



Enseignement agricole
Formations grandeur nature



MINISTÈRE
DE L'ALIMENTATION
DE L'AGRICULTURE
ET DE LA PÊCHE

Les réseaux des EPLEFPA

Guide « VPN Site à Site IpCop »

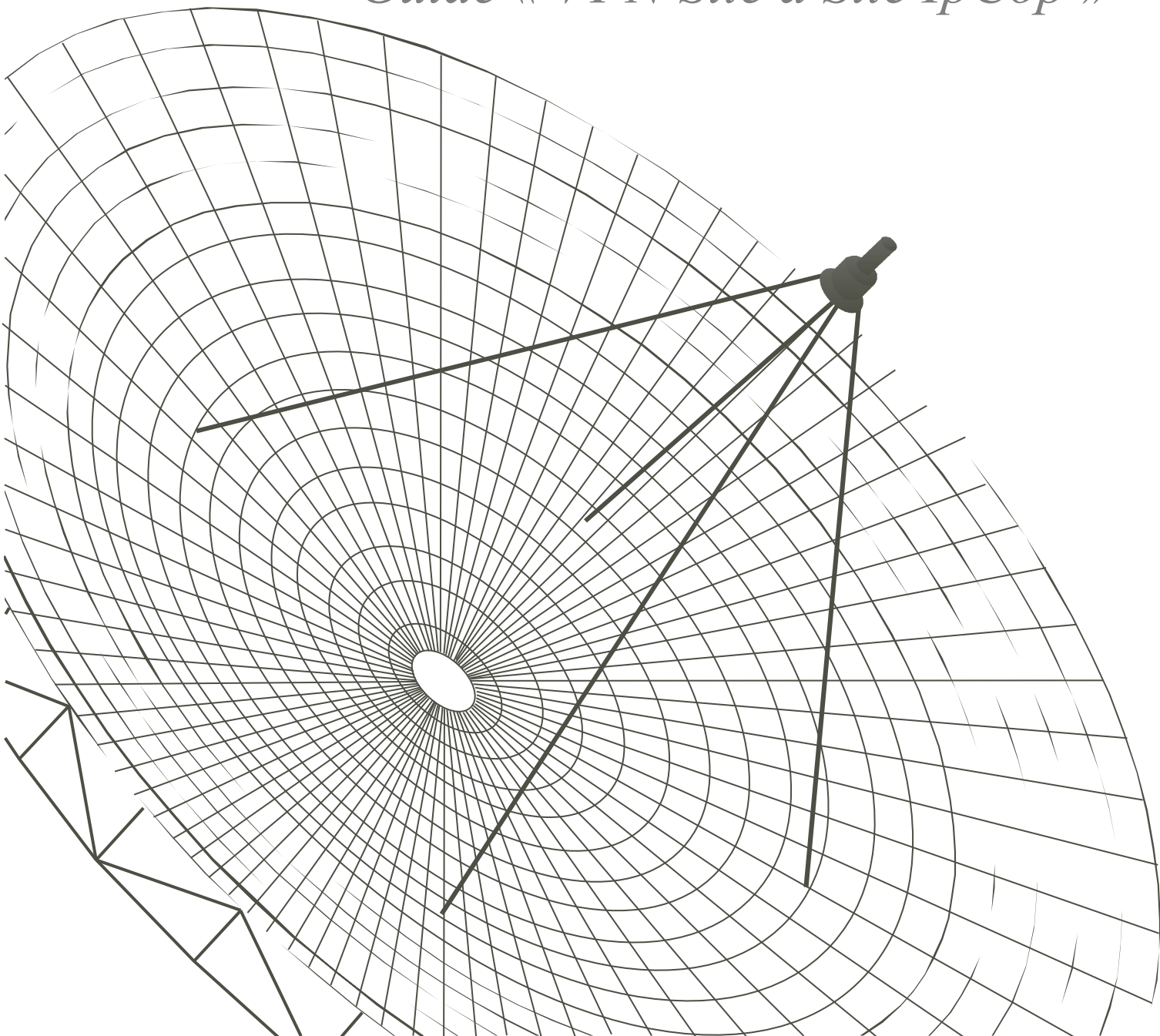


Table des matières

1	Introduction.....	3
2	Schéma de principe	3
3	Procédure pas à pas.....	4
3.1	Préparation.....	4
3.2	Génération des certificats racine et Système	5
3.3	Échange des CA Certificates	7
3.4	Création du tunnel VPN.....	8
3.5	Fonctionnement du tunnel VPN.....	10

