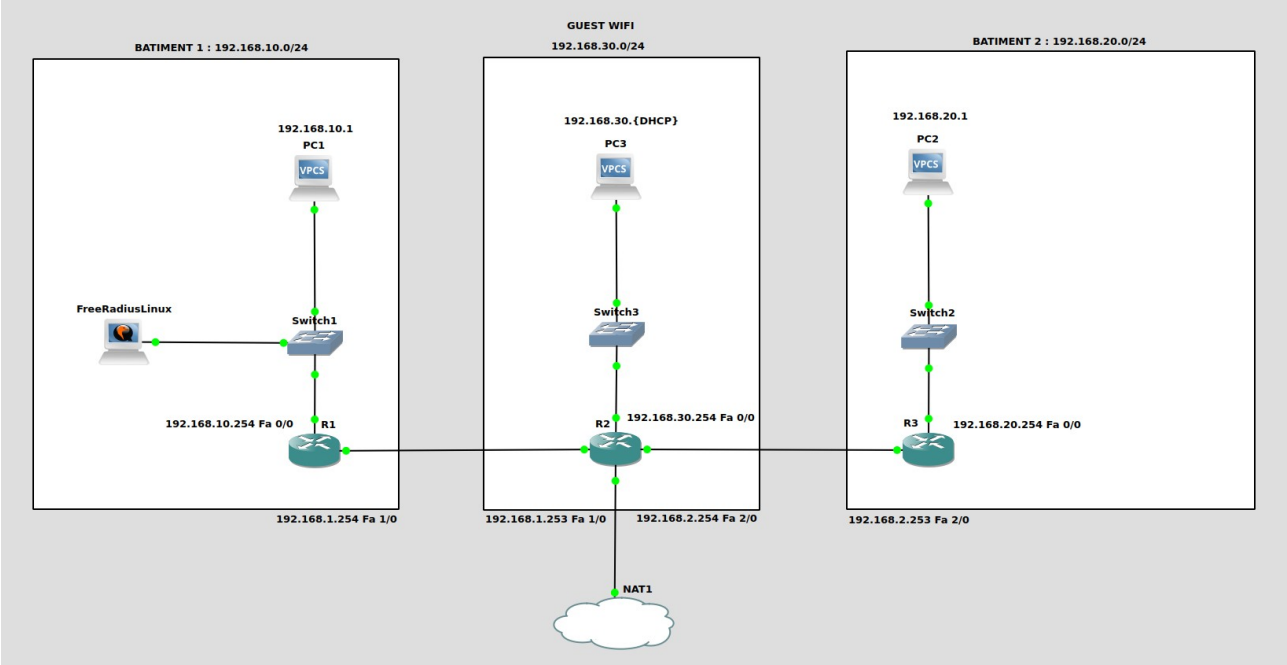
Travaux pratiques
VPN IPsec CISCO de site à site sur GNS3

Je vais vous ici montrer comment créer une liaison d'interconnexion site à site, au travers d'un réseau non sécurisé avec authentification RADIUS sur les routeurs.
Cette liaison est un tunnel VPN IPsec utilisé afin de sécuriser une connexion entre deux sites.
Le TP vise à montrer la configuration de base pour l'établissement du VPN IPsec site à site (de routeur à routeur), reposant sur le protocole ISAKMP avec secret partagé.
Chaque site reproduit l'image d'un petit réseau local accédant à internet via un routeur NAT avec fonction "overload".

La topologie utilisée pour la maquette



Les routeurs utilisés sont des Cisco C7200.

Configuration de base de R1 :

R1>enable
R1#configure terminal
R1(config)#hostname R1
R1(config)#interface FastEthernet 0/0
R1(config-if)#no shutdown
R1(config-if)#ip address 192.168.10.254 255.255.255.0
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#interface FastEthernet 1/0
R1(config-if)#no shutdown
R1(config-if)#ip address 192.168.1.254 255.255.255.0
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.253

Mise en place du SSH sur R1 :

R1(config)#hostname R1
R1(config)#ip domain-name cesi
R1(config)#crypto key generate rsa general-keys modulus 2048
R1(config)#ip ssh version 2
R1(config)#service password-encryption
R1(config)#username admin privilege 15 password 0 cesi
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#transport input telnet ssh
R1(config)#exit

