Procédure de mise en place d’un réseau avec site distant et VPN IPsec

Gildas CHERAUD BOISTEAU

BTS Service Informatique aux Organisations option SISR

Sommaire

1 – Descriptif du projet

Contexte professionnel

Dans le cadre de la sécurisation des échanges inter-sites d'une PME fictive, ce projet vise à concevoir et déployer une infrastructure réseau répartie sur deux sites géographiques. L'entreprise souhaite interconnecter ses réseaux locaux via un tunnel VPN IPSec sécurisé, tout en assurant la distribution dynamique des adresses IP et le filtrage des flux.

Le projet s'inscrit dans une logique de mise en œuvre réelle en entreprise, avec une transposabilité complète en environnement atelier. Il mobilise des équipements Cisco ISR 900 Series pour les routeurs, des commutateurs Cisco Catalyst 2960, un serveur Debian pour le DHCP, et deux postes clients.

Objectifs pédagogiques

- Mettre en œuvre une infrastructure réseau multi-sites avec routage et VPN.
- Configurer un serveur DHCP centralisé avec relais sur site distant.
- Appliquer des règles de sécurité réseau via ACLs.
- Documenter et justifier les choix techniques dans une logique professionnelle.
- Tester et valider la connectivité, la sécurité et la performance de l'ensemble.

Résultats attendus

- Les deux sites doivent pouvoir communiquer de manière sécurisée via un tunnel VPN IPSec.
- Les postes clients doivent recevoir une adresse IP dynamique via le serveur DHCP centralisé.
- Le routage doit permettre la connectivité complète entre les sous-réseaux.
- Les ACLs doivent filtrer les flux non autorisés.
- Tous les tests de connectivité, de sécurité et de performance doivent être validés avec succès.

Compétences mobilisées

Code	Compétence
C1.1	Recueillir les besoins et les contraintes techniques
C2.1	Installer et configurer les équipements réseau
C2.2	Sécuriser les équipements et les flux réseau
C3.1	Administrer les services réseau (DHCP, VPN, routage)
C3.2	Diagnostiquer et corriger les dysfonctionnements
C4.1	Rédiger une documentation technique claire et structurée

Délai de réalisation

Durée estimée : 2 semaines, incluant la phase de conception, de configuration, de test et de documentation.

2a – Plan d'adressage des divers réseaux

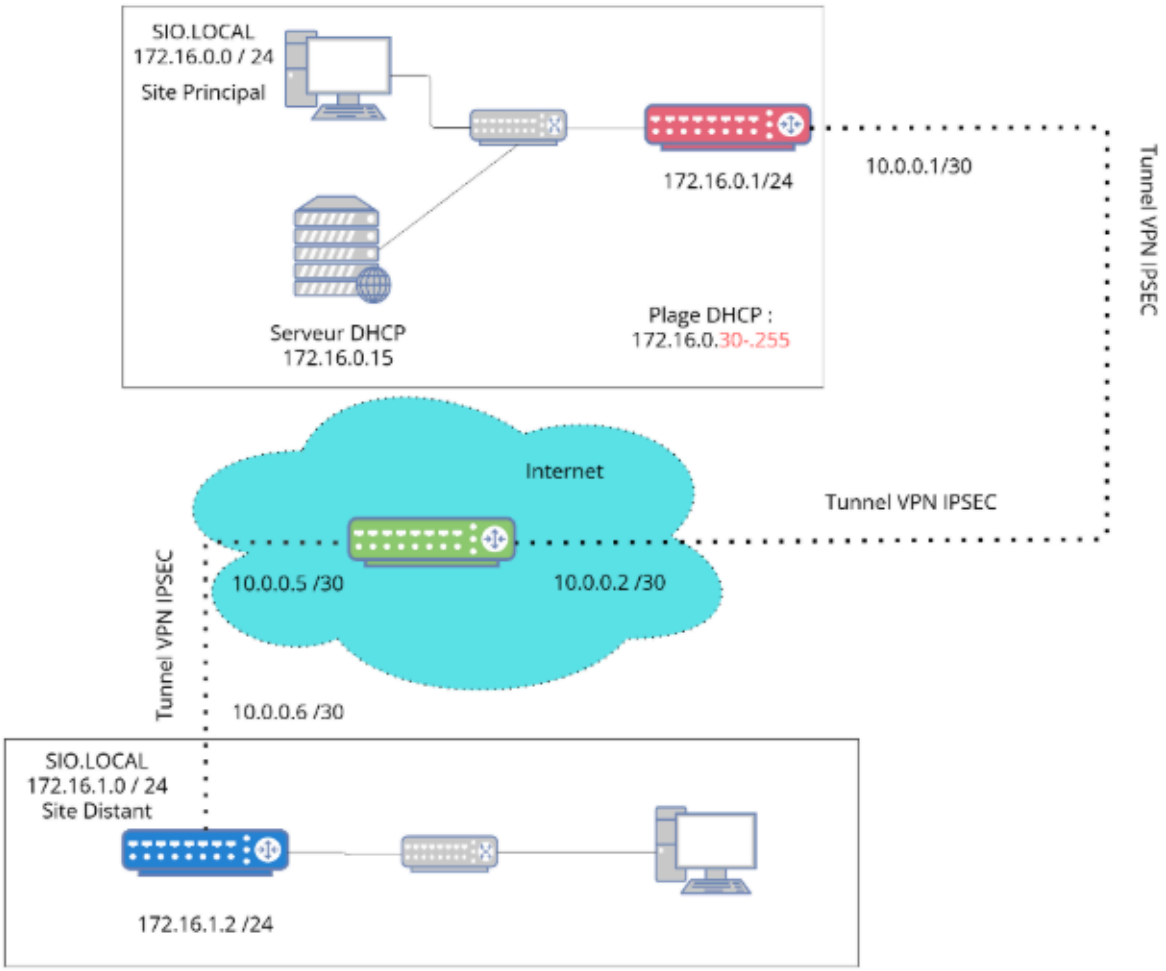
2 réseaux distincts avec des IPs différentes pour éviter les conflits, une plage d'adresse DHCP de 172.16.0.30 à 172.16.0.254 (idem pour 172.168.1.30 à 172.16.1.254)