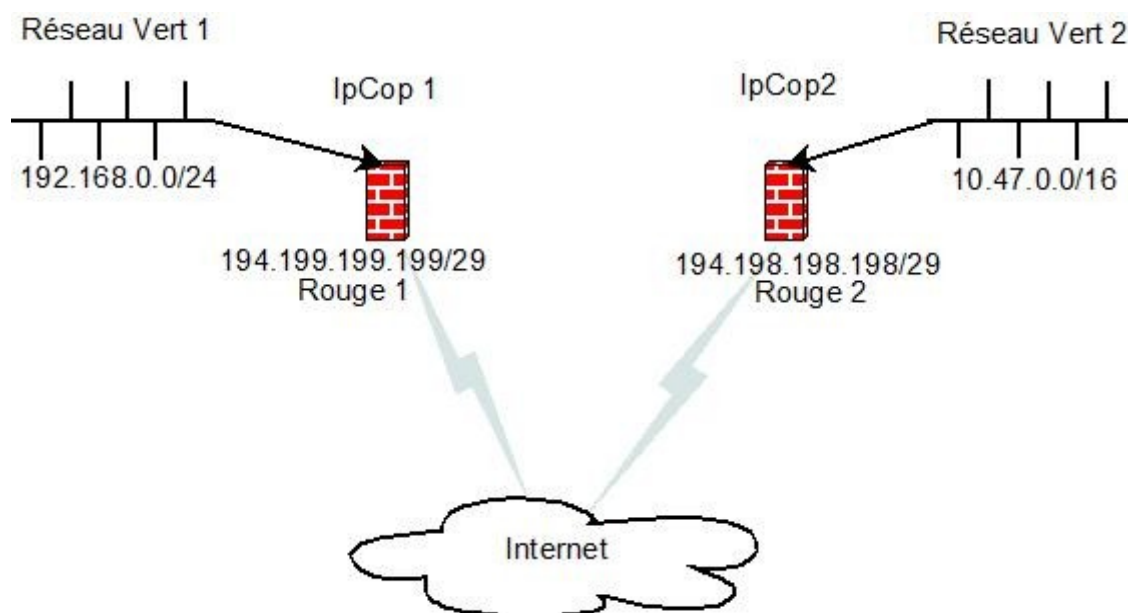
1 Introduction

Les distributions IpCop intègrent de façon native les outils nécessaires à la mise en place de tunnels VPN IpSec entre elles. Nous étudierons dans ce document sa mise en œuvre entre deux sites connectés directement à Internet et disposant d'adresses IP Fixes. Le principe restera le même pour établir un ou plusieurs tunnels supplémentaires entre deux ou plusieurs IpCop.

La suite de ce guide suppose que vous avez téléchargé, installé et paramétré correctement les deux serveurs ainsi que les accès au réseau conformément à la documentation de référence.

2 Schéma de principe

Nous allons étudier comment relier par un tunnel VPN deux réseaux vert en utilisant deux serveurs IpCop connectés à Internet par leur interface rouge disposant d'une adresse IP fixe.



Les noms et adresses utilisés sur ce schéma le sont à titre d'exemple

Vert1---- IPCOP1----Rouge1----- Internet -----Rouge1---- IPCOP2---- Vert2

- Le réseau Vert1 a pour réseau local 192.168.0.0/24
- L'interface Rouge 1 du serveur IpCop1 a pour adresse publique fixe 194.199.199.199/29
- Le réseau Vert2 a pour réseau local 10.47.0.0/16
- L'interface Rouge 2 du serveur IpCop2 a pour adresse publique fixe 194.198.198.198/29

