2022-2023

MISSION 3 : Mise en place d'un VPN

Sofiane AININE, Daniel GOLGI, , Yvan-loic SOH , Alexandre AUBERMAS, Lina HAOUAS

2022-2023

Sommaire

1.Contexte :

1.1 Présentation de l'entreprise :

Lors de la construction de ce stade, le réseau qui prenait en charge ses bureaux commerciaux et ses services de sécurité proposait des fonctionnalités de communication de pointe. Au fil des ans, la société a ajouté de nouveaux équipements et augmenté le nombre de connexions sans tenir compte des objectifs commerciaux généraux ni de la conception de l'infrastructure à long terme. Certains projets ont été menés sans souci des conditions de bande passante, de définition de priorités de trafic et autres, requises pour prendre en charge ce réseau critique de pointe.

StadiumCompany fournit l'infrastructure réseau et les installations sur le stade.

StadiumCompany emploie 170 personnes à temps plein :

- 35 dirigeants et responsables
- 135 employés

Environ 80 intérimaires sont embauchés en fonction des besoins, pour des événements spéciaux dans les services installations et sécurité.

À présent, la direction de StadiumCompany veut améliorer la satisfaction des clients en ajoutant des fonctions haute technologie et en permettant l'organisation de concerts, mais le réseau existant ne le permet pas.

La direction de StadiumCompany sait qu'elle ne dispose pas du savoir-faire voulu en matière de réseau pour prendre en charge cette mise à niveau. StadiumCompany décide de faire appel à des consultants réseau pour prendre en charge la conception, la gestion du projet et sa mise en œuvre.

Ce projet sera mis en œuvre suivant trois phases. La première phase consiste à planifier le projet et préparer la conception réseau de haut niveau. La deuxième phase consiste à développer la conception réseau détaillée. La troisième phase consiste à mettre en œuvre la conception.

1.2 Présentation du prestataire informatique :

Après quelques réunions, StadiumCompany charge NetworkingCompany, une société locale spécialisée dans la conception de réseaux et le conseil, de la phase 1, la conception de haut niveau.

Créée en 1989, NetworkingCompany est une société spécialiste en infrastructures systèmes et vente de matériel informatique pour professionnels de la vidéo. Employant aujourd'hui 20 ingénieurs réseau, l'activité de NetworkingCompany s'établit à 1,8 millions d'euros de chiffre d'affaires. Son cœur de métier se situe au niveau de l'infrastructure

informatique afin de garantir les besoins des activités « métiers ». NetworkingCompany est l'une des seules sociétés de services informatique qui accompagne réellement et jusqu'au bout ses clients dans le choix et la mise en œuvre de solutions.

Pour créer la conception de haut niveau, NetworkingCompany a tout d'abord interrogé le personnel du stade et décrit un profil de l'organisation et des installations.

NetworkingCompany intervient en mode Projet (Engagement de résultats), Régie (Engagement de moyens) et Infogérance des environnements Windows. Son outil de compétitivité et de productivité réside dans la capitalisation de son savoir-faire, le haut niveau de certification de ses partenariats ainsi qu'une veille technologique active.

NetworkingCompany a développé une expertise forte dans les domaines de la virtualisation, les infrastructures d'accès (Application delivery), l'industrialisation du poste de travail (Itil, Supervision, Télédistribution), les annuaires et la gestion de l'identité.

Reconnu depuis 25 ans comme une entreprise innovante, et avec aujourd'hui plus de 300 collaborateurs, cette société répond avec flexibilité et efficacité à tous les besoins, qu'ils émanent de PME ou de grands comptes. Enfin, NetworkingCompany est en partenariat avec de nombreux gros groupes du monde de l'informatique, tout comme Microsoft, CISCO, HP, Huawei ou encore DELL, pour ne citer que les plus importants.

1.3 Renseignements sur le système actuel

Le site n'est pas sécurisé, c'est pourquoi stadiumCompany fais appel à nous pour le faire.

1.4 Solutions & Choix

Un VPN (Virtual Private Network) est un réseau virtuel s'appuyant sur un autre réseau comme Internet. Il permet de faire transiter des informations, entre les différents membres de ce VPN, le tout de manière sécurisée. On peut considérer qu'une connexion VPN revient à se connecter en réseau local mais en utilisant Internet. On peut ainsi communiquer avec les machines de ce réseau en prenant comme adresse de destination, l'adresse IP local de la machine que l'on veut atteindre. Il existe plusieurs types de VPN fonctionnant sur différentes couches réseau, voici les VPN que nous pouvons mettre en place sur un serveur dédié ou à la maison :

PPTP : Facile à mettre en place, mais beaucoup d'inconvénients liés à la lourdeur du protocole de transport GRE, le matériel réseau (routeur ADSL, wifi, doit être compatible avec le PPTP)