Mise en place du routage OSPF sur R1 :

R1(config)#router ospf 1
R1(config-router)#network 192.168.10.0 0.0.0.255 area 0
R1(config-router)#network 192.168.1.0 0.0.0.255 area 0
R1(config)#exit

Mise en place de la fonction NAT sur R1 :

R1(config)#access-list 100 deny ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
R1(config)#access-list 100 permit ip 192.168.10.0 0.0.0.255 any
R1(config)#ip nat inside source list 100 interface FastEthernet 1/0 overload
R1(config)#do wr

Configuration de base de R2 :

R2>enable
R2#configure terminal
R2(config)#interface FastEthernet 0/0
R2(config-if)#no shutdown
R2(config-if)#ip address 192.168.30.254 255.255.255.0
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#interface FastEthernet 1/0
R2(config-if)#no shutdown
R2(config-if)#ip address 192.168.1.253 255.255.255.0
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#interface FastEthernet 2/0
R2(config-if)#no shutdown
R2(config-if)#ip address 192.168.2.254 255.255.255.0
R2(config)-if#ip nat inside
R2(config-if)#exit
R2(config)#interface FastEthernet 3/0
R2(config-if)#no shutdown
R2(config-if)#ip address dhcp
R2(config-if)#ip nat outside
R2(config-if)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 192.168.122.1

Mise en place du SSH sur R2 :

R2(config)#hostname R2
R2(config)#ip domain-name cesi
R2(config)#crypto key generate rsa general-keys modulus 2048
R2(config)#ip ssh version 2
R2(config)#service password-encryption
R2(config)#username admin privilege 15 password 0 cesi
R2(config)#line vty 0 4
R2(config-line)#login local
R2(config-line)#transport input telnet ssh
exit

Mise en place du routage OSPF sur R2 :

R2(config)#router ospf 1
R2(config-router)#network 192.168.1.0 0.0.0.255 area 0
R2(config-router)#network 192.168.2.0 0.0.0.255 area 0
R2(config-router)#network 192.168.30.0 0.0.0.255 area 0
R2(config)# exit

Mise en place de la fonction NAT sur R2 :

R2(config)#access-list 100 permit any
R2(config)#ip nat inside source list 100 interface fastEthernet 3/0 overload

Mise en place du DHCP sur R2 :

R2(config)#ip dhcp pool GUEST-WIFI
R2(dhcp-config)#network 192.168.30.0 255.255.255.0
R2(dhcp-config)#domain-name cesi
R2(dhcp-config)#dns-server 8.8.8.8
R2(dhcp-config)#lease 0 8
R2(dhcp-config)#exit
R2(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.10
R2(config)#do wr

Configuration de base de R3 :

R3>enable
R3#configure terminal
R3(config)#interface FastEthernet 0/0
R3(config-if)#no shutdown
R3(config-if)#ip address 192.168.20.254 255.255.255.0
R3(config-if)#ip nat inside
R3(config-if)#exit
R3(config)#interface FastEthernet 2/0
R3(config-if)#no shutdown
R3(config-if)#ip address 192.168.2.253 255.255.255.0
R3(config-if)#ip nat outside
R3(config-if)#exit
R3(config)#ip route 0.0.0.0 0.0.0.0 192.168.2.254

Mise en place du SSH sur R3 :

R3(config)#hostname R3
R3(config)#ip domain-name cesi
R3(config)#crypto key generate rsa general-keys modulus 2048
R3(config)#ip ssh version 2
R3(config)#service password-encryption
R3(config)#username admin privilege 15 password 0 cesi
R3(config)#line vty 0 4
R3(config-line)#login local
R3(config-line)#transport input telnet ssh
R3(config)#exit

Mise en place du routage OSPF sur R3 :

R3(config)#router ospf 1
R3(config-router)#network 192.168.20.0 0.0.0.255 area 0
R3(config-router)#network 192.168.2.0 0.0.0.255 area 0
R3(config)#exit

Mise en place de la fonction NAT sur R3 :

R3(config)#access-list 100 deny ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
R3(config)#access-list 100 permit ip 192.168.20.0 0.0.0.255 any
R3(config)#ip nat inside source list 100 interface FastEthernet 2/0 overload

Mise en place du tunnel VPN Ipsec

Configuration de la négociation des clés (phase 1)

Détail de la configuration sur R1 :

L'objectif est d'activer le protocole 'IKE', configurer le protocole 'ISAKMP' qui gère l'échange des clés et établir une stratégie de négociation des clés et d'établissement de la liaison VPN.
La clé pré partagée (PSK) sera définie avec pour valeur 'cesi'.

