I - 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. NetworkingCompany est une société partenaire Cisco Premier Partner. Elle emploie 20 ingénieurs réseau qui disposent de diverses certifications et d'une grande expérience dans ce secteur.
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.

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.

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 technologiques 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 Enseignements sur le système informatique de l'organisation :

Organisation de StadiumCompany :

Téléphones et PC de StadiumCompany :

Tous les dirigeants et responsables de StadiumCompany utilisent des PC et téléphones connectés à un PABX vocal numérique. À l'exception des préposés au terrain à temps plein et des gardiens, tous les salariés utilisent également des PC et des téléphones.
Cinquante téléphones partagés sont répartis dans le stade pour le personnel de sécurité. On compte également12 téléphones analogiques, certains prenant également en charge les télécopies et d'autres offrant un accès direct aux services de police et des pompiers. Le groupe sécurité dispose également de 30 caméras de sécurité raccordées à un réseau distinct.

Installations existantes et prises en charge :

StadiumCompany propose des installations et une prise en charge de réseau pour deux équipes de sports (Équipe A et Équipe B), une équipe « visiteurs », un restaurant et un fournisseur de concessions.
Le stade mesure environ 220 mètres sur 375. Il est construit sur deux niveaux. En raison de la taille des installations, plusieurs locaux techniques connectés par des câbles à fibre optique sont répartis sur l'ensemble du stade. Les vestiaires des équipes A et B et les salons des joueurs sont situés au premier niveau de la partie sud du stade. Les bureaux des équipes occupent une surface d'environ 15 mètres par 60 au deuxième niveau.
Le bureau et le vestiaire de l'équipe « visiteuse » sont également situés au premier niveau.

Les bureaux de StadiumCompany se trouvent dans la partie nord du stade, répartis sur les deux niveaux.

L'espace des bureaux occupe environ 60 mètres par 18 au premier niveau et 60 mètres par 15 au deuxième niveau.

Les équipes A et B sont engagées dans des compétitions sportives différentes, organisées à des dates différentes. Elles sont toutes les deux sous contrat avec StadiumCompany pour leurs bureaux et services au sein du stade.

Organisation de l'équipe A :

L'équipe A compte 90 personnes :
· 4 dirigeants
· 12 entraîneurs
· 14 employés (y compris des médecins, kinés, secrétaires, assistants, comptables et assistants financiers)
· 60 joueurs
L'équipe A dispose de 15 bureaux dans le stade pour ses employés non joueurs. Cinq de ces bureaux sont partagés. 24 PC et 28 téléphones sont installés dans les bureaux. L'équipe A dispose également d'un vestiaire des joueurs, d'un grand salon pour les joueurs et d'une salle d'entraînement. Les employés non joueurs utilisent les locaux toute l'année. Les joueurs ont accès au vestiaire et aux équipements d'entraînement pendant et en dehors de la saison. Le vestiaire est équipé de 5 téléphones et le salon des joueurs de 15 téléphones. Des rumeurs indiquent que l'équipe A aurait récemment installé un concentrateur sans fil dans le salon des joueurs.

Organisation de l'équipe B :

L'équipe B compte 64 personnes :
· 4 dirigeants
· 8 entraîneurs
· 12 employés (y compris des médecins, kinés, secrétaires, assistants, comptables et assistants financiers)
· 40 joueurs
L'équipe B dispose de 12 bureaux dans le stade pour ses employés autres que les joueurs. Trois de ces bureaux sont partagés. 19 PC et 22 téléphones sont installés dans les bureaux. L'équipe B dispose également d'un vestiaire des joueurs et d'un grand salon pour les joueurs. Les employés non joueurs utilisent les locaux toute l'année. Les joueurs ont accès au vestiaire et aux équipements d'entraînement pendant et en dehors de la saison. Le vestiaire est équipé de 5 téléphones et le salon des joueurs de 15 téléphones.

Accueil de l'équipe « visiteuse » :

L'équipe « visiteuse » dispose d'un vestiaire et d'un salon équipés de 10 téléphones. Chaque équipe « visiteuse » demande des services provisoires le jour du match et quelques jours

auparavant. Les équipes « visiteuses » passent également un contrat avec StadiumCompany pour les bureaux et services au sein du stade.