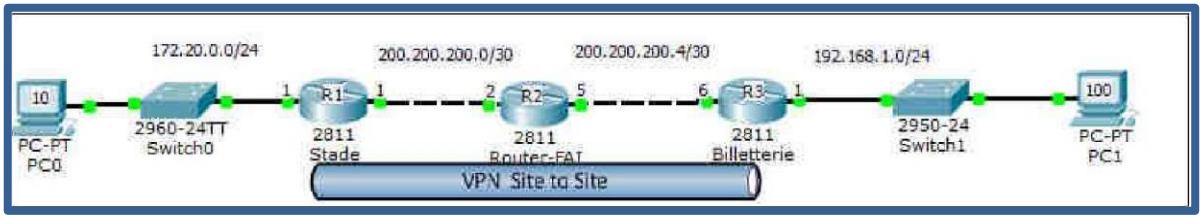
IPsec : Plus efficace que le PPTP en termes de performance, mais aussi très contraignant au niveau de la mise en place.

OpenVPN : La Rolls des VPN, il suffit de se prendre un peu la tête sur la mise en place, mais son utilisation est très souple.

Dans notre cas nous allons utiliser IPsec.

1.5 Schéma réseau

Dans cette activité nous allons avoir besoin de trois routeurs, que nous allons nommer R1, R2 et R3. Nous allons connecter les routeurs entre eux comme dans le schéma ci-dessous :



2. Mise en place de l'infrastructure

2.1 Configuration du Routeur 1

Pour configurer le premier, nous allons procéder comme suit :

- Attribuer les adresses IP aux interfaces FastEthernet

```
interface FastEthernet0/0
 ip address 172.20.0.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 200.200.200.1 255.255.255.252
 duplex auto
 speed auto
```

Nos interfaces sont maintenant configurées, il nous reste à configurer le routage. Nous avons choisi de faire du routage EIGRP.

```
!
router eigrp 1
 network 172.20.0.0 0.0.0.255
 network 200.200.200.0 0.0.0.3
 auto-summary
!
```

La configuration de base de notre R1 est terminée.

2.2 Configuration du Routeur 2

Nous allons faire la même procédure pour le routeur 2 :

- Nous allons d'abord renommer notre routeur

```
R2#show run
Building configuration...

Current configuration : 875 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 25
ip cef
!
!
!
!
!
!
voice-card 0
!
```

- Configuration des adresses IP des deux interfaces

```
interface FastEthernet0/0
 ip address 200.200.200.2 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 200.200.200.5 255.255.255.252
 duplex auto
 speed auto
```

- Configuration du routage

```
router eigrp 1
 network 200.200.200.0 0.0.0.3
 network 200.200.200.4 0.0.0.3
 auto-summary
```

La configuration de base du routeur 2 est terminée.

2.3 Configuration du Routeur 3

Même procédure pour le routeur 3 :

- Configuration du routage et des adresses IP des deux interfaces

```
interface Serial0/1/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/1/1
 no ip address
 shutdown
 clock rate 2000000
!
router eigrp 1
 network 192.168.1.0
 network 200.200.200.4 0.0.0.3
 auto-summary
!
!
!
ip http server
no ip http secure-server
```

La configuration de base du routeur 3 est terminée.

2.4 Test de fonctionnement

Nous allons pinguer le PC du réseau local du stade vers le PC du réseau local de la billetterie.

```
C:\Users\Iris>ping 192.168.1.1

Envoi d'une requête 'Ping'  192.168.1.1 avec 32 octets de données :
Réponse de 192.168.1.1 : octets=32 temps<1ms TTL=255
Réponse de 192.168.1.1 : octets=32 temps<1ms TTL=255
Réponse de 192.168.1.1 : octets=32 temps<1ms TTL=255
Réponse de 192.168.1.1 : octets=32 temps<1ms TTL=255

Statistiques Ping pour 192.168.1.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

3. Mise en place du VPN

Il faut savoir que le VPN se configure juste sur les routeurs d'extrémités dans notre cas le R1 et le R3 on n'aura aucune modification à faire sur le R2.

3.1 Configurations du routeur 1

Etape 1 : Sur le R1 on active les fonctions crypto du routeur (cette fonction est activée de base sur les IOS avec les options cryptographique).

R1(config)#crypto isakmp enable

Etape 2 : Nous allons configurer la police qui détermine quelle encryptions on utilise, quelle Hash, quel type d'authentification, etc.

```
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 5
 lifetime 3600
crypto isakmp key iris123 address 200.200.200.6
!
crypto ipsec security-association lifetime seconds 1800
!
crypto ipsec transform-set 50 esp-3des esp-md5-hmac
!
crypto map stade 10 ipsec-isakmp
 set peer 200.200.200.6
 set security-association lifetime seconds 900
 set transform-set 50
 match address 101
!
!
!
!
interface FastEthernet0/0
 ip address 172.20.0.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 200.200.200.1 255.255.255.252
 duplex auto
 speed auto
 crypto map stade
```

Etape 3 : Ensuite nous devons configurer la clef

```
crypto isakmp key iris123 address 200.200.200.6
```

Etape 4 : On configure les options de transformations des données et on fixe un temps avec ***Lifetime.***

```
crypto ipsec transform-set 50 esp-3des esp-md5-hmac
crypto ipsec security-association lifetime seconds 1800
```

Etape 5 : Cette étape consiste à créer une ACL qui va déterminer le trafic.

