

Romain

Barillet

Ipfire



1- Installation de ipfire :

Il suffira d'une VM avec l'image ISO de ipfire qu'on peut retrouver sur le site officiel : <https://www.ipfire.org/>

2- Ipfire et VPN :



Accéder a la partie VPN de l'ipfire

Configuration générale

Statut actuel du serveur OpenVPN : **EN FONCTION**
OpenVPN sur ROUGE

Configuration réseau:

Nom d'hôte/IP du VPN local :

176.148.32.102

Sous-réseau OpenVPN

10.109.97.0/255.255.255.0

Protocole :

UDP

Port de destination :

1194

Taille du MTU :

1400

Options cryptographiques:

Algorithme de hashage

SHA2 (512 bit)

Chiffrer :

AES-CBC (256 bit)

Protection du canal TLS :

Sauvegarder

Pools adresses IP statiques

Options avancées du serveur

Arrêter serveur OpenVPN

Etat et contrôle de connexion :

Pool d'adresses IP dynamiques OpenVPN

Nom	type	Remarque	Statut	Action
debroise	Hôte (Certif)		DECONNECTE	<input checked="" type="checkbox"/>
dylan	Hôte (Certif)	atelier sio	DECONNECTE	<input checked="" type="checkbox"/>
romain	Hôte (Certif)		DECONNECTE	<input checked="" type="checkbox"/>
tristan	Hôte (Certif)	atelier sio	CONNECTE	<input checked="" type="checkbox"/>

Légende :

Télécharger le package client non sécurisé (zip)

Télécharger le paquet client (zip)

Afficher le certificat

Afficher QRCode OTP

Télécharger le certificat

Désactivé (cocher pour activer)

Activé (décocher pour désactiver)

Modifier

Enlever

Ajouter

Statistiques de connexions OpenVPN

Autorité de certification

Nom	Sujet	Action
Certificat racine	C = FR, ST = Normandie, L = Avranches, O = ateliersio2, OU = Manche, CN = ateliersio2 CA	
Certificat hôte	C = FR, ST = Normandie, O = ateliersio2, OU = Manche, CN = srvpn.labo.sio	
Parametre-Diffie-Hellman	DH Parameters: (4096 bit)	
Clé d'authentification TLS	2048 bit OpenVPN static key	

L'interface du VPN de l'ipfire

– Il va falloir générer un certificat

Autorité de certification

Nom	Sujet	Action
Certificat racine	C = FR, ST = Normandie, L = Avranches, O = ateliersio2, OU = Manche, CN = ateliersio2 CA	
Certificat hôte	C = FR, ST = Normandie, O = ateliersio2, OU = Manche, CN = srvpn.labo.sio	
Parametre-Diffie-Hellman	DH Parameters: (4096 bit)	
Clé d'authentification TLS	2048 bit OpenVPN static key	

Légende : Afficher le certificat Télécharger le certificat

Une fois le certificat installer, il va falloir le telecharger :

Autorité de certification

Nom	Sujet	Action
Certificat racine	C = FR, ST = Normandie, L = Avranches, O = ateliersio2, OU = Manche, CN = ateliersio2 CA	 
Certificat hôte	C = FR, ST = Normandie, O = ateliersio2, OU = Manche, CN = srvpn.labo.sio	 
Parametre-Diffie-Hellman	DH Parameters: (4096 bit)	
Clé d'authentification TLS	2048 bit OpenVPN static key	 

Légende :  Afficher le certificat  Télécharger le certificat

Puis, il a falloir creer des "comptes" qui va permette l'autorisation pour se connecter au VPN

OpenVPN 

Type de connexion

Type de connexion:

- Réseau privé virtuel (VPN) de l'hôte au réseau (client nomade)
- Réseau privé virtuel (VPN) site-à-site
- Réseau privé virtuel (VPN) site-à-site (Upload Client Package)

Aucun fichier sélectionné.

Import Connection Name

Par défaut: Client Packagename

[Retour](#)

Ici, on a differents types de VPN, dans notre cas on sera sur un VPN avec (client nomade)

On clique sur ajouter :

OpenVPN 

Type de connexion

Type de connexion:

- Réseau privé virtuel (VPN) de l'hôte au réseau (client nomade)
- Réseau privé virtuel (VPN) site-à-site
- Réseau privé virtuel (VPN) site-à-site (Upload Client Package)

Aucun fichier sélectionné.

Import Connection Name

Par défaut: Client Packagename

[Retour](#)

On va arriver sur cette page, et c'est ici qu'on va pouvoir configurer le compte et generer notre certificat

OpenVPN

Connexion:

Nom: *

Remarque:

Activé:

Choisissez un réseau

Pool d'adresses IP dynamiques OpenVPN (10.109.97.0/255.255.255.0)

Authentification :

Envoyer une demande de certificat : Aucun fichier sélectionné.

Envoyer un certificat :

Générer un certificat :

Nom d'utilisateur complet ou nom d'hôte du système : *

Adresse email de l'utilisateur :

Département de l'utilisateur :

Nom d'organisation :

Ville :

Etat ou région :

Pays :

Valide jusqu'au (days): *

Mot de passe PKCS12 :

Mot de passe PKCS12 : (confirmation)

* Champs requis

On rentre les informations necessaire pour le certificat, et nous pouvons meme attribuer un mot de passe qui sera demandé lors de la connexion au vpn

Une fois fini, vous aller apercevoir vos utilisateurs ici

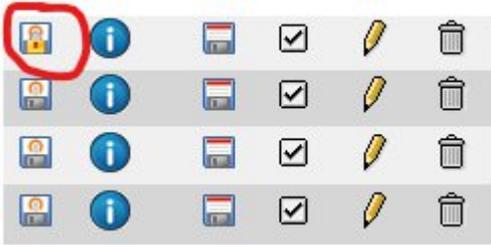
Pool d'adresses IP dynamiques OpenVPN

Nom	type	Remarque	Statut	Action
debroise	Hôte (Certif)		DECONNECTE	
dylan	Hôte (Certif)	atelier sio	DECONNECTE	
romain	Hôte (Certif)		DECONNECTE	
tristan	Hôte (Certif)	atelier sio	CONNECTE	

Légende

- Télécharger le package client non sécurisé (zip)
- Télécharger le paquet client (zip)
- Afficher le certificat
- Afficher QRCode OTP
- Télécharger le certificat
- Désactivé (cocher pour activer)
- Activé (décocher pour désactiver)
- Modifier
- Enlever

Et il va falloir telecharger leurs certificats qui sera utile pour la connexion au vpn :



Cela va vous telecharger un fichier zip avec dedans le certificat et vos informations

Fichier zip
telecharge