On va ici utiliser les paramètres suivants:

- Encryptage AES
- Mode de secret partagé PSK
- Authentification par clé pré-partagées
- Algorithme de hachage SHA (valeur par défaut)
- Méthode de distribution des clés partagées DH-2 (clés Diffie-Hellman groupe 2 - 1024bits)
- Durée de vie 86400 secondes (valeur par défaut)

On spécifie le protocole de hash utilisé, le type et la durée de validité des clés de sessions.
On indique ensuite si le routeur 'peer' (celui situé au bout du tunnel) est identifié par un nom ou son adresse.

R1(config)#crypto isakmp enable	→ active IKE
R1(config)#crypto isakmp policy 10	→ active une politique IKE
R1(config-isakmp)# encryption aes	→ fixe l'algorithme de cryptage
R1(config-isakmp)# authentication pre-share	→ fixe la méthode d'authentification
R1(config-isakmp)# hash sha	→ fixe l'algorithme de hachage
R1(config-isakmp)# group 2	→ définit le groupe Diffie Hellman
R1(config-isakmp)# lifetime 86400	→ fixe la durée de vie de la SA
R1(config-isakmp)#exit	
R1(config)# crypto isakmp key cesi address 192.168.2.253	→ indique la clé partagée et l'adresse du routeur pair qui doit être contacté

Configuration de la méthode de chiffrage des données (phase 2)

Il faut établir l'opération en trois phases

1. Créer la méthode de cryptage (transform-set) que je nomme "VPNLABO", avec "esp-aes" comme méthode de cryptage et "esp-sha-hmac" comme méthode d'authentification.
On définit la durée de vie de la clé soit en durée (secondes).

2. Je créé ensuite une liste de contrôle d'accés (access-list) que je nomme "VPN", servant à identifier le trafic à traiter par le tunnel VPN. Pour R1, ce sera le trafic d'origine 192.168.10.0/24 à destination de 192.168.20.0/24.

3. Je déclare finalement une carte de cryptage (crypto-map) que j'appelle "CARTEVPN", servant à spécifier le pair distant, le 'transform set' et l'access list.

Voici le détail de la configuration sur R1 :

R1(config)#crypto ipsec transform-set VPNLABO esp-aes esp-sha-hmac
R1(config)#crypto ipsec security-association lifetime seconds 86400
R1(config)#ip access-list extended VPN
R1(config-ext-nacl)#permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
R1(config-ext-nacl)#exit
R1(config)#crypto map CARTEVPN 10 ipsec-isakmp
R1(config-crypto-map)# match address VPN
R1(config-crypto-map)#set peer 192.168.2.253
R1(config-crypto-map)#set transform-set VPNLABO
R1(config-crypto-map)#exit

Il faut maintenant appliquer la crypto-map à l'interface WAN de R1.

R1(config)# interface FastEthernet 1/0
R1(config-if)#crypto map CARTEVPN
R1(config-if)#do wr

Le R1 est prêt, il reste à faire l'équivalent sur R3.

Voici le détail de la configuration sur R3
La configuration est très similaire, il suffit d'adapter les adresses des réseaux à filtrer et préciser l'adresse du routeur pair.

