

# Pfsense - OpenVPN & Captive Portal

Grégoire Roumache

Mars 2021

## 1 Installations & Configurations

### 1.1 Configuration internet explorer - windows server

Pour pouvoir configurer pfsense àpd internet explorer, il faut:

1. ouvrir le *server manager*
2. dans le menu de gauche, cliquer sur *local server*
3. au centre à droite, cliquer sur *On* à droite de *IE Enhanced Security Configuration*
4. désactiver la sécurité (cliquer sur *off* pour les 2 paramètres), puis cliquer sur *ok*

**Remarque:** si internet explorer était ouvert, il faut le fermer puis le rouvrir pour que le changement ait lieu.

### 1.2 Installation active directory - windows server

**Attention !** Il faut configurer la machine windows serveur en ip statique, avec le DNS = 127.0.0.1.

1. ouvrir le *server manager*
2. en haut à droite, cliquer sur *manage*, puis sur *add roles and features*
3. à gauche dans *server roles*, sélectionner *active directory domain services*
4. cliquer sur *add features* dans la popup, puis continuer jusqu'à l'installation
5. quand un signe danger apparaît en haut à droite, cliquer dessus
6. cliquer sur *promote this server to a domain controller*
7. sélectionner l'option *add a new forest*, et ajouter le nom de domaine (ex: *domaine.local*)
8. ensuite, ajouter le mot de passe DSRM: *Tigrou007*, et terminer la configuration

### 1.3 Créer un groupe d'utilisateurs sur active directory - windows server

- Ajouter un groupe d'utilisateurs:
  1. dans le *server manager*, cliquer sur *tools* en haut à droite
  2. ouvrir *active directory users and computers*
  3. faire un clic-droit sur *<domaine>/users*, puis cliquer sur *new*, puis sur *group*
  4. compléter le formulaire
- Ajouter des utilisateurs à un groupe:
  1. dans le *server manager*, cliquer sur *tools* en haut à droite
  2. ouvrir *active directory users and computers*

3. faire un clic-droit sur *<domaine>/users*, puis cliquer sur *new*, puis sur *group*
- Ajouter des utilisateurs:
  1. dans le *server manager*, cliquer sur *tools* en haut à droite
  2. ouvrir *active directory users and computers*
  3. cliquer sur *<domaine>/users*, faire un clic-droit sur le groupe, puis cliquer sur *properties*
  4. dans l'onglet *members*, cliquer sur *add*
  5. écrire les noms des utilisateurs à ajouter, cliquer sur *check names*, puis *ok*

## 1.4 Installer et configurer RADIUS - windows server





**Attention !** Il faut que le parefeu soit désactivé pour que ça fonctionne correctement.

- Installer RADIUS:
  1. ouvrir le *server manager*
  2. en haut à droite, cliquer sur *manage*, puis sur *add roles and features*
  3. à gauche dans *server roles*, sélectionner *network policy and access services*
  4. cliquer sur *add features* dans la popup, puis continuer jusqu'à l'installation
  5. continuer et installer le service
- Configurer RADIUS:
  1. dans le *server manager*, cliquer sur *tools* en haut à droite
  2. ouvrir *network policy server*
  3. dans le menu de gauche, faire un clic gauche sur *radius clients and servers/radius clients*
  4. cliquer sur *new*, et compléter le formulaire:
    - Friendly name = VPN pfsense (pas d'impact sur le fonctionnement)
    - Address (IP or DNS) = IP du parefeu pfsense
    - Shared secret template = None
    - Manual/Generate = Generate
    - Shared secret  $\Rightarrow$  cliquer sur *generate*

**Remarque:** copier le secret partagé dans un fichier texte, pour l'ajouter au parefeu plus tard.

  5. cliquer sur *ok*
  6. dans le menu de gauche, faire un clic gauche sur *policies/network policies*
  7. cliquer sur *new*, et ajouter un nom (ex: *allow pfsense*), puis cliquer sur *next*
  8. cliquer sur *add*, sélectionner *windows groups*, puis cliquer sur *add*
  9. cliquer sur *add groups*, taper le nom du groupe (ex: *VPNusers*)
  10. cliquer sur *check names*, puis sur *ok*, encore sur *ok*, puis sur *next*
  11. sélectionner *access granted*, puis cliquer sur *next*
  12. dans *configure authentication method*, sélectionner uniquement *MS-CHAP-v2*
  13. cliquer 3 fois sur *next*, puis sur *finish*

**Remarque:** il faut que la stratégie créée ait un *processing order* plus petit que les autres pour que le trafic ne soit pas bloqué.

