Service Telecom Réseaux

Configuration VPN pour accès Internet + Wifi
- CNRS DE MONTPELLIER -

Titre :	Configuration VPN access Internet + Wifi – CNRS de Montpellier		
Auteur :	Nicolas BROTE	Nb de pages (celle-ci incluse) :	11
Date :	27 Janvier 2011	Révision :	1.03

Tél : 04 66 56 40 49 Site-web : www.st-r.com Fax : 04 66 56 40 48
Siège social : ZAC de Mejannes, 146 avenue Jean Chaptal - 30340 Mejannes-les-Ales
SIRET 418 116 49700011 - NAF 721 Z – ART 4372 C - CAPITAL 34300 €

Evolutions du document

Itération	Date	Justification modification	Référence
1.00	05/01/11	Création	CVPNNETPLUSWIFI100
1.01	13/01/11	Ajout configurations	CVPNNETPLUSWIFI101
1.02	14/01/11	Modification filtrage Meru	CVPNNETPLUSWIFI102
1.03	27/01/11	Modification redirection Fortinet	CVPNNETPLUSWIFI103

SOMMAIRE

1 – Architecture réseau et adressage IP 4

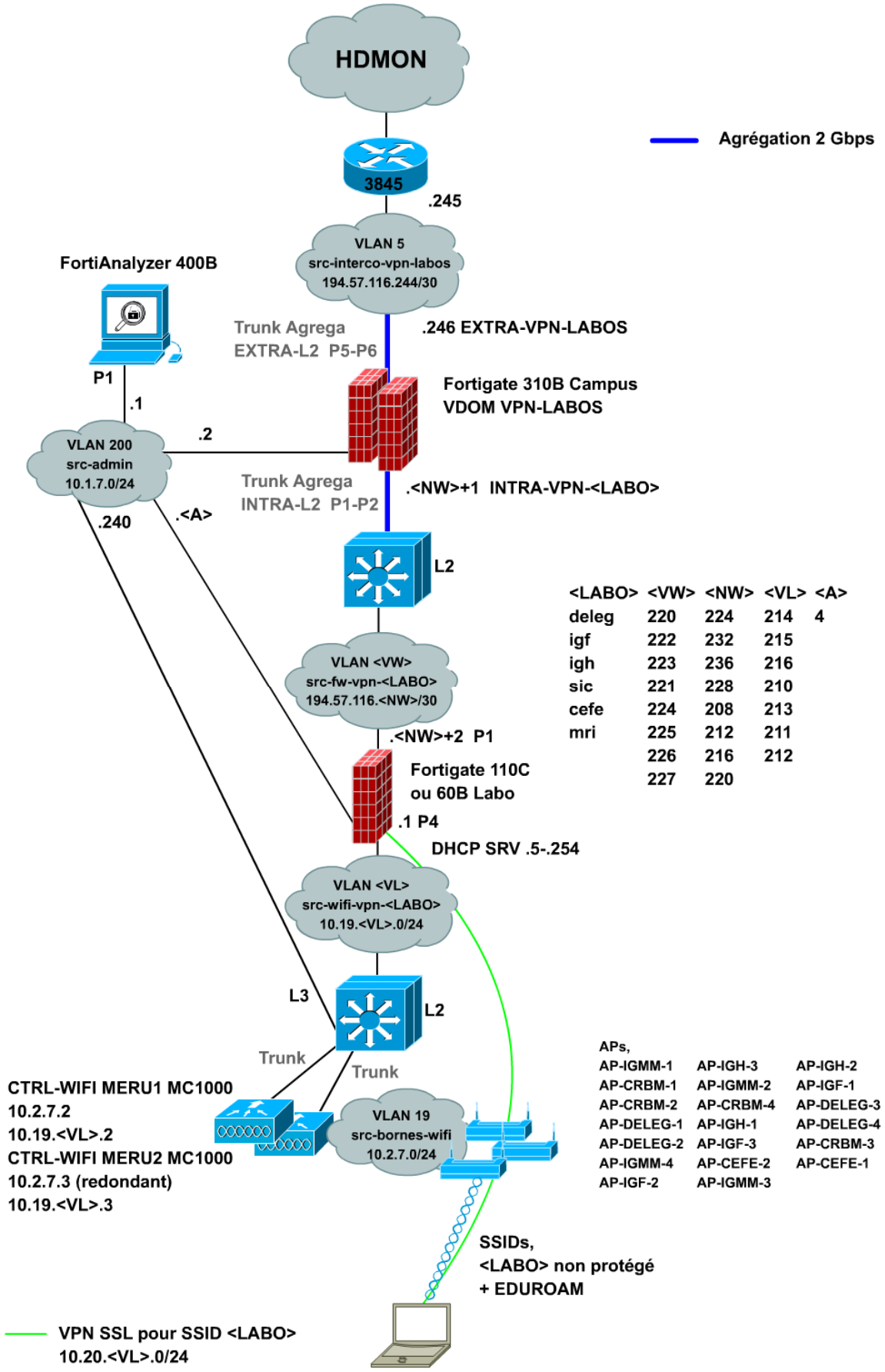
2 – Configuration contrôleur wifi Meru 5