Fournisseur de concessions :

Un fournisseur de concessions gère les services proposés lors des matchs et événements. Il compte 5 employés à temps plein. Ils occupent deux bureaux privés et deux bureaux partagés équipés de cinq PC et sept téléphones. Ces bureaux se trouvent dans la partie sud du stade, entre les bureaux des équipes A et B. Deux employés à temps partiel prennent les commandes auprès des loges au cours des événements. Le concessionnaire de services emploie des intérimaires saisonniers pour gérer 32 stands permanents et autres services répartis sur l'ensemble du stade. Il n'y a actuellement aucun téléphone ni PC dans les zones de vente.

Organisation du restaurant de luxe :

Le stade propose un restaurant de luxe ouvert toute l'année. En plus des salles et des cuisines, le restaurant loue des bureaux auprès de StadiumCompany. Les quatre dirigeants ont chacun un bureau privé. Les deux employés en charge des questions financières et comptables partagent un bureau. Six PC et téléphones sont pris en charge. Deux téléphones supplémentaires sont utilisés en salle pour les réservations.

Prise en charge des loges de luxe :

Le stade compte 20 loges de luxe. StadiumCompany équipe chaque loge d'un téléphone permettant de passer des appels locaux et d'appeler le restaurant et le concessionnaire de services.

Prise en charge de la zone de presse :

StadiumCompany propose un espace presse avec trois zones partagées :
· La zone presse écrite accueille généralement 40 à 50 journalistes au cours d'un match. Cette zone partagée est équipée de 10 téléphones analogiques et de deux ports de données partagés. On sait qu'un journaliste stagiaire apporte un petit point d'accès sans fil lorsqu'il couvre un match.
· La zone de presse pour les radios peut accueillir 15 à 20 stations de radio. Elle estéquipée de 10 lignes téléphoniques analogiques.
· La zone de presse télévisée accueille généralement 10 personnes. Elle est équipée de 5 téléphones.

Prise en charge de site distant :

StadiumCompany compte actuellement deux sites distants : une billetterie en centre-ville et une boutique de souvenirs dans une galerie marchande locale. Les sites distants sont connectés via un service DSL à un FAI local. Le stade est connecté au FAI local à l'aide de FAI1, un routeur de services gérés qui appartient au FAI. Les deux sites distants sont connectés au même FAI par les routeurs FAI2 et FAI3, fournis et gérés par le FAI. Cette connexion permet aux sitesdistants d'accéder aux bases de données situées sur les serveurs

dans les bureaux de StadiumCompany. StadiumCompany dispose également d'un routeur de périmètre, nommé Routeur de périphérie, connecté au routeur FAI1 du stade.

En résumé :

Nombre de serveurs : 9 dont : (web, DHCP, commerce électronique, comptabilité(x3), paie)

Utilisateurs :

- 35 dirigeants
- 135 employés
- environs 80 intérimaires
- équipe A (90 personnes : 4 dirigeants, 12 entraineurs, 14 employé, 60 joueurs)
- équipe B
- équipe visiteurs
- restaurant
- fournisseur de concessions
- équipe B (4 dirigeants, 8 entraineurs, 12 employé, 40 joueurs)
- équipe visiteurs :
- fournisseur de concessions 5 employé 2 employé a temps partiel : intérimaire non défini
- restaurant de luxe : 4 dirigent, 2 employé,
- 20 loges de luxe
- 2 sites distants

Services : DNS, DHCP, web

- dirigeants : PC et téléphones connecter à un PABX
- personnel et sécurité : 50 téléphones et PC réparti dans le stade
- 12 téléphones analogiques répartis dans le stade qui prennent en charges la télécopie, et d'autres offrant un accès direct aux services de police et pompier.
- locaux connecté par fibre optiques
- équipe A : 15 bureaux dont 5 partagé 24 PC et 28 téléphones dans ces bureaux ; vestiaire 5 téléphone, salon des joueurs : 15 téléphones
- équipe B : 12 bureaux dont 3 partagé, 19 PC et 22 téléphones, vestiaires 5 téléphones, salon des joueurs 15 téléphones
- équipe visiteur : salon et vestiaire doté de 10 téléphones
- fournisseur de concession : 2 bureau privée 5 PC et 7 téléphones, 32 stand permanent non équipé pour le moment.
- restaurant de luxe : 4 bureau privé, 6 téléphones + 2 utilisé en salle pour les réservations
- 20 loges de luxe : 20 téléphones
- zone de presse : 10 téléphones analogique, 2 ports de données réseaux + Wireless AP
- 2 sites distant : connecter Via VPN (router FAI x3 pour gérer la connexion

StadiumCompany dispose d'un routeur de périmètre

Pas d'information sur les processus, contrats et chartes informatiques.