Network Policies					
 Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.					
Policy Name	Status	Processing Order	Access Type	S	
 allow pfsense	Enabled	1	Grant Acce...	U	
 Connections to Microsoft Routing and Remote Access server	Enabled	999998	Deny Access	U	
 Connections to other access servers	Enabled	999999	Deny Access	U	

## 1.5 Configuration routeur - routeur debian

Pour transformer la machine debian en routeur, il faut décommenter la ligne suivante dans `/etc/sysctl.conf`:

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

Remarque: il faut ajouter des default gateways/routes statiques sur toutes les machines.

## 1.6 Configuration de base - pfsense

```
Starting CRON... done.
pfSense 2.5.0-RELEASE amd64 Tue Feb 16 08:56:29 EST 2021
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 3fe8c15be287cd9654c2

*** Welcome to pfSense 2.5.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24
GUEST (opt1)   -> em2      -> v4: 10.0.0.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 
```

Il faut configurer pour avoir comme sur l'image, pour cela:

1. aller dans l'option 1 - mettre les interfaces dans le réseau auxquelles elles appartiennent (wan, lan, guest/opt1)
2. ne pas créer de vlans
3. aller dans l'option 2 - mettre em0 en dhcp, le reste en statique
4. désactiver l'ipv6
5. mettre non à "do you want to revert to http as the webconfigurator protocol?"

## 1.7 Configuration parefeu nat - pfsense

1. ouvrir l'interface web de pfsense
2. aller sur *firewall/nat/outbound*
3. sélectionner le mode *automatic outbound nat rule generation* et enregistrer

## 1.8 Configuration parefeu règles - pfsense

1. ouvrir l'interface web de pfsense
2. aller sur *firewall/rules/guest* ou sur *firewall/rules/wan*
3. cliquer sur *add* pour ajouter une nouvelle règle
4. modifier les protocoles et les sources/destinations autorisées

5. enregistrer et appliquer la nouvelle règle

**Attention!**

- Il faut que le firewall **et les routes** soient bien configurées pour que les manip fonctionnent.
- Si l'interface WAN est connectée à un réseau privé (10/8, 172.16/12, 192.168/16), il faut désactiver la règle qui bloque ce trafic.

## 1.9 Configuration routes statiques - pfsense

**Attention!** Il faut que le firewall **et les routes** soient bien configurées pour que les manip fonctionnent.

1. ouvrir l'interface web de pfsense
2. aller sur *system/routing/static routes*
3. cliquer sur *add*, puis ajouter le réseau, le masque
4. enregistrer et appliquer la nouvelle route

## 1.10 Certificats (CA, CR, import, export) - pfsense

- Créer une CA (= certificate authority):
  1. ouvrir l'interface web de pfsense
  2. aller sur *system/certificate manager/ca*
  3. rentrer un nom pour la CA (ex: *server-ca*)
  4. sélectionner la méthode *create an internal certificate authority*
  5. enregistrer la CA

**Remarque:** il ne peut y avoir qu'une CA pour toute l'infra - à moins de faire des CA intermédiaires mais on ne fait pas ça dans le cours.

- Créer un certificat:
  1. ouvrir l'interface web de pfsense
  2. aller sur *system/certificate manager/certificates*
  3. cliquer sur *add*, puis sélectionner la méthode *create an internal certificate*
  4. donner un nom au certificat, sélectionner la bonne CA
  5. dans *common name*, donner le nom du site sur lequel le certificat va aller (ex: *siteA*)
  6. dans *certificate type*, sélectionner *user certificate*
  7. dans *alternative names*, sélectionner *fqdn or hostname* et ajouter le nom du site sur lequel le certificat va aller (ex: *siteA*)
- Exporter un certificat/une clé:
  1. ouvrir l'interface web de pfsense
  2. aller sur *system/certificate manager/certificates*
  3. cliquer sur un de ces boutons:










System / Certificate Manager / Certificates

CA's Certificates Certificate Revocation

Search

Search term  Both

Enter a search string or \*nix regular expression to search certificate names and distinguished names.

