Rapport de Configuration et Sécurisation du Réseau

Ismail AKBOULATOV / Sarah BADER / Nassima BOUARABA / Messaline DUBOIS / 3-SI1

1. Introduction

La mise en place d'un réseau d'entreprise interconnectant plusieurs sites géographiques est une tâche exigeante nécessitant une planification rigoureuse. Ce rapport présente les choix d'adressage, la configuration DHCP, et la redondance via HSRP (Hot Standby Router Protocol). Dans les prochaines étapes, le routage OSPF, la sécurité par VPN/IPsec, et les ACLs seront intégrés.

L'objectif de ce réseau est de garantir :

- **Connectivité fluide** entre les agences et le siège à Paris.
- **Optimisation des adresses IP** grâce au VLSM pour éviter le gaspillage tout en prévoyant une évolutivité.
- **Redondance et fiabilité** via HSRP pour éviter les interruptions en cas de défaillance.
- **Facilité de gestion** en utilisant des VLANs pour isoler les sous-réseaux.

---

2. Plan d'Adressage

L'adressage est conçu selon les principes du VLSM (**Variable Length Subnet Mask**) afin d'optimiser l'utilisation des adresses tout en assurant une marge pour l'évolutivité.

2.1. Détails des Adresses IP

Ville	LAN	VLAN	Adresse Réseau	Masque	Plage d'Adresses	Hôtes Disponibles
Paris	LAN 1	VLAN 10	192.168.0.0	/22 (255.255.252.0)	192.168.0.1 - 192.168.3.254	1022
	LAN 2	VLAN 20	192.168.4.0	/22	192.168.4.1 - 192.168.7.254	1022
Rennes	LAN 1	VLAN 101	192.168.19.0	/25 (255.255.255.128)	192.168.19.1 - 192.168.19.126	126
	LAN 2	VLAN 102	192.168.19.128	/26 (255.255.255.192)	192.168.19.129 - 192.168.19.190	62
Strasbourg	LAN 1	VLAN 201	192.168.16.0	/24	192.168.16.1 - 192.168.16.254	254
	LAN 2	VLAN 202	192.168.17.0	/24	192.168.17.1 - 192.168.17.254	254

Ville	LAN	VLAN	Adresse Réseau	Masque	Plage d'Adresses	Hôtes Disponibles
Bordeaux	LAN 1	VLAN 301	192.168.8.0	/22	192.168.8.1 - 192.168.11.254	1022
	LAN 2	VLAN 302	192.168.12.0	/22	192.168.12.1 - 192.168.15.254	1022
Grenoble	LAN 1	VLAN 401	192.168.18.0	/25	192.168.18.1 - 192.168.18.126	126
	LAN 2	VLAN 402	192.168.18.128	/25	192.168.18.129 - 192.168.18.254	126

2.2. Justification des Masques

1. **Paris et Bordeaux** :
    - Les deux villes disposent de LANs avec 500 machines. Un **/22** (1022 hôtes) est suffisant pour couvrir les besoins actuels tout en prévoyant une marge de croissance.
2. **Rennes** :
    - **LAN 1 (60 machines)** : Un **/25** (126 hôtes) est utilisé, offrant une capacité supplémentaire pour l'évolutivité.
    - **LAN 2 (27 machines)** : Un **/26** (62 hôtes) est choisi, suffisant pour le réseau actuel et sa croissance.
3. **Strasbourg** :
    - **LAN 1 (120 machines)** et **LAN 2 (200 machines)** : Chaque réseau utilise un **/24** (254 hôtes), garantissant une marge de sécurité en termes d'adresses disponibles.
4. **Grenoble** :
    - **LAN 1 et LAN 2** : Chaque LAN est configuré en **/25** (126 hôtes), offrant un équilibre parfait entre efficacité et évolutivité.

Ces choix permettent d'optimiser les adresses tout en respectant les besoins spécifiques de chaque site.

---

3. Configuration DHCP

Le protocole DHCP est configuré sur les routeurs pour attribuer dynamiquement les adresses IP aux hôtes. Voici un exemple de configuration pour Paris.

