GlobalProtect pour Linux (Ubuntu / CentOS)

Guide d'utilisation

Table des matières

GlobalProtect avec client Linux OpenConnect

Openconnect est un client VPN SSL supporté sur Debian, Ubuntu,CentOS, Fedora, RedHat

Openconnect est le seul client recommandé. Les autres clients Linux ne seront pas supportés.

Installation OpenConnect Linux Debian / Ubuntu

Versions supportées : ***Ubuntu 18.4 ou 16.04***

sudo apt-get install openconnect

Attention : le protocole gb (Global Protect) n'est géré par openconnect que depuis la version 8.0.
Veuillez vérifier la version de votre client avant de poursuivre cette documentation.

sudo openconnect --version *(avec deux tiret)*

Installation OpenConnect Linux CentOS / Fedora / RedHat

Versions supportées : ***Centos 5 minimum***

yum –y install openconnect

Attention : le protocole gb (Global Protect) n'est géré par openconnect que depuis la version 8.0.
Veuillez vérifier la version de votre client avant de poursuivre cette documentation.

openconnect --version *(avec deux tiret)*

Il se peut que les paquetages ne soient pas disponibles si le dépôt logiciel afférent est manquant.
En fonction de votre version d'Entreprise ou CentOs, il vous suffit – dans ce cas – d'ajouter les paquetages depuis le dépôt EPEL comme suit :

Enterprise Linux 5 ou Centos 5

rpm -Uvh http://download.fedoraproject.org/pub/epel/5/i386/epel-release-5-4.noarch.rpm

yum install foo

Enterprise Linux 6 ou Centos 6

rpm -Uvh http://download.fedoraproject.org/pub/epel/6/i386/epel-release-6-8.noarch.rpm

yum install foo

Enterprise Linux 7 ou Centos 7

rpm -Uvh http://download.fedoraproject.org/pub/epel/7/x86_64/e/epel-release-7-5.noarch.rpm

yum install foo

Connexion accès à distance Openconnect Debian / Ubuntu / CentOS Fedora / RegHat

openconnect --protocol=gp -u prenom.nom vpn.universite-paris-saclay.fr

ou

sudo openconnect --protocol=gp -u prenom.nom vpn.universite-paris-saclay.fr

Saisissez votre mot de passe

```
POST https://vpn.universite-paris-saclay.fr/ssl-vpn https://vpn.universite-
paris-saclay.fr/ssl-vpn/prelogin.esp?tmp=tmp&clientVer=4100&clientos=Linux
Connected to 129.175.255.100:443
Négociation SSL avec vpn.universite-paris-saclay.fr
Connected to HTTPS on vpn.universite-paris-saclay.fr
…
```

Des messages d'erreur peuvent apparaître, n'en tenez pas compte si la connexion est bien établie.

La connexion VPN est alors établie.

Lorsque vous n'aurez plus besoin d'accéder aux systèmes nécessitant un accès sécurisé, n'oubliez pas de vous déconnecter. En effet, le nombre de connexions sécurisées étant limités, il est important de les libérer dès que possible. Pour se faire, il faut :

1. Appuyez sur les touches Ctrl + C pour arrêter OpenConnect.
2. Fermer votre terminal.

Il est possible d'utiliser openconnect en mode graphique si `network-manager-openconnect` et `network-manager-openconnect-gnome` (debian et ubuntu) sont installés.

GlobalProtect avec client linux StrongSwan

Installation StrongSwan Ubuntu

sudo apt-get install strongswan

Installation StrongSwan CentOS

yum install strongswan

Configuration StrongSwan Ubuntu / CentOS

Modifier les fichiers de configuration (*ipsec.conf* / *ipsec.secrets*) comme indiqué ci-après. Ces fichiers sont habituellement dans le répertoire */etc/strongswan*.

ipsec.conf

config setup

conn %default

ikelifetime=20m
reauth=yes
rekey=yes
keylife=10m
rekeymargin=3m
rekeyfuzz=0%
keyingtries=1
type=tunnel

conn VPNUPS

keyexchange=ikev1
ikelifetime=1440m
keylife=60m
aggressive=yes
ike=aes-sha1-modp1024,aes256
esp=aes-sha1
xauth=client
*left=**adresseIP-client***
*leftid=@#**groupeVPN-Hex***
leftsourceip=%modeconfig
leftauth=psk
rightauth=psk
leftauth2=xauth
right=vpn.universite-paris-saclay.fr
rightid=129.175.255.100
rightsubnet=0.0.0.0/0
*xauth_identity=**nomutilisateur***
auto=add

Remplacer les valeurs suivantes par :

adresseIP-client : adresse IP du PC client, par exemple *192.168.1.10*

groupeVPN-Hex : valeur fournie lors de la création du compte VPN. En cas d'oubli *securite.di@universite-paris-saclay.fr*
nomutilisateur : identifiant de la forme *prenom.nom* (compte Adonis, mail)

ipsec.secrets

*: PSK "**motdepasseVPN**"*
nomutilisateur *: XAUTH "**motdepasseutilisateur**"*

Remplacer les valeurs suivantes par:

motdepasseVPN : valeur fournie lors de la création du compte VPN. En cas d'oubli *securite.di@universite-paris-saclay.fr*
nomutilisateur : identifiant de la forme *prenom.nom* (compte Adonis, mail)
motdepasseutilisateur :mot de passe associé au login *prenom.nom*

Attention, le mot de passe utilisateur est en clair dans le fichier *ipsec.secrets*. Il est donc nécessaire de protéger ce fichier (écriture et lecture uniquement par le compte *root*).

Connexion accès à distance StrongSwan Ubuntu

ipsec start
ipsec up VPNUPS

La connexion VPN est alors établie.
Pour se déconnecter de la connexion VPN, ***ipsec stop***

Connexion accès à distance StrongSwan CentOS

strongswan start
strongswan up VPNUPS

La connexion VPN est alors établie.
Pour se déconnecter de la connexion VPN, ***strongswan stop***