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (603aad2894bb1) Server Certificate CA: No Server: Yes	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-603aad2894bb1 Valid From: Sat, 27 Feb 2021 20:35:52 +0000 Valid Until: Fri, 01 Apr 2022 20:35:52 +0000	webConfigurator Captive Portal	  
Server-CR Server Certificate CA: No Server: Yes	Server-CA	CN=10.0.2.17 Valid From: Mon, 12 Apr 2021 07:53:03 +0000 Valid Until: Thu, 10 Apr 2031 07:53:03 +0000	OpenVPN Server	  
Client-CR User Certificate CA: No Server: No	Server-CA	CN=10.0.2.15 Valid From: Mon, 12 Apr 2021 07:54:01 +0000 Valid Until: Thu, 10 Apr 2031 07:54:01 +0000		  

**Remarque:** il faut exporter le certificat de la CA et la clé + le certificat pour chaque client.

- Importer un certificat:
  1. ouvrir l'interface web de pfsense
  2. aller sur *system/certificate manager/certificates*
  3. cliquer sur *add*, puis sélectionner la méthode *import an existing certificate*
  4. donner un nom au certificat, puis copier les données du certificat et enregistrer le certificat

## 1.11 Ajouter RADIUS dans pfsense - pfsense

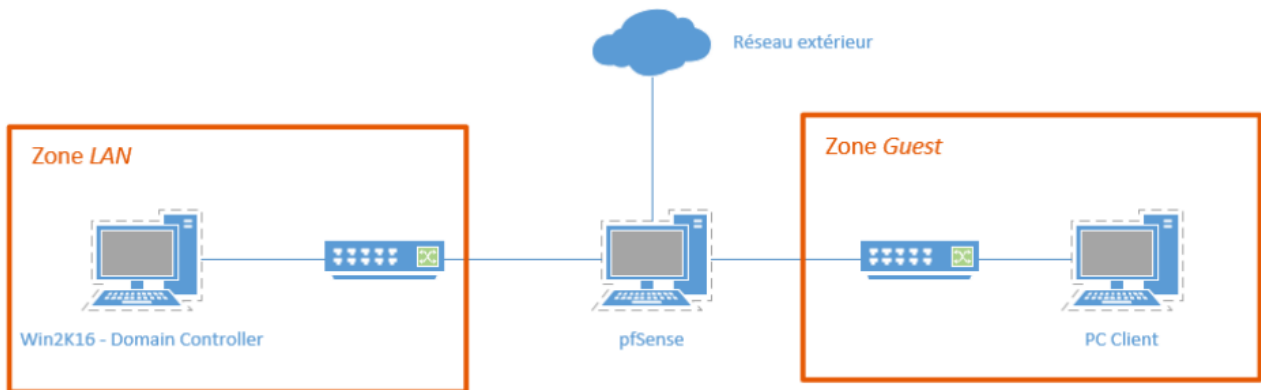
1. dans *system/user manager/authentication servers*, cliquer sur *add*
  - Descriptive name = RADIUS
  - Type = RADIUS-Hostname or IP address = 192.168.1.2 (= adresse du serveur radius)
  - Shared Secret = copier le secret généré pour ce parefeu sur le serveur radius
  - Services offered = Authentication and Accounting
  - Authentication port value = 1812
  - Accounting port value = 1813
  - RADIUS NAS IP Attribute = LAN - 192.168.1.1
2. cliquer sur *save*
3. dans *diagnostics/authentication*, tester la connexion d'un utilisateur à radius

## 1.12 Configuration FreeRadius - serveur debian

...