3 – Configuration des pares feu Fortinet 7

3.1 – Configuration sur le FW-Campus 7

3.2 – Configuration sur le FW-Labo 8

1 – Architecture réseau et adressage IP



2 – Configuration contrôleur wifi Meru

https://10.2.7.2

Déclarer un profil de sécurité ouvert (à ne faire qu'une fois),
Configuration > Security > Profile > Add

```
Security Profile Name = ouvert
Laisser tout par défaut (pas de sécurité à ce niveau)
Cliquer sur OK
```

Déclaration du VLAN <VL> src-wifi-vpn-<LABO> pour chaque Labo,
Configuration > Wired > VLAN > Add

```
VLAN Name = src-wifi-vpn-deleg
Tag = 214
Fast Ethernet Interface Index = 2
IP Address = 10.19.214.2
Netmask = 255.255.255.0
IP Address of the Default Gateway = 10.19.214.1
DHCP Server IP Address = 10.19.214.1
```

Déclaration d'un SSID <LABO> ouvert pour chaque Labo,
Configuration > Wireless > ESS > Add

```
ESS Profile Name = deleg
SSID = deleg
Security Profile Name = ouvert
SSID Broadcast = yes
Tunnel Interface Type = Configured VLAN Only
VLAN Name = src-wifi-vpn-deleg
```

Eventuellement filtrer la diffusion du SSID par point d'accès RADIO,
Configuration > Wireless > ESS > cliquer sur la flèche à gauche du SSID puis sur l'onglet 'ESS-AP Table'

A ce point on peut ajouter ou supprimer la connaissance de ce SSID en fonction des points d'accès.

Filtrage pour que les utilisateurs wifi ne puissent pas avoir de connectivité réseau entre eux,
QoS > System Settings > QoS and Firewall Rules

```
Add,
ID = <100-plus-numero-vlan-exemple-314>
Destination IP = 10.19.214.1
Destination Netmask = 255.255.255.255
Cocher la case de la colonne match à gauche de "Destination IP"
QoS Protocol = none
Action = FORWARD
OK

Add,
ID = <200-plus-numero-vlan-exemple-414>
Source IP = 10.19.214.1
Source Netmask = 255.255.255.255
Cocher la case de la colonne match à gauche de "Source IP"
QoS Protocol = none
Action = FORWARD
OK

Add,
ID = <300-plus-numero-vlan-exemple-514>
Destination IP = 10.19.214.0
Destination Netmask = 255.255.255.0
Cocher la case de la colonne match à gauche de "Destination IP"
Source IP = 10.19.214.0
Source Netmask = 255.255.255.0
Cocher la case de la colonne match à gauche de "Source IP"
QoS Protocol = none
Action = DROP
OK
```

Sauvegarder la configuration du contrôleur,
Cliquer sur le lien Save en haut à droite

3 – Configuration des pares feu Fortinet

3.1 – Configuration sur le FW-Campus

https://10.1.7.2:4443/

Dans le VDOM Global ajouter une interface,
System > Network > Interface > Create New

```
Name = INTRA-VPN-<NOM-LABO>
Type = VLAN
Interface = INTRA-L2
VLAN ID = <VL>
IP/Netmask = 194.57.116.<NW>/30
```

Puis aller dans le VDOM VPN-LABOS.