II - Cahier des charges :

Cette année, vous allez intégrer la division du stade de StadiumCompany. Vous serez chargé de la maintenance des systèmes et réseaux informatiques.

StadiumCompany est composé de plusieurs sites :
Site 1 : Stade (hébergement informatique, siège social et centre administratif)
Site 2 : Billetterie (vente des billets)
Site 3 : Magasin (vente des souvenirs)

Les différentes solutions retenues pour l'étude du projet d'un point de vue général de StadiumCompany pourront faire l'objet de documentations techniques suivant la complexité de la mise en œuvre.

Mission 3
Solution permettant l'administration à distance sécurisées et la sécurisation des interconnexions
- La sécurité du système d'information devra être renforcée entre les différents sites
- Sécurisation des interconnexions entre le site du stade et les sites distants Billetterie et le Magasin.
- La solution retenue devra être administrable à distance via un accès sécurisé par SSH

Les fonctionnalités du SSL :

- Authentification : Le client doit pouvoir s'assurer de l'identité du serveur.

Depuis SSL 3.0, le serveur peut aussi demander au client de s'authentifier.

Cette fonctionnalité est assurée par l'emploi de certificats.

- Confidentialité : Le client et le serveur doivent avoir l'assurance que leur

conversation ne pourra pas être écoutée par un tiers. Cette fonctionnalité est

assurée par un algorithme de chiffrement.

- Identification et intégrité : Le client et le serveur doivent pouvoir s'assurer que

les messages transmis ne sont ni tronqués ni modifiés (intégrité), qu'ils

proviennent bien de l'expéditeur attendu. Ces fonctionnalités sont assurées par la signature des données.

SSL et TLS reposent donc sur la combinaison de plusieurs concepts cryptographiques, exploitant la fois le chiffrement asymétrique et le chiffrement symétrique.

SSL et TLS se veut en outre évolutif, puisque le protocole est indépendant des algorithmes de cryptage et d'authentification mis en œuvre dans une transaction. Cela lui permet de s'adapter aux besoins des utilisateurs et aux législations en vigueur. Cela assure de plus une meilleure sécurité, puisque le protocole n'est pas soumis aux évolutions théoriques de la cryptographie.

III - Solution :

3.2.1 Accès distant :

Nous utiliserons le SSH, qui permet d'avoir une connexion distante en mode terminale (ou console) de manière sécurisée grâce aux algorithme proposés (RSA, DSA, ...)

3.2.2 Accès Internet :

NAT – PAT, car le NAT statique est obsolète, le NAT dynamique monopolise trop d'adresse publics, et le NAT PAT permet de combiner les avantages du NAT statique sans les inconvénients du NAT dynamique.

3.2.3 VPN :

Nous utiliserons et mettrons en place IPSec, c'est le seul capable de crypter les données échangées.

IV/ Projet

4.1 Objectifs et but du projet :

Mise en place des outils de sécurité au sein de l'infrastructure Stadiumcompany.

4.2.1.1 Configurez les informations de base du routeur et de l'interface :

R-Stade>en

R-Stade#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R-Stade(config)#ip domain-name stadiumcompany.com