3.1. Configuration DHCP à Paris

```
ip dhcp excluded-address 192.168.0.1 192.168.0.10
ip dhcp excluded-address 192.168.4.1 192.168.4.10
```

```
ip dhcp pool VLAN10
 network 192.168.0.0 255.255.252.0
 default-router 192.168.0.1
 dns-server 8.8.8.8

ip dhcp pool VLAN20
 network 192.168.4.0 255.255.252.0
 default-router 192.168.4.1
 dns-server 8.8.8.8
```

3.2. Vérifications

Après configuration, les commandes suivantes permettent de vérifier l'attribution des adresses :

```
show ip dhcp binding
show ip dhcp pool
```

Ces commandes confirment si les hôtes reçoivent bien des adresses dans les plages définies.

---

4. Configuration des VLANs

Les VLANs permettent de segmenter les réseaux pour améliorer la sécurité et la gestion.

4.1. Exemple de Configuration sur un Switch

Création des VLANs à Rennes

```
vlan 101
 name VLAN_Rennes_LAN1
vlan 102
 name VLAN_Rennes_LAN2
```

Configuration des Ports d'Accès

```
interface FastEthernet0/2
 switchport mode access
 switchport access vlan 101
 no shutdown
```

Configuration des Trunks

Les ports reliant les switches entre eux ou les switches aux routeurs sont configurés en mode trunk.

```
interface GigabitEthernet0/1
 switchport mode trunk
 switchport trunk allowed vlan 101,102
 no shutdown
```

4.2. Vérifications des VLANs

Pour vérifier que les VLANs sont correctement configurés :

```
show vlan brief
show interfaces trunk
```

---

5. Configuration HSRP (Redondance)

HSRP est configuré sur les routeurs pour garantir la disponibilité en cas de panne d'un routeur.

Exemple : HSRP à Paris

Configuration sur le Routeur Principal (Paris-1)

```
interface GigabitEthernet0/0
 ip address 192.168.0.1 255.255.252.0
 standby 1 ip 192.168.0.254
 standby 1 priority 110
 standby 1 preempt
```

Configuration sur le Routeur de Secours (Paris-2)

```
interface GigabitEthernet0/0
 ip address 192.168.0.2 255.255.252.0
 standby 1 ip 192.168.0.254
 standby 1 priority 90
```

Avec cette configuration, l'adresse virtuelle **192.168.0.254** est utilisée comme passerelle par défaut pour les hôtes du LAN1 à Paris. En cas de panne du routeur principal, le routeur de secours prend automatiquement le relais.

Vérifications

La commande suivante permet de vérifier l'état du HSRP :

```
show standby
```

6. Configuration OSPF

Le protocole **OSPF (Open Shortest Path First)** a été choisi pour implémenter le routage dynamique entre les différents sites du réseau. OSPF est un protocole de routage à état de lien, adapté aux réseaux complexes et à grande échelle, car il offre une convergence rapide et une meilleure gestion des chemins multiples. Dans cette section, nous expliquons les étapes de configuration d'OSPF, y compris l'ajout de mesures de sécurité pour garantir l'authenticité des routeurs participant au routage.

6.1. Configuration de Base d'OSPF

Pour la mise en œuvre d'OSPF, chaque routeur a été configuré pour participer à l'aire principale (area 0). Voici les étapes de base suivies pour configurer le routage OSPF sur chaque routeur :

1. **Activer OSPF** et définir l'ID du processus, généralement `1`.
2. **Annonce des réseaux connectés** : Chaque réseau connecté à un routeur a été annoncé au processus OSPF pour permettre l'échange de routes entre les différents sites.
3. **Vérification de la Convergence** : Après la configuration, l'état des voisins a été vérifié pour s'assurer que chaque routeur avait bien formé des relations de voisinage avec ses voisins immédiats.

Exemple de Configuration OSPF sur un Routeur

```
router ospf 1
 network 192.168.0.0 0.0.3.255 area 0
 network 192.168.4.0 0.0.3.255 area 0
 network 10.1.2.0 0.0.0.3 area 0
```

- `router ospf 1` : Démarre le processus OSPF avec un ID de `1`.
- `network` : Chaque réseau directement connecté est ajouté au processus OSPF, avec le **wildcard mask** approprié et une affectation à l'aire **0**.