## 2 Labos

### 2.1 Captive Portal (accès internet sur un réseau invité)



**Attention!** Il faut que le firewall et les routes soient bien configurées.

- Activer le captive portal:
  1. aller sur `services/captive portal`, et cliquer sur `add`
    - Zone name = GUEST
    - Zone description = Zone for guests
  2. cliquer sur `save & continue`
  3. sur `services/captive portal/guest/configuration`
    - Enable captive portal = cocher la case
    - Interface = GUEST
    - After authentication Redirection URL = `https://youtu.be/dQw4w9WgXcQ` (laisser vide)
    - Authentication Method = Use an Authentication backend
    - Authentication Server = Local Database
    - Enable HTTPS login = cocher la case
    - HTTPS server name = ip de la pfsense (interface guest)
  4. cliquer sur `save`
- Mettre l'interface guest en dhcp (si ce n'est pas déjà fait):
  1. aller sur `services/dhcp server/guest`
  2. cocher la case `enable dhcp server on guest interface`
  3. cliquer sur `save`
- Créer le groupe des utilisateurs qui peuvent se connecter à captive portal:
  1. aller sur `services/user manager/groups`, et cliquer sur `add`
    - Group Name = CaptivePortal
    - Scope = Local
  2. ajouter les membres si ils sont déjà créés (sinon, on peut les rajouter après)
  3. cliquer sur `save`, puis éditer le groupe créé
  4. dans `assigned privileges`, cliquer sur `add`
  5. sélectionner le privilège `user - services: captive portal login`, puis cliquer 2 fois sur `save`
- Ajouter un utilisateur local:
  1. aller sur `services/user manager/users`, puis cliquer sur `add`

2. ajouter un *username* et un mot de passe
  3. dans *group membership*, cliquer sur *captive portal*, puis sur *move to "member of" list*
  4. cliquer sur *save*
- Modifier le serveur d'authentification:
    1. aller sur **system/user manager/settings**
    2. dans *authentication server*, sélectionner *local database*
    3. cliquer sur *save*

## 2.2 Captive Portal avec des vouchers (= codes d'accès wifi individuels)

- Activer le captive portal:
  1. aller sur **services/captive portal**, et cliquer sur *add*
    - Zone name = GUEST
    - Zone description = Zone for guests
  2. cliquer sur *save & continue*
  3. sur **services/captive portal/guest/configuration**
    - Enable captive portal = cocher la case
    - Interface = GUEST
    - After authentication Redirection URL = <https://youtu.be/dQw4w9WgXcQ> (laisser vide)
  4. cliquer sur *save*
  5. sur **services/captive portal/guest/vouchers**
  6. cocher la case *enable the creation, generation and activations of rolls with vouchers*
  7. cliquer sur *generate new keys*
  8. cliquer sur *save*, puis cliquer sur *add*
    - Roll = 1 (  $\implies$  numéro identifiant la génération de ces vouchers (pas important))
    - Minutes per ticket = 1440
    - Count = 150 (  $\implies$  nombre de vouchers)
  9. cliquer sur *save*
- Modifier le serveur d'authentification:
  1. aller sur **system/user manager/settings**
  2. dans *authentication server*, sélectionner *local database*
  3. cliquer sur *save*

## 2.3 Captive Portal avec RADIUS via active directory

- Ajouter un serveur d'authentification:
  1. dans **system/user manager/authentication servers**, cliquer sur *add*
    - Descriptive name = RADIUS
    - Type = RADIUS
    - Hostname or IP address = 192.168.1.2 (= adresse du serveur radius)
    - Shared Secret = copier le secret généré pour ce parefeu sur le serveur radius
    - Services offered = Authentication and Accounting
    - Authentication port value = 1812
    - Accounting port value = 1813
    - RADIUS NAS IP Attribute = LAN - 192.168.1.1

2. cliquer sur *save*
- Tester l'authentification au serveur radius en allant sur *diagnostics/authentication*.
  - Activer le captive portal:
    1. aller sur **services/captive portal**, et cliquer sur *add*
      - Zone name = GUEST
      - Zone description = Zone for guests
    2. cliquer sur *save & continue*
    3. sur **services/captive portal/guest/configuration**
      - Enable captive portal = cocher la case
      - Interface = GUEST
      - After authentication Redirection URL = <https://youtu.be/dQw4w9WgXcQ> (laisser vide)
      - Authentication Method = Use an Authentication backend
      - Authentication Server = radius
      - Enable HTTPS login = cocher la case
      - HTTPS server name = ip de la pfsense (interface guest)
    4. cliquer sur *save*
  - Modifier le serveur d'authentification:
    1. aller sur **system/user manager/settings**
    2. dans *authentication server*, sélectionner *radius*
    3. cliquer sur *save*