R3(config)#crypto isakmp enable
R3(config)#crypto isakmp policy 10
R3(config-isakmp)# encryption aes
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#hash sha
R3(config-isakmp)#group 2
R3(config-isakmp)#lifetime 86400
R3(config-isakmp)#exit

R3(config)# crypto isakmp key cesi address 192.168.1.254

R3(config)# crypto ipsec transform-set VPNLABO esp-aes esp-sha-hmac
R3(config)# crypto ipsec security-association lifetime seconds 86400
R3(config)# ip access-list extended VPN
R3(config-ext-nacl)# permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
R3(config-ext-nacl)# exit

R3(config)# crypto map CARTEVPN 10 ipsec-isakmp
R3(config-crypto-map)# match address VPN
R3(config-crypto-map)#set peer 192.168.1.254
R3(config-crypto-map)#set transform-set VPNLABO
R3(config-crypto-map)#exit

R3(config)# interface FastEthernet 2/0
R3(config-if)#crypto map CARTEVPN
R3(config-if)#do wr

Vérification du fonctionnement tunnel VPN

Pour établir la liaison VPN et vérifier le fonctionnement, il faut envoyer du trafic au travers du tunnel, en faisant un ping entre les stations.
Une fois le tunnel configuré, plusieurs commandes permettent de vérifier si le tunnel fonctionne.

- R1#show crypto isakmp policy
- R1#show crypto isakmp sa
- R1#show crypto ipsec sa
- R1#show crypto engine connection active

Mise en place de l’authentification RADIUS

Dans l'optique de garantir l'aspect sécuritaire et bénéficier d'une utilisation optimale des ressources d'un réseau, la centralisation des informations est d'une importance cruciale.

Le but de ce TP est de se connecter à distance par SSH à un routeur en utilisant des comptes stockés sur un serveur RADIUS.

Configuration du serveur FreeradiusLinux

root@debian:~# apt install freeradius freeradius-utils -y

On précise l'adresse réseau et le mot de passe dans le fichier /etc/freeradius/3.0/clients.conf pour y mettre ceci :

root@debian:~# nano /etc/freeradius/3.0/clients.conf

```
client 192.168.10.0 {
        ipaddr = 192.168.10.0/24
        secret = cesi123
}

client 192.168.20.0 {
        ipaddr = 192.168.20.0/24
        secret = cesi123
}

client 192.168.30.0 {
        ipaddr = 192.168.30.0/24
        secret = cesi123
}

client 192.168.1.0 {
        ipaddr = 192.168.1.0/24
        secret = cesi123
}

client 192.168.2.0 {
        ipaddr = 192.168.2.0/24
        secret = cesi123
}
```

On crée les comptes utilisateurs dans le fichier /etc/freeradius/3.0/users
Nous allons créer deux comptes (antonin et nathan)

root@debian:~# nano /etc/freeradius/3.0/users

```
antonin Cleartext-Password := "cesi123"
        Reply-Message = "Bienvenue %{User-Name} sur le routeur !"

nathan Cleartext-Password := "boss123"
        Reply-Message = "Bienvenue %{User-Name} sur le routeur !"
```

Configuration du routeur R1 :

R1(config)#aaa new-model
R1(config)#aaa authentication dot1x default group radius
R1(config)#aaa authentication login default group radius
R1(config)#aaa authorization network default group radius
R1(config)#aaa authorization exec default group radius
R1(config)#radius-server host 192.168.10.10 auth-port 1812 acct-port 1646 key cesi123

Avant qu'on aille plus loin, faisons un test en local sur le routeur.

R1# test aaa group radius antonin cesi123 legacy

```
R1#test aaa group radius antonin cesi123 legacy
Attempting authentication test to server-group radius using radius
User was successfully authenticated.
```

L'utilisateur **antonin** est authentifié avec succés !

La configuration est terminée. Nous allons pouvoir tester l'authentification ***RADIUS*** via SSH depuis un poste client.

Connectez vous sur votre routeur R1 à l'aide du compte configuré sur le serveur RADIUS :

ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 -oHostkeyAlgorithms=+ssh-rsa -l <user-radius> <@IP Cisco R1>

```
root@debian:~# ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 -oHostkeyAlgorithms=+ssh-rsa -l antonin 192.168.10.254
(antonin@192.168.10.254) Password:
Bienvenue antonin sur le routeur !

R1>_
```

Vous êtes connecté sur le routeur par l'intermédiaire du serveur RADIUS. Vous pouvez également utiliser la commande « show privilege » afin de vérifier le niveau de privilège du compte utilisé.

Vous êtes à présent capable d'installer un serveur RADIUS et d'implémenter l'authentification par celui-ci sur des routeurs Cisco.