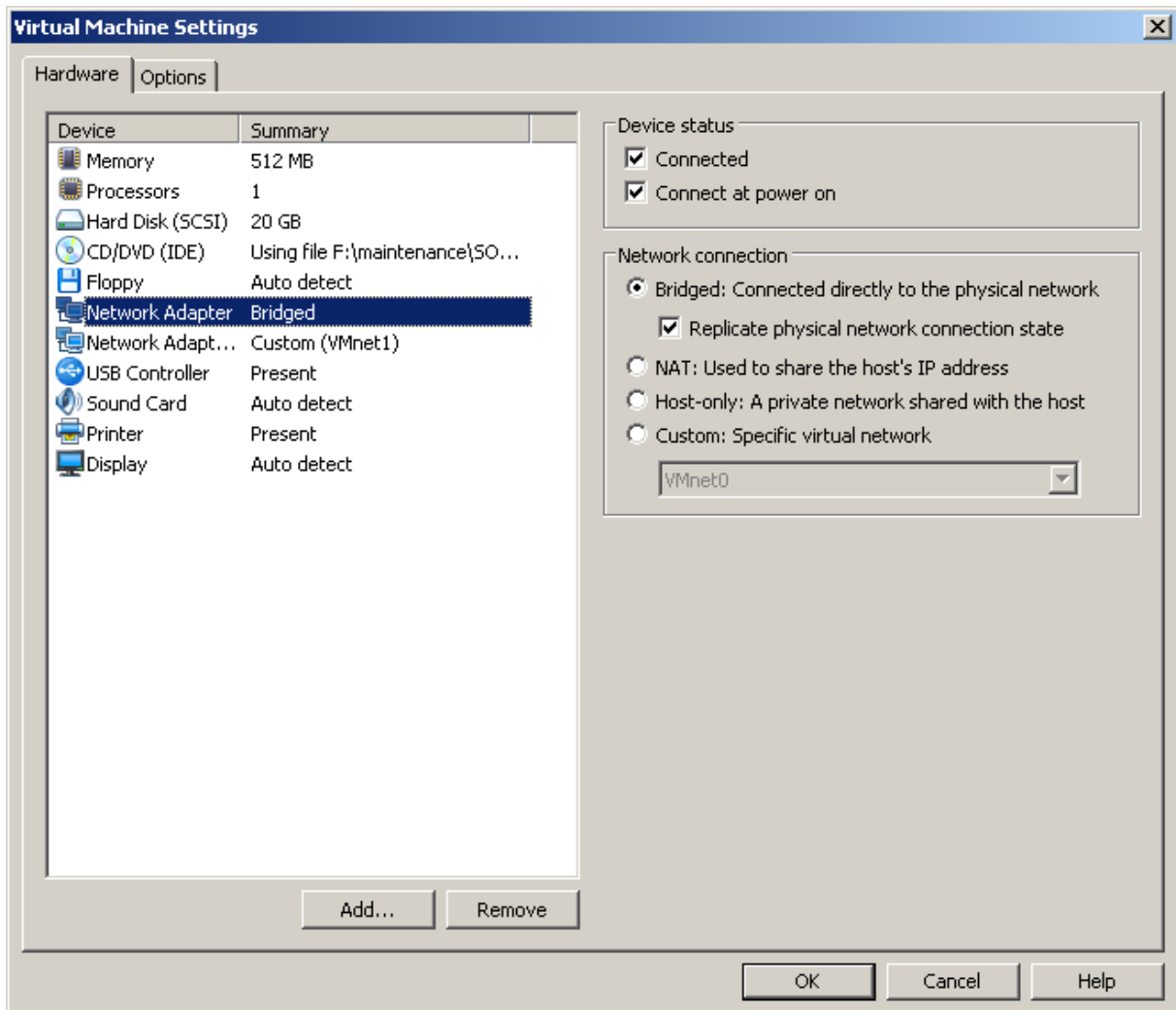
Essayer de capturer les trames liées à la connexion openvpn site à site ainsi créée.

Si vous n'arrivez pas à capturer les trames (à cause de vmware notamment) , Essayer de connecter un vpn site à site avec votre voisin et tenter de capturer les trames

On a configuré les cartes réseau des postes et les routeurs côté LAN en mode "host-only" sous vmware workstation



On va donc réalisé une capture de trame au niveau de cette interface VMnet1



Configuration vmware workstation du routeur 1.