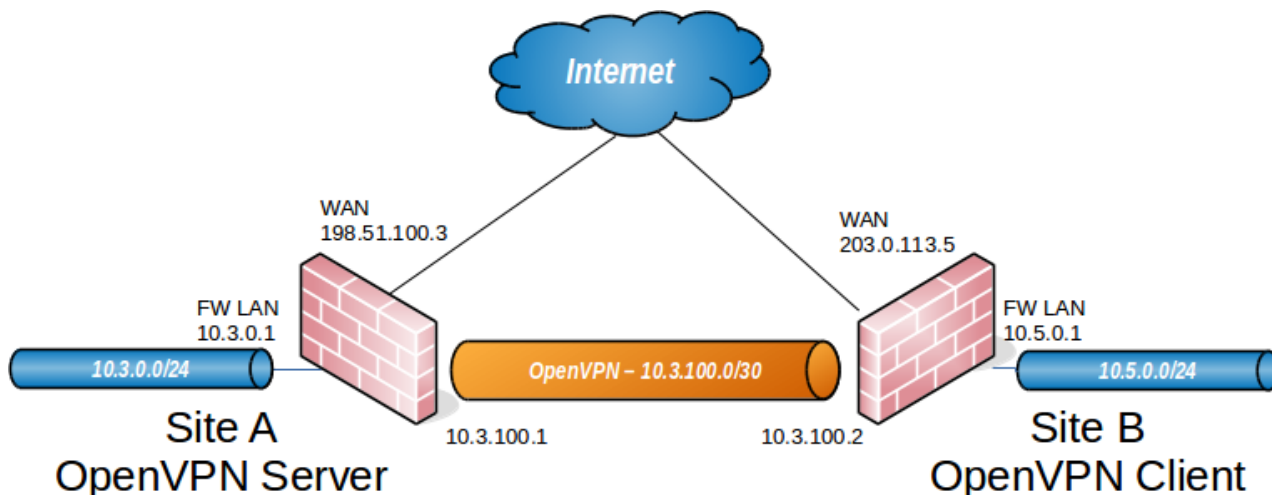
## 2.4 Captive Portal - attaque man in the middle

1. désactiver le login en https sur le captive portal
2. lancer le programme ettercap sur une kali dans le réseau guest
3. une fois les ip du pc client et de pfsense trouvé, cliquer sur *mitm* et lancer l'arp poisoning
4. lancer wireshark et appliquer le filtre: `ip.src == <ip_client> and ip.dst == <ip_pfsense> and http`
5. lancer une connexion sur un site en http (pour éviter la redirection https) et se connecter sur le captive portal
6. obtenir les informations de connexion dans la requête http post dans wireshark