6.2. Sécurisation d'OSPF avec l'Authentification MD5

Pour prévenir les intrusions et garantir que seuls les routeurs autorisés participent au processus de routage OSPF, une **authentification MD5** a été implémentée. L'authentification MD5 permet de hacher un mot de passe pour vérifier l'authenticité des messages OSPF échangés.

Configuration de l'Authentification MD5 sur les Interfaces

Pour chaque interface connectée à un lien série entre les routeurs, la configuration suivante a été appliquée :

1. **Accéder à l'interface série**.
2. **Activer l'authentification OSPF MD5** et configurer une clé d'authentification.

Exemple de Configuration sur RT-PARIS-1

```
interface Serial0/0/1
 ip address 10.1.2.1 255.255.255.240
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 Groupe4
 no shutdown
```

- `ip ospf authentication message-digest` : Active l'authentification **MD5** sur l'interface.
- `ip ospf message-digest-key 1 md5 Groupe4` : Spécifie la clé d'authentification MD5. Le numéro de clé est `1` et `Groupe4` est le mot de passe (doit être le même de chaque côté du lien).

Application Globale de l'Authentification MD5 sur l'Aire 0

Pour simplifier la configuration, une authentification OSPF globale pour **l'aire 0** a été définie sur chaque routeur participant à l'aire 0. Cette commande applique l'authentification MD5 à **toutes les interfaces** appartenant à cette aire :

```
router ospf 1
 area 0 authentication message-digest
```

Ainsi, toutes les interfaces faisant partie de **l'aire 0** sur ce routeur doivent nécessiter l'authentification **MD5**. Pour que la relation de voisinage soit établie correctement, les **routeurs voisins doivent également être configurés avec la même clé d'authentification** sur les interfaces connectées.

6.3. Vérifications Après Configuration

Après la configuration d'OSPF avec authentification, il était essentiel de vérifier la bonne établissement des relations de voisinage et la propagation des routes.

- **Vérifier les voisins OSPF** :

  ```
  show ip ospf neighbor
  ```

  Cette commande vérifie que les relations de voisinage sont bien établies entre les routeurs.

- **Vérifier les routes OSPF** :

  ```
  show ip route ospf
  ```

  Cela permet de s'assurer que les routes apprises via OSPF apparaissent correctement dans la table de routage.

6.4. Conclusion sur la Configuration OSPF

La configuration d'OSPF a permis d'assurer la **connectivité dynamique** entre tous les sites, facilitant la **redondance** et permettant une **convergence rapide** du réseau. L'ajout de l'authentification MD5 a renforcé la sécurité, en prévenant toute tentative de participation non autorisée au processus de routage. Les vérifications effectuées ont confirmé que tous les routeurs sont bien synchronisés et que le routage fonctionne comme prévu.

7. Configuration et Sécurisation du Réseau avec IPsec

La sécurisation des communications inter-sites était une priorité essentielle pour assurer la confidentialité, l'intégrité et la disponibilité des données circulant entre les agences. Pour répondre à cet objectif, la mise en place d'un **VPN IPsec** a permis de créer des tunnels sécurisés entre les sites distants. Ces tunnels permettent le chiffrement des données échangées entre les routeurs situés dans chaque ville, garantissant ainsi une sécurité accrue sur le réseau.

7.1. Objectifs d'IPsec

- **Confidentialité des Données** : IPsec permet de chiffrer les données pour empêcher toute interception par des tiers non autorisés.
- **Intégrité des Messages** : Assurer que les messages ne sont pas modifiés en cours de route.
- **Authenticité des Périphériques** : Garantir que les équipements participant aux communications sont authentiques.

7.2. Configuration de Base d'IPsec

La configuration IPsec a été appliquée sur chaque routeur interconnectant deux sites. Les étapes suivantes expliquent comment la configuration a été mise en place pour garantir des communications sécurisées.

1. **Configuration de l'ISAKMP (Phase 1)** : L'échange ISAKMP est la première étape pour établir une connexion sécurisée en utilisant l'**authentification mutuelle** des routeurs.

```
crypto isakmp policy 10
 encr aes 256
 hash sha
 authentication pre-share
 group 2
crypto isakmp key SOLEIL address 10.1.1.1
```

   - `encr aes 256` : Utilisation de l'algorithme de chiffrement AES avec une clé de 256 bits pour une grande sécurité.
   - `hash sha` : Utilisation de l'algorithme de hachage SHA pour garantir l'intégrité des données.
   - `authentication pre-share` : Utilisation de clés partagées pour l'authentification.
   - `group 2` : Utilisation du groupe 2 (Diffie-Hellman) pour établir une clé de session sécurisée.

