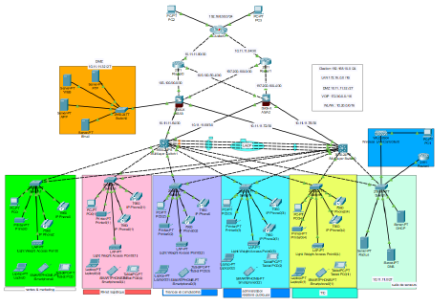
Procédure : Mise en Œuvre d'un Réseau d'Entreprise Sécurisé

TOPOLOGIE :



Informations du Projet :

- **Catégorie :** Projet Réseaux SISR
- **Languages utilisés :** Cisco IOS
- **Outils :** Cisco Packet Tracer
- **Date du projet :** 2024

Contexte du projet :

Dans ce projet, Nous avons été chargé de concevoir et de mettre en œuvre un système de réseau sécurisé pour le nouveau bâtiment de @Tech Innovation Ltd, une entreprise spécialisée dans les solutions cloud. Ce projet visait à créer une infrastructure réseau répondant aux exigences de sécurité, de performance et d'évolutivité, tout en garantissant une disponibilité optimale des ressources pour tous les départements de l'entreprise, y compris la gestion des serveurs essentiels et la connectivité entre plusieurs sites.

Cahier des charges et Objectifs :

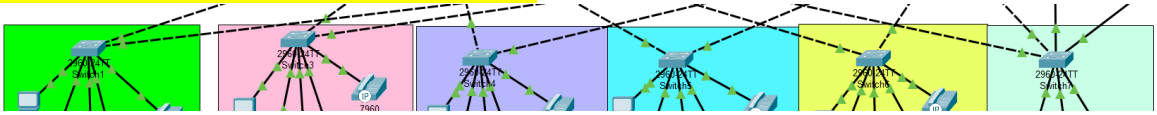
Le projet s'appuie sur un cahier des charges précis, comprenant la planification détaillée de l'architecture réseau. Les objectifs principaux incluent la création de différentes zones de sécurité à travers des pare-feu Cisco ASA, l'implémentation de VLANs pour la segmentation du réseau, la configuration de services essentiels comme DHCP, DNS, et VOIP, ainsi que l'intégration de technologies comme OSPF pour le routage dynamique. De plus, des mesures de redondance et de haute disponibilité sont mises en place via des protocoles comme HSRP et des commutateurs multicouches pour le routage inter-VLAN. L'objectif est de garantir une connectivité sécurisée et une gestion efficace du réseau à travers une infrastructure solide et évolutive.

1. Pré-requis

- **Équipements :**
  - **6 Switches de niveau 2**
  - **2 Switches de niveau 3**
  - **1 Routeur pour la VoIP**
  - **2 Pare-feu Cisco ASA**
  - **10 Téléphones IP**

---

2. Configuration des Switches de Niveau 2



2.1. Création des VLANs

- **Connectez-vous au switch de niveau 2 via la console.**
- **Entrez en mode de configuration globale et configurez les VLANs.**

Commandes :

- **vlan 10**
- **exit**
- **vlan 20**
- **exit**
- **vlan 50**
- **exit**
- **vlan 70**
- **exit**
- **vlan 100**
- **exit**

2.2. Configurer les interfaces des ports

Affectez les interfaces aux VLANs et configurez les paramètres Spanning Tree PortFast et BPDU Guard.

Commandes :

- interface FastEthernet0/1
- switchport trunk allowed vlan 10,20,50,70,100
- switchport mode trunk

- interface FastEthernet0/2
- switchport trunk allowed vlan 10,20,50,70,100
- switchport mode trunk

- interface FastEthernet0/3
- switchport access vlan 20
- switchport mode access
- spanning-tree portfast
- spanning-tree bpduguard enable

- interface FastEthernet0/5
- switchport voice vlan 70
- spanning-tree portfast
- spanning-tree bpduguard enable

- interface FastEthernet0/8
- switchport access vlan 10
- switchport mode access
- spanning-tree portfast
- spanning-tree bpduguard enable

2.3. Configurer le Trunk entre les Switches

Configurez les ports de liaison entre les switches de niveau 2 et 3 en mode trunk.

