Reliez un réseau domestique à l'aide d'un VPN

1 INTRODUCTION

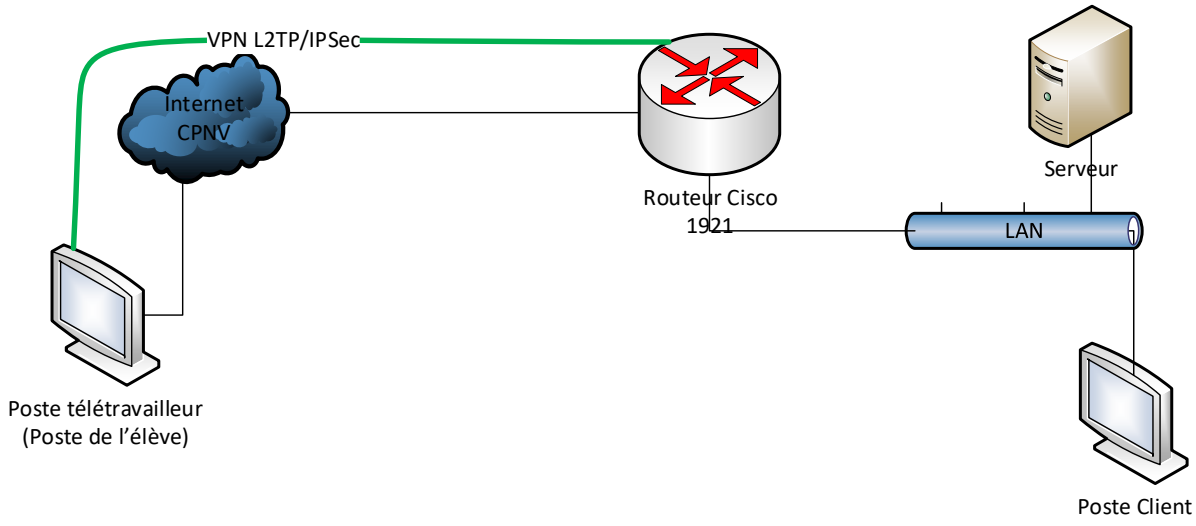
- Durée estimée : 30 minutes

1.1 Objectif

Configuration d'un VPN Accès distant avec L2TP/IPSEC afin qu'un télétravailleur puisse accéder à des ressources (partage de fichiers) du LAN depuis le WAN (réseau CPNV)

1.2 Scénario

Au cours de cet exercice, vous allez modifier la configuration du routeur afin d'accepter des connexions de type VPN accès distant depuis le réseau WAN.



2 CREER UNE RESSOURCE

Sur le serveur, créer un partage réseau « commun » accessible en lecture et écriture à l'utilisateur « User1 », mot de passe « Test123$ ».

Vérifier à l'aide du poste client que l'écriture et l'ajout de fichiers est possible, depuis le poste client \\serveur\commun
Vérifier que vous n'êtes pas capable de à l'aide du lien \\192.168.xx.10\commun accéder au partage de fichier depuis votre machine physique.

3 MISE EN PLACE DU VPN DU RESEAU DOMESTIQUE

- Sur le routeur cisco (virtuel), adapter la configuration suivante à votre environnement

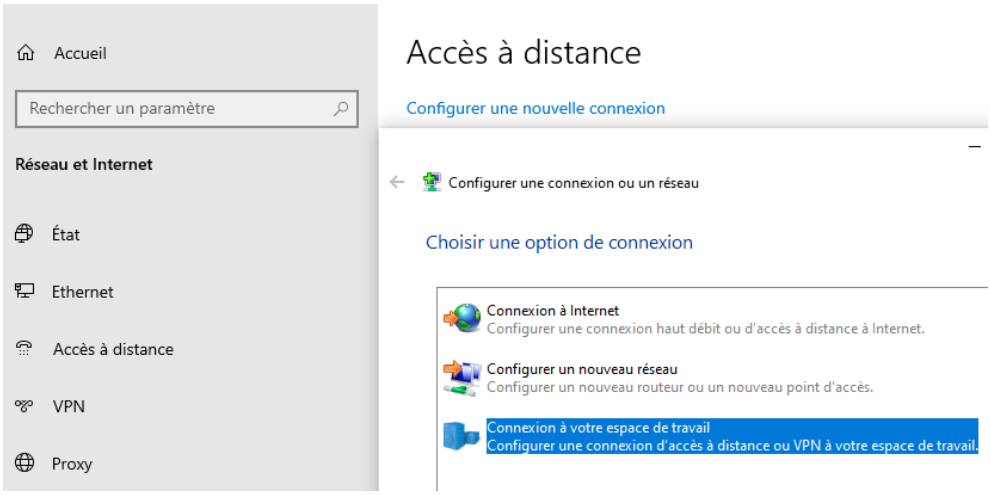
```
aaa new-model
aaa authentication ppp VPDN_AUTH local

vpdn enable
!
vpdn-group L2TP
```