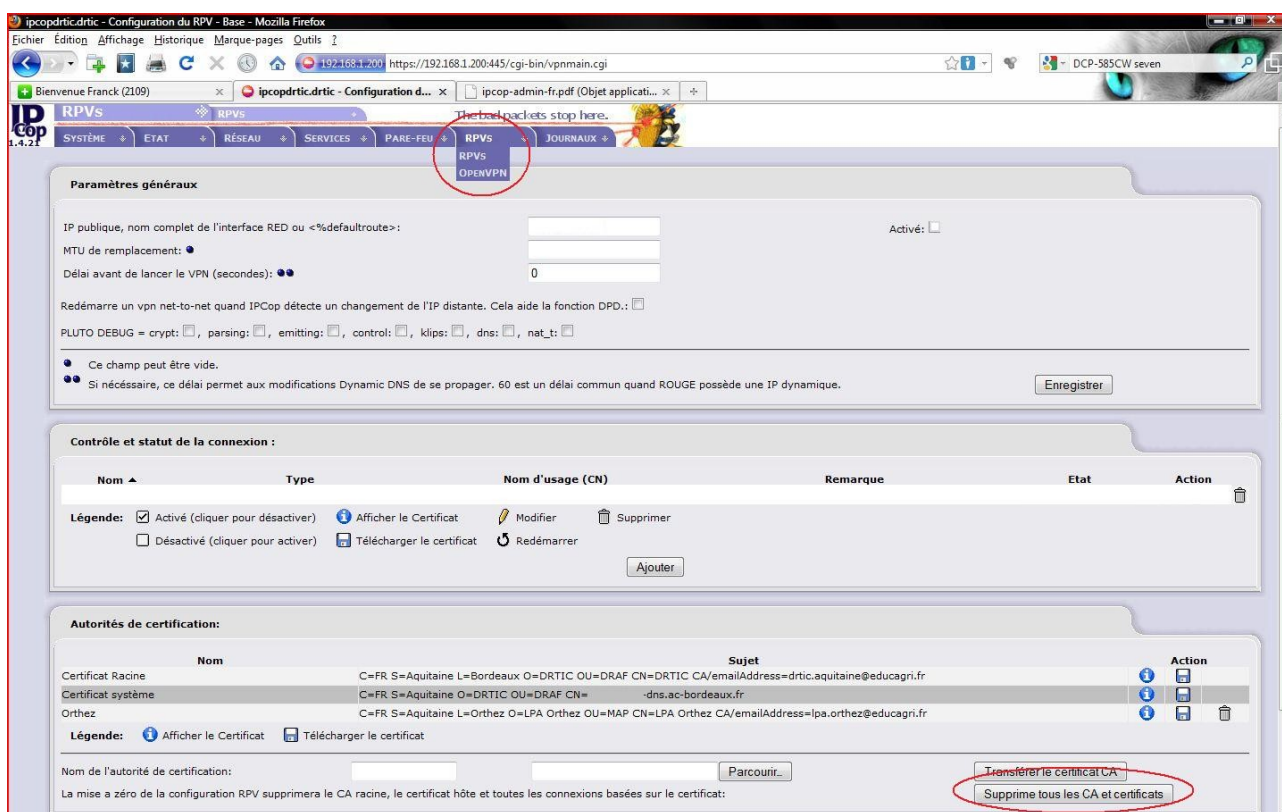
Attention : Les noms et adresses utilisés dans ce tutoriel sont des exemples à remplacer par les valeurs réelles de votre configuration.

3 Procédure pas à pas

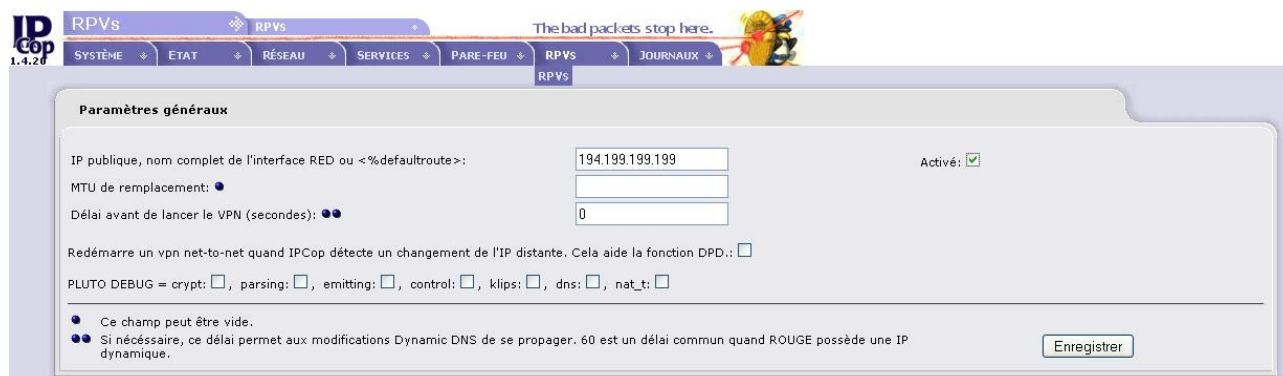
3.1 Préparation

Sur ipcop1

Faire un RAZ pour supprimer les anciennes configurations s'il y a lieu.



