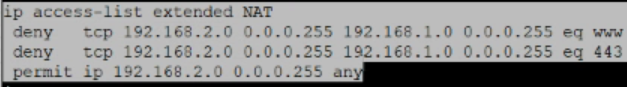
FAI ne fait rien pas configuré sauf interfaces

idem webserver pc et switch ip uniquement et allumé

vpnclient et server allumé et une ip par interfaces conf de base

le nat est des deux cotés nat avec access-list étendu

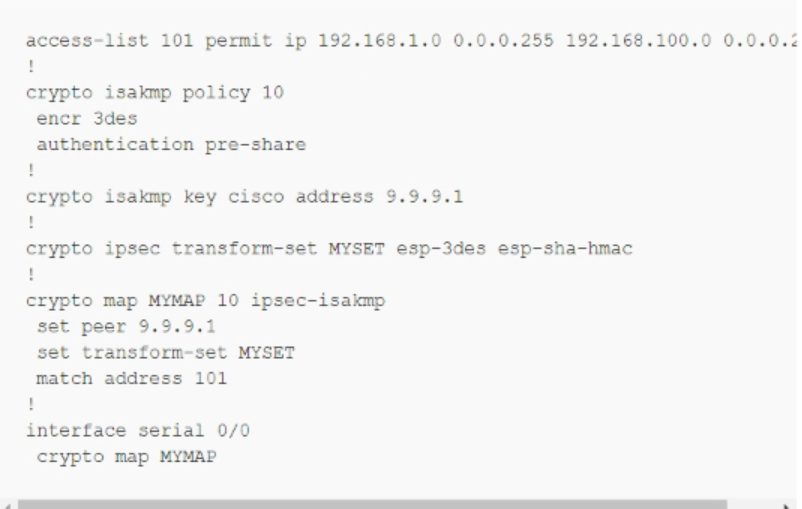


Nat prioritaire sur vpn pour envoie paquet donc on conf cette access list pour dire au nat ces paquets ne sont pas envoyés du réseau (client) refusé si ca vient du client vers serveur et vont vers port 80 ou 443

Permit permet de transmettre tout le reste

Vu que le nat deny les paquets ils sont envoyable depuis le vpn  
  
<https://packetu.com/2012/05/29/defining-the-need-for-nat-exemption/>

Pour vpn



Même conf coté serveur ou client

Cette acceslist correspond au vpn autorise tout donc client vers webserver en 80 ou 443 le reste passe par le nat

Internet Security Association and Key Management Protocol

Crypto isakmp est le nom du groupe

Le chiffrement est fait par algo 3des (168bit triple des)

Et réalisé par une clé partagé cette clé servira au communication (le choix le plus adapté pour une topologie avec pas bcp de poste)

Crypto isakmp cisco address 9.9.9.1 c’est l’adresse du routeur avec qui on va communiquer

Crypto ipsec transform-set permet de définir en transform-set MYSET esp est une encapsulation qui permet d’assurer l’intégrité des données déjà chiffré

Donc vérifier si paquet est pas modifié et vérifié si l’envoie est au bonne endroit

Crypto map est la conf qu’on av créer nommé mymap ipsec vu qu’on fait un ipsec

Set peer c’est le routeur avec qui on communique

On indique le transform set crée au-dessus

Et on lui dit d’utiliser l’acces list 101

Et on définit sur l’interface cité fai du routeur 0/0 la map qui vient d’être crée

Clé diffie helman

Au début

Les deux routeurs

Bob et alice se mettent d’accord sur un nombre de base et premier commun

Le premier routeur alice prend un nombre secret appelé petit a et envoie à bob grand A qui vaut (G^a) % P

Bob fais la même chose avec b et grand B est envoyé a alice (G^b) %P

Alice calcule ce quelle a recu de bob (GRAND B ^a ) % P

Et bob fais la même chose inversé de son coté

Et avec ca il tombe sur le même nombre a la fin

Cette technique est très sécurisé car c’est quasiment impossible de retrouver les différents nombres existants

Ce protocole est vulnérable a man in the middle puisque c’est lui qui envoie la clé