Il faut ensuite déclarer les règles globales qui rajoutent un niveau de filtrage au-dessus de ce qui est autorisé par les FW-LABOS (filtrage du flux filtré par les FW-LABOS),
Firewall > Policy > Policy > Create New

De EXTRA-VPN-LABOS vers INTRA-VPN-<LABO>,

Source	Destination	Service	Nat Source	Action
All	All	HTTPS ICMP_ANY IKE	-	ACCEPT

De INTRA-VPN-<LABO> vers EXTRA-VPN-LABOS,

Source	Destination	Service	Nat Source	Action
All	All	HTTP ICMP_ANY DNS	-	ACCEPT

3.2 – Configuration sur le FW-Labo

Exemple Labo = deleg, https://10.1.7.4:4443

Ajouter l'interface d'interconnexion au FW-Campus et l'interface d'interconnexion au contrôleur Meru,
System > Network > Interface > Create New

```
Name = src-fw-vpn-deleg
Type = VLAN
Interface = P1
IP/Netmask = 194.57.116.226/30

Name = src-wifi-vpn-deleg
Type = VLAN
Interface = P4
IP/Netmask = 10.19.214.1/24
```

Configurer le serveur DHCP,
System > DHCP Server > Service > Create New

```
Interface Name = port4(src-wifi-vpn-deleg)
Mode = Server
Cocher Enable
Type = Regular
IP Range = 10.19.214.3 - 10.19.214.254
Network Mask = 255.255.255.0
Default Gateway = 10.19.214.1
DNS Service = Use System DNS Setting
```

Ajouter des règles de routage (attention le séquencement est important) si on a plusieurs interfaces de sortie vers Internet,
Router > Static > Policy Route > Create New

```
Incoming interface = ssl.root
Source address / mask = 10.20.214.0/24
Destination address / mask = 193.49.133.0/24
Outgoing interface = DR13

Incoming interface = ssl.root
Source address / mask = 10.20.214.0/24
Destination address / mask = 0.0.0.0/0
Outgoing interface = port1
Gateway Address = 194.57.116.225

Incoming interface = port4(src-wifi-vpn-deleg)
Source address / mask = 10.19.214.0/24
Destination address / mask = 193.49.133.0/24
Outgoing interface = DR13
```

```
Incoming interface = port4(src-wifi-vpn-deleg)
Source address / mask = 10.19.214.0/24
Destination address / mask = 0.0.0.0/0
Outgoing interface = port1
Gateway Address = 194.57.116.225
```

Changer le message par défaut pour le blocage Fortiguard d'URLs,
System > Config > Replacement Message > HTTP > URL block message > Edit

```
<html><head><title>Service disponible avec client VPN</title></head><body><font size=2><table width="100%"><tr><td bgcolor=#ff6600 align="center" colspan=2><font color=#ffffff><b>Service disponible avec client VPN.</b></font></td></tr></table><br><br>Ce service est disponible seulement si vous activez votre connexion VPN.<br><br><br>Pour vous connecter au VPN : <u><a href="https://10.19.214.1">Cliquer ici.</a></u></font></body></html>
```

Créer une règle de filtrage URL qui interdit tout pour intercepter les requêtes http,
UTM > Web Filter > URL Filter > Create New

```
Name = REDIRECT-VPNSSL
URL = *
Type = Wildcard
```

Créer un profil pour appliquer la règle précédente,
UTM > Web Filter > Profile > Create New

```
Name = PROFIL-REDIRECT-VPNSSL
Cocher 'Web URL Filter' pour la colonne http
Sélectionner REDIRECT-VPNSSL
```

Créer un pool d'adresse pour les clients VPN,
Firewall > Address > Address > Create New

```
Address Name = VPN-POOL
Type = Subnet / IP Range
Subnet / IP Range = 10.20.214.3 - 10.20.214.254
Interface = Any
```

Ensuite il faut configurer le portail VPN SSL,
VPN > SSL > Config

```
Vérifier que 'Enable SSL-VPN' est bien coché
```

VPN > SSL > Portal > Create New

```
Donner un nom au portail
```

Supprimer les composants qui ne vous intéresse pas (par exemple Bookmark et Connection Tool) en cliquant sur la croix en haut à droite du composant.