- Tapez dans le champ “Nom d'hôte ou IP locale du RPV:” l'adresse IP publique utilisée pour votre serveur IpCop1 ou son nom FDQN, par exemple « 024XXXX.ac-bordeaux.fr ».
- Cochez la case Activé et cliquer sur Enregistrer.



Sur ipcop2

Recommencez les mêmes opérations en utilisant les bons paramètres :

- Faire un RAZ pour supprimer les anciennes configurations s'il y a lieu.
- Tapez dans le champ “Nom d'hôte ou IP locale du RPV:” l'adresse IP publique utilisée pour votre serveur IpCop2 ou son nom FDQN exemple « 033YYYY.ac-bordeaux.fr ».
- Cochez la case Activé et cliquer sur Enregistrer.

3.2 Génération des certificats racine et Système

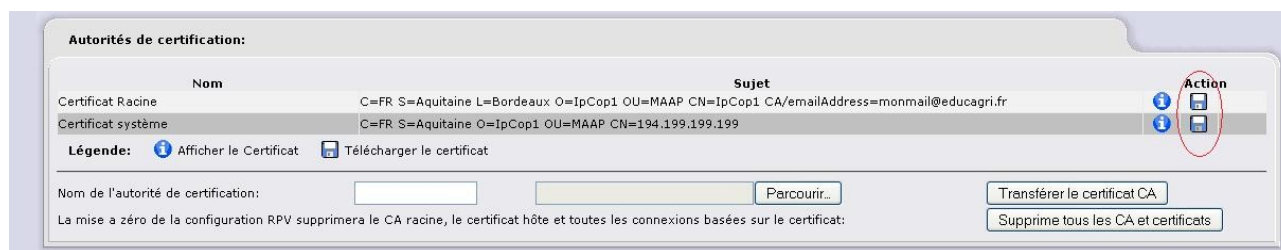
Sur ipcop1

- Cliquez sur “Génération des certificats racine et Système”

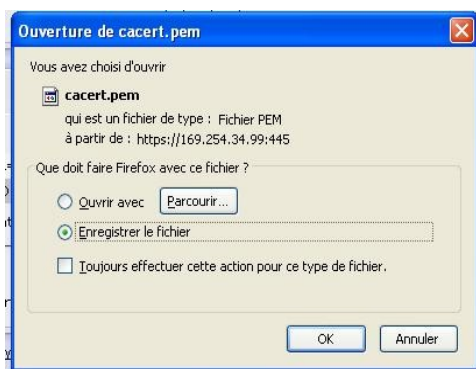
- puis remplir comme ci-dessous:
 - ipcop1 pour “Nom d'Organisation”
 - IP-FIXE-ipcop1 pour “Nom d'Hote IPCop's”
 - Sélectionner le pays

- Cliquez sur “Génération des certificats racine et Système”, cela va créer les certificats (qui peut prendre un moment) et enfin retour à la page d'accueil de RPVs.

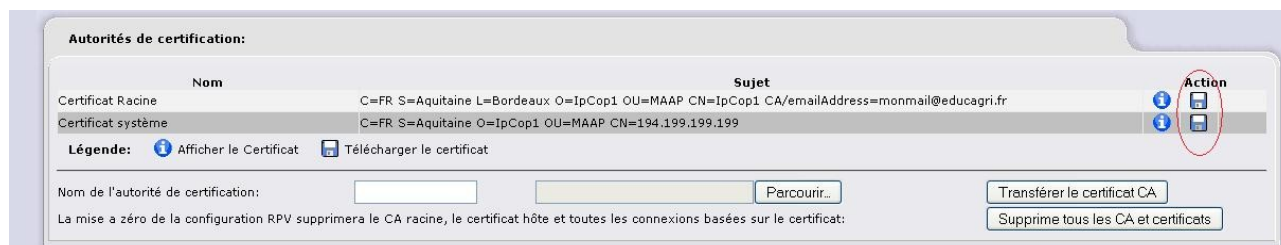
- Cliquer sur l'icône qui ressemble à une disquette “Télécharger le certificat racine”.