**Remarque:** une fois qu'on a un compte de l'active directory, qu'est-ce qu'on peut en faire ?



## 2.5 OpenVPN site to site avec clé partagée (pas dans le cours mais plus simple)

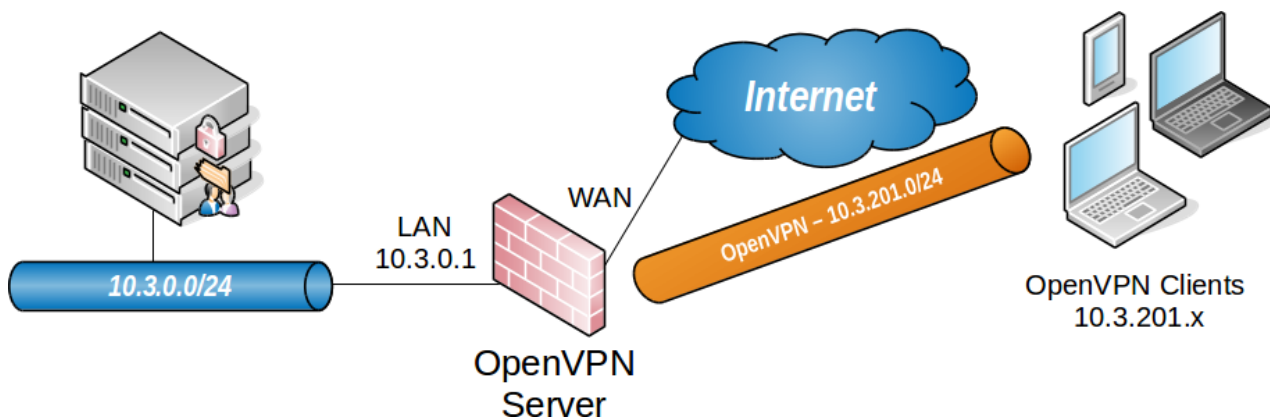


- sur l'openvpn serveur, dans `vpn/openvpn/servers`, ajouter une entrée:
  - Server mode = Peer to Peer (Shared Key)
  - IPv4 Tunnel Network = 10.0.3.0/24 (= réseau virtuel s2s)
  - IPv4 Remote Network(s) = 192.168.2.0/24, 10.0.1.0/24 (= lans du côté openvpn client)
  - éditer le serveur et exporter la clé *shared key* sur l'openvpn client
- sur l'openvpn client, dans `vpn/openvpn/clients`, ajouter une entrée:
  - Server mode = Peer to Peer (Shared Key)
  - Server host or address = 10.0.2.17 (= ip wan de l'openvpn serveur)
  - Auto generate = décocher la case
  - Shared Key = copier la clé exportée tantôt
  - IPv4 Tunnel Network = 10.0.3.0/24 (= réseau virtuel s2s)
  - IPv4 Remote Network(s) = 192.168.1.0/24, 10.0.0.0/24 (= lans du côté openvpn serveur)
- sur l'openvpn client, dans `interfaces/interface assignments`, cliquer sur *add*, puis sur *save*
- sur l'openvpn client, dans `interfaces/<nouvelle_interface>`:
  - Enable interface = cocher la case
  - Description = VPN-S2S
- sur l'openvpn client, dans `status/openvpn`, redémarrer le service
- sur les 2 openvpn, dans `firewall/rules/wan`, ajouter une entrée:
  - Protocol = UDP
  - Port = 1194 (OpenVPN)
- sur les 2 openvpn, dans `firewall/rules/wan`, désactiver la règle: *block private networks*
- sur les 2 openvpn, dans `firewall/rules/OpenVPN`, ajouter une entrée:
  - Protocol = any
- sur l'openvpn client, dans `firewall/rules/VPN-S2S`, ajouter une entrée:
  - Protocol = any