Commandes :

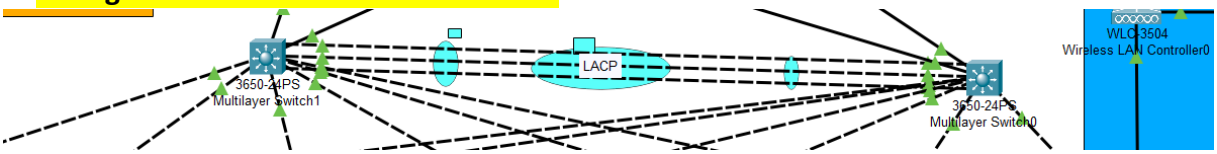
- interface FastEthernet0/1
- switchport trunk allowed vlan 10,20,50,70,100
- switchport mode trunk

- interface FastEthernet0/2
- switchport trunk allowed vlan 10,20,50,70,100
- switchport mode trunk

!

---

3. Configuration des Switches de Niveau 3



3.1. Configurer l'interface Port-Channel (EtherChannel)

Utilisez LACP pour configurer l'agrégation de liens entre les switches.

Commandes :

- interface GigabitEthernet1/0/7-9
- switchport mode trunk
- channel-group 1 mode active

- interface Port-channel1
- switchport mode trunk

3.2. Configurer les Interfaces VLANs

Configurez les interfaces VLANs pour le routage inter-VLAN.

- Commandes :
- interface Vlan10
- ip address 192.168.10.2 255.255.255.0
- ip helper-address 10.11.11.3
- standby 10 ip 192.168.10.1
- ---
- interface Vlan20
- ip address 172.16.0.2 255.255.0.0
- ip helper-address 10.11.11.3
- standby 20 ip 172.16.0.1
- !---
- interface Vlan50
- ip address 10.20.0.2 255.255.0.0
- ip helper-address 10.11.11.3
- standby 50 ip 10.20.0.1
- !---
- interface Vlan70
- ip address 172.30.0.2 255.255.0.0
- ip helper-address 172.30.0.1
- 3.3. Activer le Routage OSPF
-

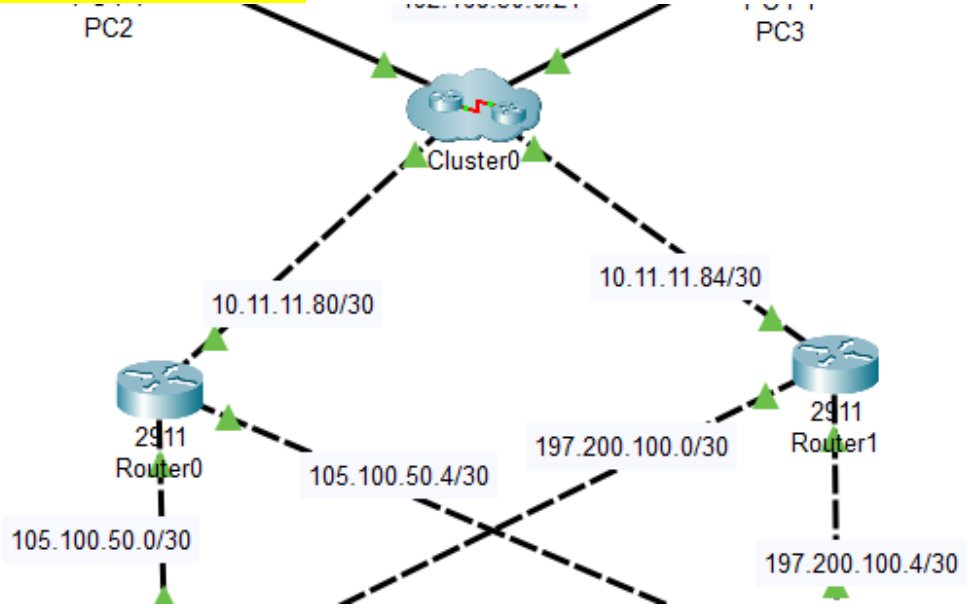
Configurez le protocole OSPF pour permettre la redondance et le routage dynamique.

Commandes :

- router ospf 40
- router-id 6.6.6.6
- network 172.16.0.0 0.0.255.255 area 0
- network 192.168.10.0 0.0.0.255 area 0

---

4. Configuration des Routeurs



4.1. Configurer les Interfaces des Routeurs

Connectez les routeurs à l'infrastructure réseau avec les bonnes adresses IP.