R-Stade(config)#username admin privilege 15 password cisco

R-Stade(config)#int fa 0/0

R-Stade(config-if)#no shut

R-Stade(config-subif)#int fa 0/0.4

R-Stade(config-subif)#encapsulation dot1Q 10

R-Stade(config-subif)#ip address 172.20.0.1 255.255.255.0

R-Stade(config-subif)#no shut

R-Stade(config-subif)#exit

R-Stade(config)#int fa 0/1

R-Stade(config-if)#ip address dhcp

R-Stade(config-if)#no shut

*Nov 2 09:08:44.239: %DHCP-6-ADDRESS_ASSIGN: Interface FastEthernet0/1

assigned DHCP address 172.20.81.43, mask 255.255.240.0, hostname R-Stade

4.2.1.2 Configurez les lignes de terminal vty entrantes afin d'accepter Telnet et SSH :

R-Stade(config)#line vty 0 4

R-Stade(config-line)#privilege level 15

R-Stade(config-line)#login local

R-Stade(config-line)#transport input telnet ssh

R-Stade(config-line)#exit

4.2.1.3 Générez la paire de clés de chiffrement RSA :

Dont se servira le routeur pour l'authentification et le chiffrement des données SSH qui sont transmises. Entrez 1024 pour le nombre de bits du modulus. La valeur par défaut est de 512.

R-Stade(config)#crypto key generate rsa

The name for the keys will be: R-Stade.stadiumcompany.com

Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R-Stade(config)#

*Nov 2 09:09:55.559: %SSH-5-ENABLED: SSH 1.99 has been enabled

R-Stade(config)#end

4.2.1.4 Vérifiez que SSH a bien été activé ainsi que la version qui est utilisée.

R-Stade#sh ip ssh

SSH Enabled - version 1.99

Authentication timeout: 120 secs; Authentication retries: 3

Minimum expected Diffie Hellman key size : 1024 bits

4.2.1.5 Test de connexion SSH via PuTTY :

On lance une connexion ssh via PuTTY à l'adresse du routeur (172.20.0.1) Le clé « fingerprint » s'affiche. Celle-ci est unique.

4.2.2 Mise en place du NAT/PAT :

4.2.2.1 Paramétrage des interfaces :

```
Router(config)#int fa 0/0
Router(config-if)#no shut
Router(config)#int fa 0/1
Router(config-if)#ip add dhcp
Router(config-if)# ip nat outside
Router(config)#int fa 0/0
Router(config-if)#ip nat inside
Router(config-if)#int fa 0/0.10
Router(config-subif)#ip nat inside
Router(config-subif)#int fa 0/0.20
Router(config-subif)#ip nat inside
Router(config-subif)#int fa 0/0.30
Router(config-subif)#ip nat inside
Router(config-subif)#int fa 0/0.40
Router(config-subif)#ip nat inside
Router(config-subif)#int fa 0/0.50
Router(config-subif)#ip nat inside
Router(config-subif)#int fa 0/0.100
Router(config-subif)#ip nat inside
Router(config-subif)#int fa 0/0.200
Router(config-subif)#ip nat inside
```

4.2.2.2 Identification des adresses sources à faire passer par le NAT. Création d'ACLs standard :

```
Router(config)#access-list 10 permit 172.20.0.0 0.0.0.255
Router(config)#access-list 20 permit 172.20.1.0 0.0.0.255
Router(config)#access-list 30 permit 172.20.3.0 0.0.0.127
```