Capture d'un ping entre les 2 PCs . ping 192.168.60.1 depuis le poste 192.168.50.1 en passant par le VPN entre les routeurs:

99	61.62423400(192.168.50.1)	192.168.60.1	ICMP	98	Echo (ping) request	id=0x0d48, seq=10/2560, ttl=62 (reply in 100)
100	61.62465300(192.168.60.1)	192.168.50.1	ICMP	98	Echo (ping) reply	id=0x0d48, seq=10/2560, ttl=64 (request in 99)

```
No.    Time      Source      Destination  Protocol Length Info
  99 61.624234000 192.168.50.1 192.168.60.1  ICMP    98    Echo (ping) request
id=0x0d48, seq=10/2560, ttl=62 (reply in 100)
```

```
Frame 99: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: Vmware_b2:01:74 (00:0c:29:b2:01:74), Dst: Vmware_5d:23:7b (00:0c:29:5d:23:7b)
Internet Protocol Version 4, Src: 192.168.50.1 (192.168.50.1), Dst: 192.168.60.1 (192.168.60.1)
Internet Control Message Protocol
```

```
No.    Time      Source      Destination  Protocol Length Info
 100 61.624653000 192.168.60.1 192.168.50.1  ICMP    98    Echo (ping) reply
id=0x0d48, seq=10/2560, ttl=64 (request in 99)
```

```
Frame 100: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: Vmware_5d:23:7b (00:0c:29:5d:23:7b), Dst: Vmware_b2:01:74 (00:0c:29:b2:01:74)
Internet Protocol Version 4, Src: 192.168.60.1 (192.168.60.1), Dst: 192.168.50.1 (192.168.50.1)
```

Internet Control Message Protocol

⇒ Pour les postes le VPN est transparent (ils ne voient pas que les données sont cryptées)

Réalisons maintenant une capture sur le côté WAN entre les 2 routeurs. Le plus simple est de réaliser cette capture depuis l'interface WAN d'un des routeurs (tout en laissant la ping continuer entre les 2 postes) :

Menu Diagnostic → packet capture → coté WAN → (parametres par défaut) → START

Applications Raccourcis jeu. 9 oct., 11:14 bob

Parcourir et lancer les applications installées localdomain - Diagnostics: Packet Capture - Iceweasel

File Edit View History Bookmarks Tools Help

192.168.60.254/diag_packet_capture.php

pfSense.localdomain - Diagn... pfSense.localdomain - Statu...

System Interfaces Firewall Services VPN Status Diagnostics Gold Help pfSense.localdomain

Note: This option does not affect the level of detail when downloading the packet capture.

Reverse DNS Lookup

This check box will cause the packet capture to perform a reverse DNS lookup associated with all IP addresses.
Note: This option can cause delays for large packet captures.

Start View Capture Download Capture

The packet capture file was last updated: January 27th, 2015 4:28:31 pm.

Packet Capture stopped.

Packets Captured:

```
16:28:16.646387 IP 192.168.5.28.1194 > 192.168.5.27.58433: UDP, length 132
16:28:16.930016 IP 192.168.5.27.58433 > 192.168.5.28.1194: UDP, length 132
16:28:16.931430 IP 192.168.5.28.1194 > 192.168.5.27.58433: UDP, length 132
16:28:17.646386 IP 192.168.5.28.1194 > 192.168.5.27.58433: UDP, length 132
16:28:17.717313 IP 192.168.5.248.17500 > 255.255.255.255.17500: UDP, length 280
16:28:17.724358 IP 192.168.5.248.17500 > 255.255.255.255.17500: UDP, length 280
16:28:17.724423 IP 192.168.5.248.17500 > 255.255.255.255.17500: UDP, length 280
16:28:17.725124 IP 192.168.5.248.17500 > 255.255.255.255.17500: UDP, length 280
16:28:17.726700 IP 192.168.5.248.17500 > 192.168.5.255.17500: UDP, length 280
16:28:17.931748 IP 192.168.5.27.58433 > 192.168.5.28.1194: UDP, length 132
16:28:17.932755 IP 192.168.5.28.1194 > 192.168.5.27.58433: UDP, length 132
16:28:18.646460 IP 192.168.5.28.1194 > 192.168.5.27.58433: UDP, length 132
16:28:18.934552 IP 192.168.5.27.58433 > 192.168.5.28.1194: UDP, length 132
16:28:18.935569 IP 192.168.5.28.1194 > 192.168.5.27.58433: UDP, length 132
16:28:19.646740 IP 192.168.5.28.1194 > 192.168.5.27.58433: UDP, length 132
16:28:19.937754 IP 192.168.5.27.58433 > 192.168.5.28.1194: UDP, length 132
```

pfSense is © 2004 - 2014 by Electric Sheep Fencing LLC. All Rights Reserved. [view license]

bob@debian76: ~ pfSense.localdomain ... bob@debian76: ~

"Download capture" pour l'enregistrer (sur clé usb) puis l'ouvrir dans wireshark.