Commandes :

interface GigabitEthernet0/0

ip address 105.100.50.2 255.255.255.252

no shut

!----------

interface GigabitEthernet0/1

ip address 105.100.50.6 255.255.255.252

no shut

4.2. Configurer OSPF sur les Routeurs

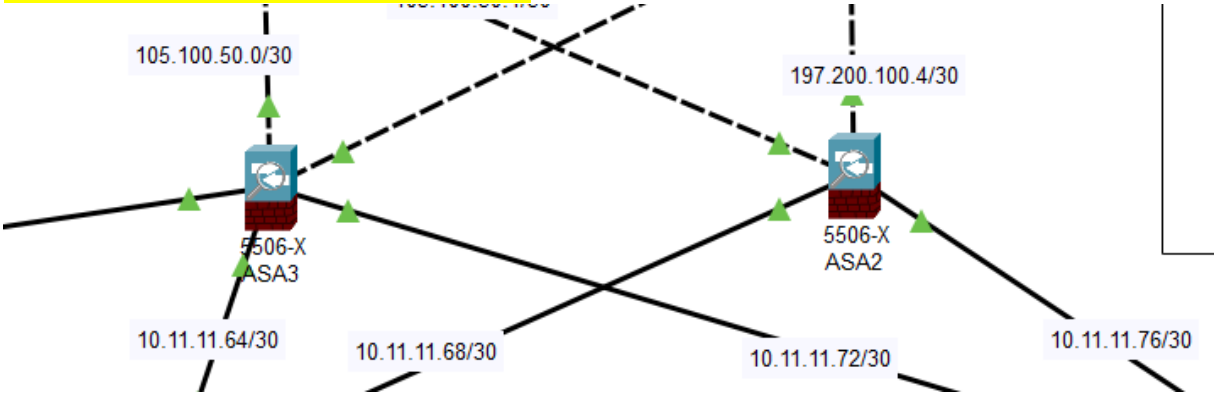
Le même protocole OSPF doit être configuré pour assurer le routage dynamique entre les routeurs.

Commandes :

- router ospf 40
- router-id 2.2.2.2
- network 20.20.20.0 0.0.0.3 area 0
- network 105.100.50.0 0.0.0.3 area 0

---

5. Configuration des Pare-Feu Cisco ASA



5.1. Configurer les Interfaces du Pare-Feu

Assignez les interfaces à leurs zones de sécurité et configurez leurs adresses IP.

Commandes :

- interface GigabitEthernet1/1
- nameif INSIDE1
- security-level 100
- ip address 10.11.11.66 255.255.255.252

- !---
- interface GigabitEthernet1/3
- nameif OUTSIDE1
- security-level 0
- ip address 105.100.50.1 255.255.255.252

5.2. Configurer NAT et ACLs

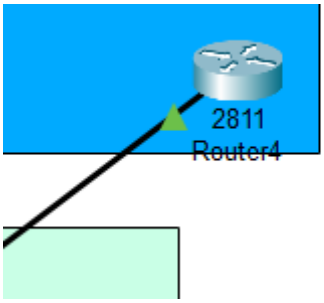
Configurez les règles NAT pour traduire les adresses IP et les ACLs pour filtrer le trafic.

Commandes :

- object network vlan_INSIDE1_OUTSIDE1
- subnet 172.16.0.0 255.255.0.0
- nat (INSIDE1,OUTSIDE1) dynamic interface
- !---
- access-list 100 extended permit icmp any any
- access-list 100 extended permit tcp any any eq www
- access-group 100 in interface INSIDE1

---

6. Configuration VoIP



6.1. Configurer DHCP pour VoIP

Attribuez des adresses IP aux téléphones IP via DHCP.

Commandes :

- ip dhcp pool VoIP
- network 172.30.0.0 255.255.0.0
- default-router 172.30.0.1
- option 150 ip 172.30.0.1

6.2. Configurer les Téléphones IP avec telephony-service

Configurez les téléphones IP sur le routeur.

Commandes :

telephony-service

max-ephones 40

max-dn 40

ip source-address 172.30.0.1 port 2000

auto assign 1 to 40

! ----------

ephone-dn 1

number 1001

---

7. Tests et Validation

1. **Ping Test : Assurez-vous que tous les VLANs peuvent se pinguer entre eux.**
2. **Vérification VoIP : Testez si les téléphones IP obtiennent des adresses IP et sont enregistrés sur le serveur VoIP.**
3. **Test de Redondance OSPF : Déconnectez un lien et vérifiez si OSPF trouve une route alternative.**

Synthèse :

Ce projet m'a permis d'acquérir une expérience précieuse dans la conception et la mise en œuvre d'une infrastructure réseau sécurisée pour une entreprise de grande envergure. Grâce à l'utilisation d'outils comme Cisco Packet Tracer et à l'intégration de technologies avancées telles que l'IPv6, OSPF, et la gestion des VLANs, j'ai pu créer un réseau performant et redondant qui répond aux exigences de sécurité et de disponibilité de @Tech Innovation Ltd. La configuration des équipements réseau et des protocoles de sécurité, ainsi que la mise en place d'une architecture résiliente, ont permis de garantir la sécurité et la performance du réseau à long terme.