Router(config)#access-list 40 permit 172.20.3.128 0.0.0.63

Router(config)#access-list 50 permit 172.20.3.192 0.0.0.31

Router(config)#access-list 98 permit 172.20.2.0 0.0.0.127

Router(config)#access-list 99 permit 172.20.2.128 0.0.0.127

Router(config)#ip nat ins source list 10 interface fastEthernet 0/1 overload

Router(config)#$de source list 20 interface fastEthernet 0/1 overload

Router(config)#$de source list 30 interface fastEthernet 0/1 overload

Router(config)#$de source list 40 interface fastEthernet 0/1 overload

Router(config)#$de source list 50 interface fastEthernet 0/1 overload

Router(config)#$de source list 98 interface fastEthernet 0/1 overload

Router(config)#$de source list 99 interface fastEthernet 0/1 overload

4.2.2.3 Vérification des access-list :

Router#sh access-lists

Standard IP access list 10

10 permit 172.20.0.0, wildcard bits 0.0.0.255

Standard IP access list 20

10 permit 172.20.1.0, wildcard bits 0.0.0.255

Standard IP access list 30

10 permit 172.20.3.0, wildcard bits 0.0.0.127

Standard IP access list 40

10 permit 172.20.3.128, wildcard bits 0.0.0.63

Standard IP access list 50

10 permit 172.20.3.192, wildcard bits 0.0.0.31

Standard IP access list 98

10 permit 172.20.2.0, wildcard bits 0.0.0.127

Standard IP access list 99

10 permit 172.20.2.128, wildcard bits 0.0.0.127

4.2.2.4 Vérification de traduction des adresses, depuis un client :

Router#sh ip nat translations

Pro Inside global Inside local Outside local Outside global

icmp 172.20.90.75:1 172.20.1.100:1 8.8.8.8:1 8.8.8.8:1

udp 172.20.90.75:137 172.20.1.100:137 64.4.23.145:137 64.4.23.145:137

udp 172.20.90.75:137 172.20.1.100:137 64.4.23.155:137 64.4.23.155:137

udp 172.20.90.75:137 172.20.1.100:137 111.221.77.167:137 111.221.77.167:137

udp 172.20.90.75:137 172.20.1.100:137 157.55.130.145:137 157.55.130.145:137

udp 172.20.90.75:137 172.20.1.100:137 157.55.130.151:137 157.55.130.151:137

udp 172.20.90.75:137 172.20.1.100:137 157.55.235.141:137 157.55.235.141:137

udp 172.20.90.75:137 172.20.1.100:137 157.55.235.165:137 157.55.235.165:137

udp 172.20.90.75:137 172.20.1.100:137 157.56.52.15:137 157.56.52.15:137

udp 172.20.90.75:137 172.20.1.100:137 157.56.52.17:137 157.56.52.17:137

udp 172.20.90.75:137 172.20.1.100:137 157.56.52.45:137 157.56.52.45:137

udp 172.20.90.75:137 172.20.1.100:137 213.199.179.148:137

213.199.179.148:137

udp 172.20.90.75:137 172.20.1.100:137 213.199.179.165:137

213.199.179.165:137

udp 172.20.90.75:137 172.20.1.100:137 213.199.179.172:137

213.199.179.172:137

udp 172.20.90.75:1581 172.20.1.100:1581 46.236.190.182:65444

46.236.190.182:65444

udp 172.20.90.75:1581 172.20.1.100:1581 101.184.60.230:9180

101.184.60.230:9180

udp 172.20.90.75:1581 172.20.1.100:1581 155.4.21.64:52189 155.4.21.64:52189

4.2.3 Mise en place des ACL :

4.2.4 Mise en place du VPN (stade vers billeterie)

4.2.4.3 Routeur R3 :

Même procédure pour notre routeur R3 :

On commence par le Hostname :

Router#configure terminal

Router(config)#hostname R3

Nous configurons ensuite les adresses IP des deux interfaces :

R3(config)#interface FastEthernet 0/0

R3(config-if)#ip address 192.168.1.1 255.255.255.0

R3(config-if)#no shutdown

R3(config-if)#exit

R3(config)#interface FastEthernet 0/1

R3(config-if)#ip address 200.200.200.6 255.255.255.252

R3(config-if)#no shutdown

R3(config-if)#exit

Nos interfaces sont maintenant configurées, il nous reste à configurer le routage.

R3(config)#router eigrp 1

R3(config-router)#network 192.168.1.0 0.0.0.255

R3(config-router)#network 200.200.200.4 0.0.0.3

R3(config-router)#exit

La configuration de base de notre routeur R3 est terminée.

4.2.4.4 Test de fonctionnement :

Nous essayons de pinger depuis le PC du réseau local du Stade vers le PC du réseau local de la billetterie.

PC> ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:

Reply from 192.168.1.100: bytes=32 time=12ms TTL=126

Reply from 192.168.1.100: bytes=32 time=11ms TTL=126

Reply from 192.168.1.100: bytes=32 time=12ms TTL=126

Reply from 192.168.1.100: bytes=32 time=13ms TTL=126

Ping statistics for 192.168.1.100:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 11ms, Maximum = 13ms, Average = 12ms

4.2.4.5 Configuration du VPN :

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

4.2.4.3 Routeur R3 :

Même procédure pour notre routeur R3 :

On commence par le Hostname :

Router#configure terminal

Router(config)#hostname R3

Nous configurons ensuite les adresses IP des deux interfaces :

R3(config)#interface FastEthernet 0/0

R3(config-if)#ip address 192.168.1.1 255.255.255.0

R3(config-if)#no shutdown

R3(config-if)#exit

R3(config)#interface FastEthernet 0/1

R3(config-if)#ip address 200.200.200.6 255.255.255.252

R3(config-if)#no shutdown

R3(config-if)#exit

Nos interfaces sont maintenant configurées, il nous reste à configurer le routage.