	Site Principal	Site Distant
Réseau Local	172.16.0.0	172.16.1.0
Routeur LAN	172.16.0.1	172.16.1.2
Serveur DHCP	172.16.0.15	172.16.1.2**
Poste Client	DHCP	DHCP
Interface WAN	10.0.0.1/30	10.0.0.6/30
Passerelle	10.0.0.2/30*	10.0.0.5/30*

*un routeur servant d'internet simulé est placé entre les deux réseaux

** DHCP Relay

2b - Schéma Réseau



3 – Configuration du site principal

Interfaces

```
interface FastEthernet0/0
 ip address 172.16.0.1 255.255.255.0
 no shutdown
interface Serial0/0/0
 ip address 10.0.0.1 255.255.255.252
 no shutdown
```

DHCP

Mise en place du DHCP avec 2 plages DHCP (1 pour chaque site) et des exclusions d'adresses.

```
ip dhcp excluded-address 172.16.0.1 172.16.0.29
ip dhcp excluded-address 172.16.0.15
ip dhcp excluded-address 172.16.1.2
ip dhcp pool SITE_PRINCIPAL
 network 172.16.0.0 255.255.255.0
 default-router 172.16.0.1
 dns-server 8.8.8.8
 domain-name entreprise.local
ip dhcp pool SITE_DISTANT
 network 172.16.1.0 255.255.255.0
default-router 172.16.1.2
dns-server 8.8.8.8
domain-name entreprise.local
```

Routage

Les routes permettent la liaison entre les différents réseaux, ici ils sont fait manuellement mais des protocoles comme RIP existent pour la gestion des routes automatiques

```
ip route 0.0.0.0 0.0.0.0 10.0.0.2
```

```
ip route 172.16.1.0 255.255.255.0 10.0.0.2
```

VPN IPSec (site principal)

Le VPN IPSec permet la sécurisation du trafic passant par internet en créant un tunnel sur le WAN (Internet). La clé VPNKEY est ici en clair mais dans le cas d'une vraie installation elle serait chiffré. Le choix de la mét hode de chiffrage ici permet la sécurisation plus importante du réseau..

```
crypto isakmp policy 10
 encr aes
 hash sha256
 authentication pre-share
 group 2
 lifetime 86400
exit
crypto isakmp key VPNKEY address 10.0.0.6
crypto ipsec transform-set TRANSFORM esp-aes esp-sha-hmac
 mode tunnel
access-list VPN-TRAFFIC permit ip 172.16.0.0 0.0.0.255 172.16.1.0 0.0.0.255
crypto map VPN-MAP 10 ipsec-isakmp
 set peer 10.0.0.6
 set transform-set TRANSFORM
 match address VPN-TRAFFIC
interface Serial0/0/0
 crypto map VPN-MAP
access-list VPN-TRAFFIC permit ip 172.16.0.0 0.0.0.255 172.16.1.0 0.0.0.255
```

4 - Configuration du routeur Internet (simulé)

```
interface Serial0/0/0
```

```
 ip address 10.0.0.2 255.255.255.252
 no shutdown
interface Serial0/0/1
 ip address 10.0.0.5 255.255.255.252
 no shutdown
ip route 172.16.0.0 255.255.255.0 10.0.0.1
ip route 172.16.1.0 255.255.255.0 10.0.0.6
```

5 – Configuration du site distant

Interfaces

```
interface FastEthernet0/0
 ip address 172.16.1.2 255.255.255.0
 ip helper-address 172.16.0.15
 no shutdown
interface Serial0/0/0
 ip address 10.0.0.6 255.255.255.252
 no shutdown
```

Routage

```
ip route 0.0.0.0 0.0.0.0 10.0.0.5
ip route 172.16.0.0 255.255.255.0 10.0.0.5
```

VPN IPSec (site distant)

```
crypto isakmp policy 10
 encr aes
 hash sha256
```

```
 authentication pre-share
 group 2
 lifetime 86400
exit
crypto isakmp key VPNKEY address 10.0.0.1
crypto ipsec transform-set TRANSFORM esp-aes esp-sha-hmac
 mode tunnel
access-list VPN-TRAFFIC permit ip 172.16.1.0 0.0.0.255 172.16.0.0
0.0.0.255
crypto map VPN-MAP 10 ipsec-isakmp
 set peer 10.0.0.1
 set transform-set TRANSFORM
 match address VPN-TRAFFIC
interface Serial0/0/0
 crypto map VPN-MAP
access-list VPN-TRAFFIC permit ip 172.16.1.0 0.0.0.255 172.16.0.0
0.0.0.255
```

6 - Conclusion

A la suite de la réalisation de la procédure, l'ensemble de l'infrastructure réseau fonctionne, le réseau principal communique bien avec le site distant via un VPN IPsec tout en passant par Internet.