- Une invite va s'afficher pour enregistrer le certificat appelé cacert.pem



- Sauvegardez le fichier puis renommez le cacertipcop1.pem pour éviter les confusions.
- Cliquer sur l'icône qui ressemble à une disquette “Télécharger le certificat système”.



- Une invite va s'afficher pour enregistrer le certificat appelé hostcert.pem



- Sauvegardez le fichier puis renommez le hostcertipcop1.pem pour éviter les confusions.

Sur ipcop2

Recommencez les mêmes opérations en utilisant les bons paramètres pour la génération des certificats racine et système :

- ipcop2 pour “Nom d'Organisation”
- IP-Fixe-ipcop2 pour “Nom d'Hôte IPCop's”
- Les bons mails, nom d'organisation , etc ...
- Sélectionnez le pays

Recommencez les opérations de sauvegarde des certificats en utilisant les bons noms :

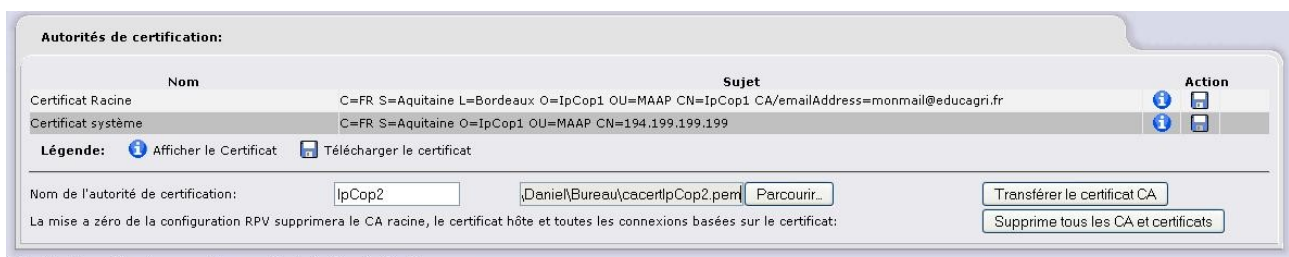
- Renommez cacert.pem en cacertipcop2.pem pour éviter les confusions.
- Renommez hostcert.pem en hostcertipcop2.pem pour éviter les confusions.
- Sauvegardez les certificats.

3.3 Échange des CA Certificates

A ce stade, nous allons faire connaître les 2 machines ipcop entre elles grâce à leur certificat AC respectifs. Le fichier cacertIpCop1 doit être envoyé au serveur IpCop2 par le moyen dont vous disposez (Messagerie, clefs USB, Disquette ...) et le fichier cacertIpCop2 doit être envoyé au serveur IpCop1 de la même manière. Ainsi nos deux serveurs pourront mutuellement se faire confiance grâce aux certificats de l'un et de l'autre.

Sur ipcop1

- Tapez ipcop2 pour le “Nom de l'autorité de certification”
- Cliquez sur Parcourir et sélectionner le fichier cacertipcop2.pem



Cette fonctionnalité est sponsorisée par : Seminole Canada Gas Company

- Cliquez sur “Transférer le certificat CA”, cela a pour but de transférer le certificat d'ipcop2 sur ipcop1. Une 3ème ligne va s'afficher en bas dans la colonne Autorités de Certification.



Sur ipcop2

Recommencez les mêmes opérations en utilisant les bons paramètres :

- Tapez ipcop1 pour le “Nom de l'autorité de certification”
- Cliquez sur Parcourir et sélectionner le fichier cacertipcop1.pem
- Cliquez sur “Transférer le certificat CA”. Une 3ème ligne va s'afficher en bas dans la colonne Autorités de Certification.

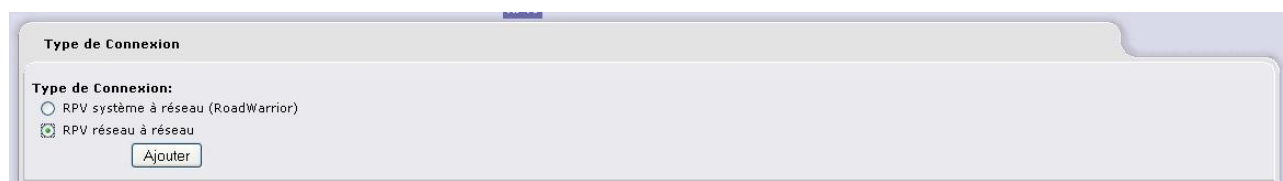
3.4 Création du tunnel VPN

Sur ipcop1

- Cliquez sur “Ajouter” bouton situé au milieu :



