

DOCUMENTATION d’exploitation

Configuration & Installation Serveur VPN



02 février 2024

projet uf infra

Aix Ynov Campus

Table of Contents

[PPTP 2](#_Toc166250449)

[Pour activer le serveur VPN PPTP : 2](#_Toc166250450)

[L2TP/IPSec 3](#_Toc166250451)

[Pour activer le serveur L2TP/IPSec VPN : 3](#_Toc166250452)

# PPTP

Le protocole PPTP (Point-to-Point Tunneling Protocol) est une solution VPN couramment utilisée et prise en charge par la plupart des clients (tels que Windows, Mac, Linux et les périphériques mobiles).

## Pour configurer le serveur VPN PPTP :

1. Ouvrez **VPN Server**, puis accédez à **PPTP** dans le panneau de gauche.



1. Cochez **Activer le serveur VPN PPTP**.
2. Spécifiez une adresse IP virtuelle de serveur VPN dans les champs **Adresse IP dynamique**. Nous faisons le choix de laisser celle par défaut qui est cohérente pour nos usages.
3. Définissez le **Nombre maximal de connexions** pour limiter le nombre de connexions VPN simultanées.

Ici nous choisissons de mettre 5 car plus n’est pas nécessaire vu que notre projet se limite à trois utilisateurs.

1. Définissez le **Nombre maximal de connexions avec le même compte** pour limiter le nombre de connexions VPN avec le même compte.

Ici nous choisissions 2 pour permettre à nos utilisateurs d’utiliser le VPN avec plusieurs appareils comme PC et téléphone pro.

1. Choisissez l'une des options suivantes dans le menu déroulant **Authentification** pour authentifier les clients VPN :
   1. **PAP** : le mot de passe des clients VPN n'est pas chiffré lors de l'authentification.
   2. **MS-CHAP v2** : le mot de passe des clients VPN est chiffré lors de l'authentification à l'aide de Microsoft CHAP version 2.

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

Nous avons sélectionné **MS-CHAP v2** pour l'authentification solution la plus sécurisée.

1. Choisissez l'une des options suivantes dans le menu déroulant **Chiffrement** pour chiffrer la connexion VPN :
   1. **Pas de MPPE** : la connexion VPN n'est pas protégée par un mécanisme de chiffrement.
   2. **MPPE facultatif** : la connexion VPN est protégée ou non par un mécanisme de chiffrement 40 bits ou 128 bits, selon les paramètres du client.
   3. **Exiger MPPE** : la connexion VPN est protégée par un mécanisme de chiffrement 40 bits ou 128 bits, selon les paramètres du client.

Dans notre cas nous avons choisi **MPPE facultatif** afin d’avoir le meilleur compromis entre sécurité et compatibilité en fonction des clients.

1. Définissez la **MTU** (unité de transmission maximale) pour limiter la taille de paquet de données transitant via le VPN.

Dans notre cas nous avons choisi 1400 la valeur par défaut.



1. Cochez **Utiliser un DNS manuel** et spécifiez l'adresse IP d'un serveur DNS pour pousser le DNS vers les clients PPTP.



Ici nous avons mis l’adresse IP du routeur de la maison faisant office de serveur DNS.

1. Cliquez sur **Appliquer** pour que la modification prenne effet.

# L2TP/IPSec

L2TP (Layer 2 Tunneling Protocol) sur IPSec fournit des réseaux virtuels privés avec une sécurité accrue et est pris en charge par la plupart des clients (tels que Windows, Mac, Linux et les périphériques mobiles).

## Pour activer le serveur L2TP/IPSec VPN :

1. Ouvrez **VPN Server**, puis accédez à **L2TP/IPSec** dans le panneau de gauche.



1. Cochez **Activer le serveur L2TP/IPSec VPN**.
2. Spécifiez une adresse IP virtuelle de serveur VPN dans les champs **Adresse IP dynamique.** Ici nous faisons le même choix que pour le PPTP
3. Définissez le **Nombre maximal de connexions** pour limiter le nombre de connexions VPN simultanées. Ici nous faisons le même choix que pour le PPTP
4. Définissez le **Nombre maximal de connexions avec le même compte** pour limiter le nombre de connexions VPN avec le même compte. Ici nous faisons le même choix que pour le PPTP

Une image contenant texte, capture d’écran, logiciel, affichage

Description générée automatiquement

1. Choisissez l'une des options suivantes dans le menu déroulant **Authentification** pour authentifier les clients VPN :
   1. **PAP** : le mot de passe des clients VPN n'est pas chiffré lors de l'authentification.
   2. **MS-CHAP v2** : le mot de passe des clients VPN est chiffré lors de l'authentification à l'aide de Microsoft CHAP version 2.

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

Nous avons sélectionné **MS-CHAP v2** pour l'authentification pour les mêmes raisons que dans la connexion PPTP

1. Choisissez l'une des options suivantes dans le menu déroulant **Chiffrement** pour chiffrer la connexion VPN :
   1. **Pas de MPPE** : la connexion VPN n'est pas protégée par un mécanisme de chiffrement.
   2. **MPPE facultatif** : la connexion VPN est protégée ou non par un mécanisme de chiffrement 40 bits ou 128 bits, selon les paramètres du client.
   3. **Exiger MPPE** : la connexion VPN est protégée par un mécanisme de chiffrement 40 bits ou 128 bits, selon les paramètres du client.

Dans notre cas nous avons choisi **MPPE facultatif** pour les mêmes raisons que dans le VPN PPTP

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

1. Définissez la **MTU** (unité de transmission maximale) pour limiter la taille de paquet de données transitant via le VPN.

Dans notre cas nous avons choisi 1400



1. Cochez **Utiliser un DNS manuel** et spécifiez l'adresse IP d'un serveur DNS pour pousser le DNS vers les clients PPTP. Ici nous utilisons la même que celle du PPTP



1. Pour des performances maximales du VPN, sélectionnez **Exécuter en mode noyau** (kernel). Cette option permet d’augmenter les performances de notre VPN



1. Saisissez et confirmez une **clé prépartagée**. Cette clé secrète peut être donnée à votre utilisateur VPN L2TP/IPSec pour authentifier la connexion.

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

1. Cochez **Activer le mode compatible SHA2-256 (96 bits)** pour autoriser certains clients (qui ne sont pas à la norme RFC) à utiliser une connexion L2TP/IPSec.



Dans notre cas nos clients ayant tous cette norme il est préférable de ne pas cocher cette case pour des raison de sécurité.

1. Cliquez sur **Appliquer** pour que la modification prenne effet.