```
access-list 101 permit ip 172.20.0.0 0.0.0.255 192.168.1.0 0.0.0.255
```

Etape 6 (dernière étape) : Dans cette étape nous allons configurer la crypto map qui va associer l'access-list, le trafic et la destination.

```
R1#sh crypto map
Crypto Map "stade" 10 ipsec-isakmp
        Peer = 200.200.200.6
        Extended IP access list 101
            access-list 101 permit ip 172.20.0.0 0.0.0.255 192.168.1.0 0.0.0.255
        Current peer: 200.200.200.6
        Security association lifetime: 4608000 kilobytes/900 seconds
        PFS (Y/N): N
        Transform sets={
                50,
        }
        Interfaces using crypto map stade:
                FastEthernet0/1
```

On vérifie si la crypto map est en marche, si elle fonctionne on doit voir le message cidessous :

```
*Jan  1 02:24:45.059: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

3.2 Configuration du VPN sur le R3

On refait la même configuration que sur le R1 :

Etape 1 :

```
R3(config)#crypto isakmp enable
```

Etape 2 :

```
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#encryption 3des
R3(config-isakmp)#hash md5
R3(config-isakmp)#group 5
R3(config-isakmp)#lifetime 3600
R3(config-isakmp)#exit
```

Etape 3 :

```
R3(config)#crypto isakmp key iris123 address 200.200.200.1
```

Etape 4 :

```
R3(config)#crypto ipsec transform-set 50 esp-3des esp-md5-hmac
R3(cfg-crypto-trans)#crypto ipsec security-association lifetime seconds 1800
```

Etape 5 :

```
R3(config)#$ 101 permit ip 192.168.1.0 0.0.0.255 172.20.0.0 0.0.0.255
```

Etape 6 :

```
R3(config)#crypto map billeterie 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R3(config-crypto-map)#set peer 200.200.200.1
R3(config-crypto-map)#set transform-set 50
R3(config-crypto-map)#set security-association lifetime seconds 900
R3(config-crypto-map)#match address 101
R3(config-crypto-map)#exit
R3(config)#interface fa0/1
R3(config-if)#crypto map billeterie
R3(config-if)#
*Jan  1 02:24:45.059: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

3.3 Vérifications

Nous allons lancer plusieurs requêtes afin de vérifier si on a bien configuré nos routeurs :

- Ping PC ❼ 192.168.1.2

```
C:\Users\Iris>ping 192.168.1.2

Envoi d'une requête 'Ping'  192.168.1.2 avec 32 octets de données :
Réponse de 192.168.1.2 : octets=32 temps<1ms TTL=125
Réponse de 192.168.1.2 : octets=32 temps<1ms TTL=125
Réponse de 192.168.1.2 : octets=32 temps<1ms TTL=125
Réponse de 192.168.1.2 : octets=32 temps<1ms TTL=125

Statistiques Ping pour 192.168.1.2:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

- On vérifie ensuite les informations retournées par le VPN sur R1 et R3

```
R3#show crypto ipsec transform-set
Transform set 50: { esp-3des esp-md5-hmac  }
   will negotiate = { Tunnel,  },
```

- On vérifie la map VPN : **R1#show crypto map / R3#show crypto map** - On vérifie la sécurité : IPsec

```
R1#show crypto ipsec sa

interface: FastEthernet0/1
    Crypto map tag: stade, local addr 200.200.200.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.20.0.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   current_peer 200.200.200.6 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 200.200.200.1, remote crypto endpt.: 200.200.200.6
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
     current outbound spi: 0x0(0)

     inbound esp sas:
```

- Pour finir on vérifie les opérations d'Isakmp :

```
R1#show crypto isakmp sa
dst             src             state          conn-id slot status
```

- Show run :

```
R1#show run
Building configuration...

Current configuration : 1363 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 25
ip cef
!
!
!
!
!
!
voice-card 0
!
```

4.ANNEXE

VPN : Un VPN (Virtual Private Network) est un « réseau privé virtuel », à savoir un service qui établit une connexion chiffrée et sécurisée entre votre ordinateur et Internet. Ce faisant, vous bénéficiez d'un tunnel privé pour vos données et vos communications lorsque vous surfez sur des réseaux publics

OpenVPN : OpenVPN est un logiciel libre permettant de créer un réseau privé virtuel VPN.

PPTP : PPTP (Point-to-point tunneling Protocol - RFC 2637), protocole de tunnel pointàpoint, est un protocole d'encapsulation PPP sur IP conçu par Microsoft. Il permet de mettre en place des réseaux privés virtuels (VPN) au-dessus d'un réseau public.

IPsec : IPsec est un groupe de protocoles qui sont utilisés ensemble pour établir des connexions cryptées entre des appareils. Il permet de sécuriser les données envoyées sur les réseaux publics.