Sur le composant Tunnel Mode,

```
Cliquer sur le crayon pour éditer
Sélectionner le pool VPN créé précédemment 'VPN-POOL'
Cocher Split Tunneling
Cliquer sur OK au niveau du composant
Cliquer sur Apply puis sur OK
```

Il faut ensuite créer des utilisateurs soit sur la base locale soit sur un serveur type RADIUS ou LDAP (on peut combiner les méthodes).

Pour créer des utilisateurs dans la base locale,
User > User > User > Create New

Pour declarer un serveur AD,
User > Remote > LDAP > Create New

```
Name = AD2008
Server Name/IP = 193.49.133.208
Server Port = 389
Common Name Identifier = sAMAccountName
Distinguished Name = OU=DR13,DC=ad,DC=dr13,DC=cnrs,DC=fr
Bind Type = Regular
User DN = CN=fortigate fortigate,OU=divers,OU=Utilisateurs,OU=DR13,DC=ad,DC=dr13,DC=cnrs,DC=fr
Password = <password>
Secure Connection = <non-par-défaut>
```

Ensuite créer un groupe d'utilisateurs qui servira à l'authentification du VPN-SSL,
User > User Group > User Group > Create New

```
Name = WIFI-VPN-GROUP
Type = Firewall
Cocher 'Allow SSL-VPN Access' et sélectionner le portail associé
Eventuellement ajouter des utilisateurs dans la zone 'Members'
Eventuellement ajouter un serveur distant en cliquant sur Add dans Remote
authentication servers
```

Pour les serveurs LDAP on peut spécifier un groupe,
Exemple: CN=VPN-Admins,OU=groupes,OU=Utilisateurs,OU=DR13,DC=ad,DC=dr13,DC=cnrs,DC=fr

Dans ce cas au niveau AD, il faut créer le groupe Windows et ajouter le groupe aux utilisateurs qui seront autorisés à se connecter en VPN-SSL.

Une fois tous les objets définis il faut créer les règles pour valider l'interception http avec message de redirection et le VPN SSL,
`Firewall > Policy > Policy > Create New`

De port4(src-wifi-vpn-deleg) vers port1(src-fw-vpn-deleg) pour redirection http,

Source	Destination	Service	Nat Source	Action	UTM > Enable Web Filter
All	All	HTTP	Oui	ACCEPT	PROFIL-REDIRECT-VPNSSL

De port4(src-wifi-vpn-deleg) vers DR13 (LAN du LABO),

Source	Destination	Service	Nat Source	Action	SSL-VPN Users
All	193.49.133.208 193.49.133.112	DNS	-	ACCEPT	-
All	All	ANY	-	SSL-VPN	WIFI-VPN-GROUP

Une fois ces règles définies l'interception http et l'authentification VPN sont opérationnelle, cependant en mode Tunnel le split tunneling et le traffic ne peut pas encore traverse le firewall.

Pour que le split-tunneling (possibilité d'utiliser le VPN uniquement pour une liste définit de réseaux) soit opérationnel il faut mettre en destination de la règle qui a pour 'Action' VPN-SSL, la liste des réseaux qui pourront-être accéder en VPN à la place de Any.

Pour que le trafic puisse passer en mode Tunnel il faut autoriser le flux depuis l'interface ssl.root vers les différents réseaux, par exemple pour avoir un accès IP complet au LAN du LABO,

De ssl.root vers DR13 (LAN du LABO),

Source	Destination	Service	Nat Source	Action	SSL-VPN Users
10.20.214.0/24	LAN_DR13	ANY	-	ACCEPT	-

Et l'inverse si besoin d'initier des connexions depuis le LAN vers un client VPN.