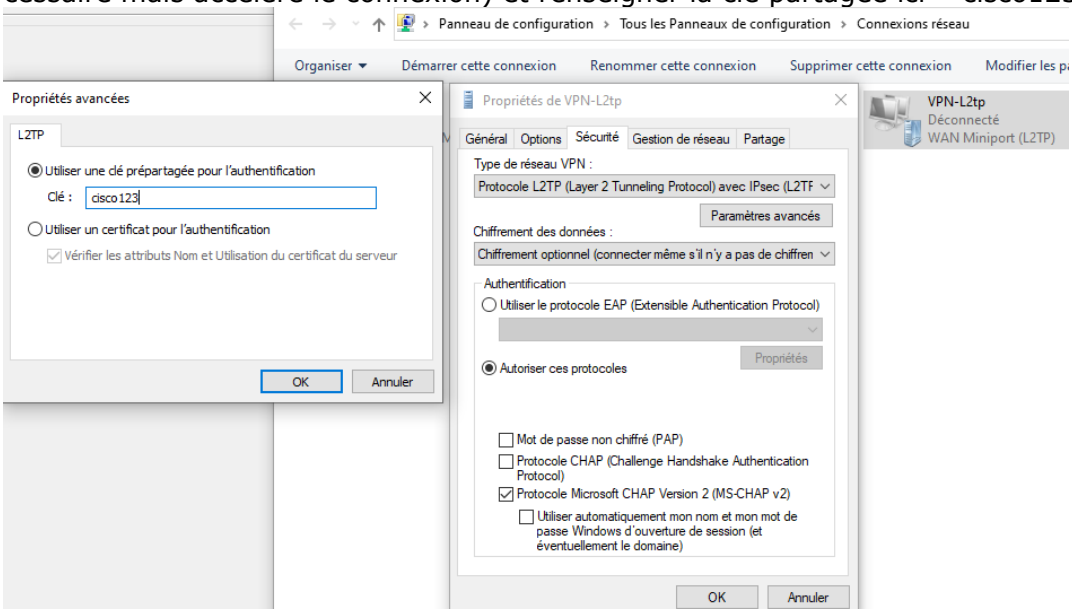
```
 ! Default L2TP VPDN group
 accept-dialin
  protocol l2tp
  virtual-template 1
  no l2tp tunnel authentication
!
! Création d'un utilisateur pour l'accès au VPN
username cisco privilege 15 password 0 cisco
!
crypto isakmp policy 1
 encr 3des
 hash sha
 authentication pre-share
 group 2
 lifetime 86400
!
! Création d'une clé partagée pour l'IPSec
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set L2TP-Set2 esp-3des esp-sha-hmac
 mode transport
!
crypto dynamic-map dyn-map 10
 set nat demux
 set transform-set L2TP-Set2
!
crypto map outside_map 65535 ipsec-isakmp dynamic dyn-map
!
interface GigabitEthernet1/0
 description LAN
 ip address 192.168.23.1 255.255.255.0
 ip nat inside
! Création d'une interface pour crocher le VPN
interface Loopback1
 description loopback for IPsec-pool
 ip address 1.1.1.11 255.255.255.255
interface FastEthernet0/0
 description WAN
 ip address dhcp
 ip nat outside
 ! Pour que l'utilisateur puisse recevoir un tunnel crypté
 crypto map outside_map
!
! Création d'un template pour les connexions VPN
interface Virtual-Template1
 ip unnumbered Loopback1
 peer default ip address pool l2tp-pool
 ppp authentication ms-chap-v2 VPDN_AUTH
!
! Pool d'adresse IP qui seront distribuée au télétravailleur lors de la connexion
ip local pool l2tp-pool 1.1.1.1 1.1.1.10
! Route par défaut
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
ip access-list extended NAT
 permit ip any any
ip nat inside source list NAT interface FastEthernet0/0 overload
```

4 CONFIGURATION DU CLIENT VPN POUR L'ACCES DISTANT

Windows 10 possède un client VPN qui supporte de multiples protocoles dont l'IPSec. Pour configurer le client VPN, créer une nouvelle connexion « accès à distance » comme sur l'illustration ci-dessous.



Une fois la connexion créée, une nouvelle carte réseau sera disponible. Modifier les paramètres de la carte réseau VPN afin de spécifier le protocole (par forcément nécessaire mais accélère le connexion) et renseigner la clé partagée ici « cisco123 »



5 TEST DE LA CONFIGURATION

Sur votre pc, lancer la connexion VPN et vérifier que le partage interne du serveur est accessible depuis votre machine du CPNV à l'aide du lien suivant : \\192.168.xx.10\commun

6 REFERENCE

https://community.cisco.com/t5/security-documents/l2tp-over-ipsec-on-cisco-ios-router-using-windows-8/ta-p/3142831