- Sélectionnez "RPV réseau à réseau" :



- Complétez les champs :
 - ipcop2 pour le “Nom”
 - l'IP publique du serveur IpCop1 pour le “Adresse Ip de la machine”
 - l'adresse du réseau local Vert1 pour le sous “Réseau Local”
 - l'IP publique du serveur IpCop2 pour le “Serveur/IP distant”
 - l'adresse du réseau local Vert2 pour “Sous Réseau Distant”

Connexion:

Nom: Activé:

Adresse IP de la machine: Serveur/IP distant:

Sous-réseau local : Sous-réseau distant :

ID Locale: ID Distant:

(câd : @xy.examp1e.com)

Action quand le 'pair' disparaît: 2

Remarque:

Poursuivre avec la configuration avancée.

- Dans la partie “Authentification” :
 - cliquez sur "Transférer un certificat".
 - cliquez sur "Parcourir" afin de sélectionner le fichier hostcertipcop2.pem

Authentification :

Utiliser une clé partagée (PSK) :

Transférer une demande de certificat :

Transférer un certificat

Transférer le fichier PKCS12 Mot de passe du fichier PKCS12:

Le pair est identifié par au choix la chaîne IPV4_ADDR, FQDN, USER_FQDN or DER_ASNI_DN présente dans le champ ID Distant

Générer un certificat :

Nom d'utilisateur ou Nom du système (CN):

Adresse courriel de l'utilisateur:

Division de l'utilisateur:

Nom d'Organisation:

Ville:

Etat ou région:

Pays:

Un sujet alternatif (subjectAltName=email:*,URI:*,DNS:*,RID:*)

Mot de passe du fichier PKCS12:

Mot de passe du fichier PKCS12:(confirmation)

- cliquez sur Enregistrer, vous obtenez :

Contrôle et statut de la connexion :

Nom	Type	Nom d'usage (CN)	Remarque	Etat	Action
Ipcop2	Réseau (Certificat)	Ipcop2 /emailAddress=monmail@educagri.fr		FERMÉ	

Légende: Activé (cliquer pour désactiver) Afficher le Certificat Modifier Supprimer

Désactivé (cliquer pour activer) Télécharger le certificat Redémarrer

Sur ipcop2

Recommencez les mêmes opérations en utilisant les paramètres inverses dans connexion :

- Tapez ipcop1 pour le “Nom de l'autorité de certification”
- l'IP publique du serveur IpCop2 pour le “Adresse Ip de la machine”
- l'adresse du réseau local Vert2 pour le sous “Réseau Local”
- l'IP publique du serveur IpCop1 pour le “Serveur/IP distant”
- l'adresse du réseau local Vert1 pour “Sous Réseau Distant”

Importez le bon certificat dans la partie authentification :

- cliquez sur "Transférer un certificat"
- cliquez sur "Parcourir" afin de sélectionner le fichier hostcertipcop1.pem
- cliquez sur Enregistrer.

3.5 Fonctionnement du tunnel VPN

Lorsque le paramétrage est terminé sur les deux serveurs IpCop correctement connectés au réseau Internet, le tunnel IpSec de site à site démarre. Vous obtenez donc un écran du type :

The screenshot shows the web interface of an IpCop device. The browser address bar shows the URL `https://192.168.1.200/cgi-bin/vpnmain.cgi`. The interface is in French and displays the 'Paramètres généraux' (General Parameters) section, which includes fields for 'IP publique', 'MTU de remplacement', and 'Délai avant de lancer le VPN'. Below this, there is a 'Contrôle et statut de la connexion' (Connection Control and Status) section containing a table with columns for 'Nom', 'Type', 'Nom d'usage (CN)', 'Remarque', 'Etat', and 'Action'. The 'Etat' column for the first entry is highlighted with a red circle and contains the text 'OUVERT'. At the bottom, there is an 'Autorités de certification' (Certificate Authorities) section with a table listing certificates and their details.

Nom	Type	Nom d'usage (CN)	Remarque	Etat	Action
Orthez	Réseau (Certificat)	194.199.XX.XX		OUVERT	[Info] [Ajouter] [Supprimer]