## 2.6 OpenVPN site to site avec certificats

1. sur l'openvpn serveur, dans `system/certificate manager/cas`, ajouter une entrée:
  - Descriptive Name = Server-CA
2. sur l'openvpn serveur, dans `system/certificate manager/certificates`, ajouter une entrée:
  - Descriptive Name = Server-CR
  - Common Name = 10.0.2.17 (= ip de l'openvpn serveur)
  - Certificate Type = Server Certificate
3. sur l'openvpn serveur, dans `system/certificate manager/certificates`, ajouter une entrée:
  - Descriptive Name = Client-CR
  - Common Name = 10.0.2.15 (= ip de l'openvpn client)
4. importer le certificat de *server-ca* et la clé et le certificat de *client-cr* sur l'openvpn client
5. sur l'openvpn serveur, dans `vpn/openvpn/servers`, ajouter une entrée:
  - Use a TLS Key = décocher la case
  - Server Certificate = Server-CR
  - IPv4 Tunnel Network = 10.0.3.0/24 (= réseau virtuel s2s)
  - IPv4 Local Network(s) = 10.0.0.0/24, 192.168.1.0/24 (= lans du côté openvpn serveur)
  - IPv4 Remote network(s) = 10.0.1.0/24, 192.168.2.0/24 (= lans du côté openvpn client)
6. sur l'openvpn client, dans `vpn/openvpn/servers`, ajouter une entrée:
  - Server host or address = 10.0.2.17 (= adresse wan de l'openvpn serveur)
  - Server Port = faire correspondre ce port à celui utilisé sur le serveur (a priori 1194)
  - Use a TLS Key = décocher la case
  - Client Certificate = Client-CR
  - IPv4 Tunnel Network = 10.0.3.0/24 (= réseau virtuel s2s)
  - IPv4 Remote network(s) = 192.168.1.0/24, 10.0.0.0/24 (= lans du côté openvpn serveur)
7. sur l'openvpn client, dans `interfaces/interface assignments`, cliquer sur *add*, puis sur *save*
8. sur l'openvpn client, dans `interfaces/<nouvelle_interface>`:
  - Enable interface = cocher la case
  - Description = VPN-S2S
9. sur l'openvpn client, dans `status/openvpn`, redémarrer le service
10. sur les 2 openvpn, dans `firewall/rules/wan`, ajouter une entrée:
  - Protocol = UDP
  - Port = 1194 (OpenVPN)
11. sur les 2 openvpn, dans `firewall/rules/wan`, désactiver la règle: *block private networks*
12. sur les 2 openvpn, dans `firewall/rules/OpenVPN`, ajouter une entrée:
  - Protocol = any
13. sur l'openvpn client, dans `firewall/rules/VPN-S2S`, ajouter une entrée:
  - Protocol = any

## 2.7 OpenVPN remote to site



1. dans `system/package manager/available packages`, installer: `openvpn-client-export`
2. sur `vpn/openvpn/wizards`, compléter le wizard:
  - Description = VPN-R2S
  - Tunnel Network = 10.0.4.0/24 (= réseau virtuel r2s)
  - Local Network = 192.168.1.0/24, 10.0.0.0/24 (= réseaux lans)
  - Firewall Rule = cocher la case
  - OpenVPN Rule = cocher la case
3. sur `vpn/openvpn/client export utility`, aller en bas de la page, dans *inline configurations*, cliquer sur *most clients*
4. exporter le fichier vers une machine debian:
  - `sudo openvpn <fichier>.ovpn`
  - `alt+f2`
  - `ip route` (normalement, il y a les routes vers les lans du vpn)
  - `ping 192.168.1.2` (= ip de la windows serveur dans le lan openvpn)

### Remarques:

- authentication via la db local [CR + mdp], il faut modifier les utilisateurs pour leur créer un certificat personnel (user manager)
- authentication radius [CR + mdp], il faut créer un certificat utilisateur normal (certificate manager)

# Table des matières

<b>1</b>	<b>Installations &amp; Configurations</b>	<b>1</b>
1.1	Configuration internet explorer - windows server . . . . .	1
1.2	Installation active directory - windows server . . . . .	1
1.3	Créer un groupe d'utilisateurs sur active directory - windows server . . . . .	1
1.4	Installer et configurer RADIUS - windows server . . . . .	2
1.5	Configuration routeur - routeur debian . . . . .	3
1.6	Configuration de base - pfsense . . . . .	3
1.7	Configuration parefeu nat - pfsense . . . . .	3
1.8	Configuration parefeu règles - pfsense . . . . .	3
1.9	Configuration routes statiques - pfsense . . . . .	4
1.10	Certificats (CA, CR, import, export) - pfsense . . . . .	4
1.11	Ajouter RADIUS dans pfsense - pfsense . . . . .	5
1.12	Configuration FreeRadius - serveur debian . . . . .	5
<b>2</b>	<b>Labos</b>	<b>6</b>
2.1	Captive Portal (accès internet sur un réseau invité) . . . . .	6
2.2	Captive Portal avec des vouchers (= codes d'accès wifi individuels) . . . . .	7
2.3	Captive Portal avec RADIUS via active directory . . . . .	7
2.4	Captive Portal - attaque man in the middle . . . . .	8
2.5	OpenVPN site to site avec clé partagée (pas dans le cours mais plus simple) . . . . .	9
2.6	OpenVPN site to site avec certificats . . . . .	10
2.7	OpenVPN remote to site . . . . .	11