R3(config)#router eigrp 1

R3(config-router)#network 192.168.1.0 0.0.0.255

R3(config-router)#network 200.200.200.4 0.0.0.3

R3(config-router)#exit

La configuration de base de notre routeur R3 est terminée.

4.2.4.4 Test de fonctionnement :

Nous essayons de pinger depuis le PC du réseau local du Stade vers le PC du réseau local de la billetterie.

PC> ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:

Reply from 192.168.1.100: bytes=32 time=12ms TTL=126

Reply from 192.168.1.100: bytes=32 time=11ms TTL=126

Reply from 192.168.1.100: bytes=32 time=12ms TTL=126

Reply from 192.168.1.100: bytes=32 time=13ms TTL=126

Ping statistics for 192.168.1.100:

Packets: Sent = 4, Received = 4, Lost = 0 (0% l

oss),

Approximate round trip times in milli-seconds:

Minimum = 11ms, Maximum = 13ms, Average = 12ms

4.2.4.5 Configuration du VPN :

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

Configurations de base

Nous commencerons par configurer notre PC et notre serveur en leur attribuant la bonne configuration réseau.

Nous attaquerons ensuite la configuration du routeur R1 :

Première étape :

Commençons par notre routeur R1, vous devez vérifier que l'IOS de vos routeurs supporte le VPN. On active ensuite les fonctions crypto du routeur :

R1(config)#crypto isakmp enable

Cette fonction est activée par défaut sur les IOS avec les options cryptographiques.

Sinon :

R-Stade#boot sy

R-Stade#conf ter

Enter configuration commands, one per line. End with CNTL/Z.

R-Stade(config)#boo

R-Stade(config)#boot sy

R-Stade(config)#boot system fla

R-Stade(config)#boot system flash:c2801-adventerprisek9-mz.124-16.bin

R-Stade(config)#^Z

R-Stade#wr

Deuxième étape :

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

R1(config)#crypto isakmp policy 10

R1(config-isakmp)#authentication pre-share

R1(config-isakmp)#encryption 3des

R1(config-isakmp)#hash md5

R1(config-isakmp)#group 5

R1(config-isakmp)#lifetime 3600

R1(config-isakmp)#exit

group 5 : Spécifie l'identifiant Diffie-Hellman

lifetime : Spécifie le temps de validité de la connexion avant une nouvelle négociation des clefs.

Troisième étape :

Ensuite nous devons configurer la clef :

R1(config)#crypto isakmp key iris123 address 200.200.200.6

Sur certains routeurs avec certains IOS la commande ne fonctionne pas car le routeur demande si le mot de passe doit être chiffré ou pas, tapez cette commande :

R1(config)#crypto isakmp key 6 iris123 address 200.200.200.6

Quatrième étape :

Configurons les options de transformations des données :

R1(config)#crypto ipsec transform-set 50 esp-3des esp-md5-hmac

esp : Signifie Encapsulation Security Protocol

N'oubliez pas d'utiliser les mêmes protocoles d'encryptions et de Hash utilisés dans la première étape. Dans notre cas :

Encryption : 3des

hash : md5

On fixe ensuite une valeur de Lifetime :

R1(config)#crypto ipsec security-association lifetime seconds 1800

Cinquième étape :

La 5éme étape consiste à créer une ACL qui va déterminer le trafic autorisé

R1(config)#access-list 101 permit ip 172.20.0.0 0.0.0.255 192.168.1.0 0.0.0255

Dernière étape de la configuration :

Dans cette dernière étape nous configurons la crypto map qui va associé l'access-

list, le traffic, et la destination :

R1(config)#crypto map stade 10 ipsec-isakmp

R1(config-crypto-map)#set peer 200.200.200.6

R1(config-crypto-map)#set transform-set 50

R1(config-crypto-map)#set security-association lifetime seconds 900

R1(config-crypto-map)#match address 101

R1(config-crypto-map)#exit

La configuration de R1 est presque terminée nous devons appliquer la crypto map sur l'interface de sortie :

Dans notre cas FastEthernet 0/1.

