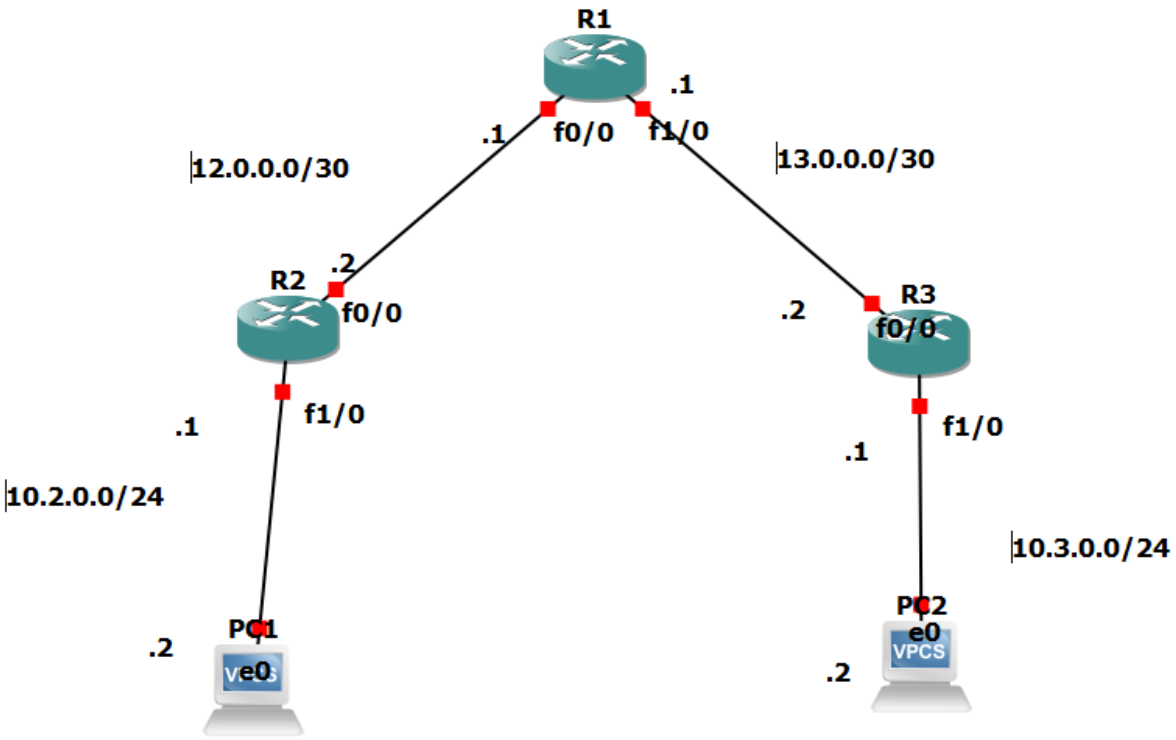
TP : Configuration VPN de type site to site avec IPsec



Etape 1 : Configurer le ISAKMP policy (pour IKE phase 1)

IPSEC IKE control plan ESP AH data plane

R2: Aes 3des

R3: 3DES

R1(config)#crypto isakmp policy 1

Configure une authentification par clé partagée :

R1(config-isakmp)#authentication pre-share

Définir l’algorithme de cryptage symétrique à utiliser :

R1(config-isakmp)#encryption aes

Définir les paramètres de l’algorithme Diffie Hellman :

R1(config-isakmp)#group 2

Fonction de hachage :

R1(config-isakmp)#hash sha

Pour vérifier: R1#show crypto isakmp policy

Configurer pre-shared keys:

R1(config)#crypto isakmp key IDOSR address 13.0.0.2

Etape 2 : Créer IPSEC transform-set (pour IKE phase2)

R1(config)#crypto ipsec transform-set ISTA esp-aes 256 esp-sha-hmac

R1(config)#crypto ipsec security-association lifetime seconds 3600 (optional)

Pour vérifier: R1# show crypto ipsec transform-set

R1# show crypto ipsec sa

Etape 3 : Definir le traffic ciblé

R1(config)#ip access-list extended LAN2_LAN3

R1(config-ext-nacl)#permit ip 10.2.0.0 0.0.0.255 10.3.0.0 0.0.0.255

Etape 4 : Créer le crypto map

R1(config)#crypto map VPN_ISTA 10 ipsec-isakmp
R1(config-crypto-map)#match address LAN2_LAN3
R1(config-crypto-map)#set peer 13.0.0.2
R1(config-crypto-map)#set transform-set ISTA

Pour Vérifier: R1# show crypto map

Etape 5: Asigner le crypto map à l'interafce

R1(config)#int f0/0
R1(config-if)#crypto map VPN_ISTA