2. **Configuration de la Phase 2 (IPsec)** : Une fois que la phase 1 est terminée, les paramètres de la **phase 2** sont définis pour créer le tunnel IPsec.

```
```

```
crypto ipsec transform-set TF esp-aes 256 esp-sha-hmac
crypto map CM_PARIS_RENNES 10 ipsec-isakmp
 set peer 10.1.1.2
 set transform-set TF
 match address 110
```

- `crypto ipsec transform-set TF esp-aes 256 esp-sha-hmac` : Création d'un ensemble de transformations pour définir les méthodes de chiffrement (AES) et d'authentification (SHA-HMAC).
- `crypto map CM_PARIS_RENNES 10 ipsec-isakmp` : Création de la carte crypto, qui associe les paramètres ISAKMP/IPsec pour l'établissement du tunnel.
- `set peer 10.1.1.2` : Définit l'adresse IP du routeur distant comme étant le pair pour la connexion.
- `match address 110` : Utilisation de l'ACL 110 pour définir le trafic devant être sécurisé par IPsec.

3. **Configuration des Listes de Contrôle d'Accès (ACL)** : Les ACL sont nécessaires pour définir quel trafic doit être protégé par IPsec.

```
access-list 110 permit ip 192.168.0.0 0.0.3.255 192.168.19.0 0.0.0.127
access-list 110 permit ip 192.168.0.0 0.0.3.255 192.168.19.128 0.0.0.63
```

- Ces ACLs définissent le trafic devant être chiffré, ici entre les sous-réseaux de Paris (`192.168.0.0/22`) et Rennes (`192.168.19.0/24`, `192.168.19.128/24`).

4. **Appliquer la Carte Crypto aux Interfaces** : Enfin, la carte crypto est appliquée à l'interface appropriée pour activer IPsec sur le trafic qui transite par cette interface.

```
interface Serial0/0/0
 crypto map CM_PARIS_RENNES
```

- `crypto map CM_PARIS_RENNES` : Applique la carte crypto (configuration IPsec) à l'interface `Serial0/0/0`, activant le chiffrement des données.

7.3. Vérification de la Configuration IPsec

Pour s'assurer que les tunnels VPN IPsec sont configurés correctement et sont **opérationnels**, plusieurs commandes de vérification ont été utilisées :

1. **Vérification des Associations de Sécurité (SA)** :

```
show crypto ipsec sa
```

- Permet de voir le statut des associations de sécurité IPsec, le nombre de paquets chiffrés et déchiffrés, ainsi que les erreurs potentielles.

2. **Vérification de l'État ISAKMP** :

```
show crypto isakmp sa
```

   - Permet de voir l'état des associations ISAKMP, pour s'assurer que la phase 1 est correctement établie.

3. **Débogage des Tunnels IPsec** :

```
debug crypto isakmp
debug crypto ipsec
```

   - Utilisé pour diagnostiquer les problèmes lors de l'établissement des tunnels et voir les détails des échanges entre les routeurs.

7.4. Conclusion sur la Configuration IPsec

La mise en place des tunnels VPN IPsec entre les différents sites a permis d'assurer la **confidentialité** et l'**intégrité** des données échangées. Les tests de connectivité ont confirmé que les communications entre chaque site sont bien chiffrées et protégées. Cette configuration ajoute une couche supplémentaire de sécurité au réseau global, garantissant que les données critiques de l'entreprise restent confidentielles lors de leur transit entre les différents sites.

---

8. Conclusion

Ce rapport décrit les étapes fondamentales de la configuration du réseau, incluant l’adressage, le DHCP, les VLANs et HSRP pour la redondance. Les choix effectués garantissent une utilisation optimale des ressources IP tout en offrant une marge d’évolutivité. Les tests confirment que les configurations sont fonctionnelles. Les prochaines étapes incluront l’implémentation d’OSPF, de VPN/IPsec, et des ACLs pour renforcer la sécurité et l’efficacité du réseau.