R1(config)#interface fastEthernet 0/1

R1(config-if)#crypto map stade

*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAK

MP is ON

R1(config-if)#

Un message vous indique que la crypto map fonctionne.

4.2.4.6 Configuration VPN sur R3 :

On refait la même configuration que sur R1 :

Première étape :

R3(config)#crypto isakmp enable

Deuxième étape :

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

R1(config-isakmp)#exit

Troisième étape :

R3(config)#crypto isakmp key iris123 address 200.200.200.1

ou

R3(config)#crypto isakmp key 6 iris123 address 200.200.200.1

Quatrième étape :

R3(config)#crypto ipsec transform-set 50 esp-3des esp-md5-hmac

R3(config)#crypto ipsec security-association lifetime seconds 1800

Cinquième étape :

R3(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 172.20.0.0. 0.0.0.255

Dernière étape de la configuration :

R3(config)#crypto map billetterie 10 ipsec-isakmp

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 FastEthernet 0/1

R3(config-if)#crypto map billetterie

*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKM

P is ON

4.2.4.7 Vérifications :

PC>ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:

Reply from 192.168.1.100: bytes=32 time=12ms TTL=126

Reply from 192.168.1.100: bytes=32 time=10ms TTL=126

Reply from 192.168.1.100: bytes=32 time=12ms TTL=126

Reply from 192.168.1.100: bytes=32 time=13ms TTL=12

Ping statistics for 192.168.1.100:

Packets: Sent = 4, Received = 4, Lost = 0 (0% l

oss),

Approximate round trip times in milli-seconds:

Minimum = 10ms, Maximum = 13ms, Average = 11ms

Nous vérifions les informations retournées par le VPN sur R1 et R3 :

R-Billeterie#show crypto ipsec tr

R-Billeterie#show crypto ipsec transform-set

Transform set 50: { esp-3des esp-md5-hmac }

will negotiate = { Tunnel, },

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac }

will negotiate = { Transport, },

Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac }

will negotiate = { Transport, },

Nous vérifions la map vpn : Pour information j'ai nommé ma map "stade".

R-Stade#show 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

5 Conclusion :

L’ensemble des équipements interconnectés répondent bien entre eux. La base du réseau est en place.

Grace à la mise en place d’un serveur de domaine les ordinateurs des différents VLANs pourront être intégré au domaine « stadiumcompany.local » et profiter desdossiers partagés sur le serveur.

Le serveur DHCP distribuera les adresses IP automatiquement aux ordinateurs qui se connecteront sur le réseau.

Des groupes d’utilisateurs ont été créés selon les services occupés par les utilisateurs. Ainsi seuls les utilisateurs du VLAN 10 ont accès au partage « G-administration », et ainsi de suite.

Compétences validées :

A.1.1.1 Analyse du cahier des charges d'un service à produire
A.1.2.1 Élaboration et présentation d'un dossier de choix de solution technique
A.1.2.2 Rédaction des spécifications techniques de la solution retenue (adaptationd'une solution existante ou réalisation d'une nouvelle solution
A.1.2.3 Évaluation des risques liés à l'utilisation d'un service
A.1.2.4 Détermination des tests nécessaires à la validation d'un service
A.1.3.1 Test d'intégration et d'acceptation d'un service
A.1.3.4 Déploiement d'un service
A.1.4.1 Participation à un projet
A.3.1.1 Proposition d'une solution d'infrastructure
A.3.1.2 Maquettage et prototypage d'une solution d'infrastructure
A.3.1.3 Prise en compte du niveau de sécurité nécessaire à une infrastructure
A.3.2.1 Installation et configuration d'éléments d'infrastructure
A.3.3.1 Administration sur site ou à distance des éléments d'un réseau, deserveurs, de services et d'équipements terminaux
A.4.1.9 Rédaction d'une documentation technique
A.5.1.2 Recueil d'informations sur une configuration et ses éléments
A.5.1.5 Évaluation d'un élément de configuration ou d'une configuration
A.5.2.1 Exploitation des référentiels, normes et standards adoptés par leprestataire informatique
A.5.2.2 Veille technologique
A.5.2.4 Étude d’une technologie, d'un composant, d'un outil ou d'une méthode