Packet Tracer – **Control**

Ce TP est une épreuve qui compte pour votre moyenne de MIF21 et éventuellement pour le CCNA. Vous avez le droit de voir la progressions des points, mais la valeur de votre note ne sera pas forcement linéaire avec cette progression.

1. Topologie



1. Scénario

Votre entreprise ouvre une succursale et vous devez la configurer un routeur et un switch à cet endroit. Le schéma est complexe, mais tout se passe donc sur la partie de la topologie présenté dans ce sujet.

Votre superviseur à déjà installé un tunnel GRE de liaison entre la sucursale à St Étienne et la maison mère à Lyon. Ce tunnel permet d'utiliser une adresse privée entre les 2 sites. Elle permettra aussi de faire circuler les paquets entre les 2 site malgré l'ajout d'ACL pour filtrer les accès extérieur. Le reste n'est pas configuré et vous devez monter l'ensemble du réseau.

**Configuration de Base**

sur le routeur **SaintEtienne** et le switch **S21** vous devez configurer les informations de bases

* Le nom ;
* le mot du jour **« acces limite »** (sans les accents mais avec les guillemets) ;
* l'accès SSH (et limiter la connection à distance au SSH) avec une clef **1024 bits** et un nom de domaine **univ.fr ;**
* un utilisateur privilégié **root** dont le mot de passe est **cisco** et qui utilisé pour la connexion distante ;
* l'interfaces d'administration pour S21 (voir tableau) ;
* désactiver la recherche DNS et rendez les logs synchrones.

À ce stade vous devez avoir 17 points.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Périphérique | Interface | Adresse IPv4 |  Masque | Passerelle par défaut |
| Remarques |
| Lyon | G0/0 | 172.16.1.2 | 255.255.255.0 | 172.16.1.1 |
| Lo0 | 209.165.200.1 | 255.255.255.224 |  |
| SaintEtienne | G0/0 | 209.165.100.61 | 255.255.255.0 | Ne pas la modifier |
| Lo0 | 209.42.100.1 | 255.255.255.240 | Ne pas modifier |
| Go/1.100 | 10.42.100.1 | 255.255.255.0 | Dans le vlan normal |
| G0/1.110 | 10.42.110.1 | 255.255.255.0 | Dans le vlan d'admin |
| G0/1.120 | 10.42.120.1 | 255.255.255.0 | Dans le vlan Wifi |
| S21 | Vlan 110 | 10.42.110.2 | 255.255.255.0 | 10.42.110.1 |
| G0/1 | Vers SaintEtienne (lien trunk) |
| Fa0/1-20 | Dans le vlan normal |
| F0/21-24 | Dans le vlan d'administration |
| G0/2 | Dans le vlan Wifi |
| w[ww.univ.fr](http://Www.univ.fr/) | Fa0 | 10.10.10.2 | 255.255.255.0 | 10.10.10.1 |
|  |  | 209.165.200.2 | 255.255.255.224 |  |
| Intra.univ.fr | Fa0 | 10.10.10.3 | 255.255.255.0 | 10.10.10.1 |
|  |  | 209.165.200.3 | 255.255.255.224 |  |
| Www.lemonde.fr | Fa0 | 209.165.100.254 | ? | ? |
| Outside Host | Fa0 | 209.165.100.62 | 255.255.255.0 | 209.165.100.1 |

**Configuration des vlan et DHCP**

Créez les vlans et le routage inter vlan

* Vous devez mettre en place les 3 vlans du shéma (Normal, Admin et Wifi) en faisant bien attention à respecter le nom demandé.
* Vous devez activer le routage inter vlan via le routeur SaintEtienne
* Placez les tous ports de S21 en mode accès dans les bon vlan ou en mode trunk (voir le tableau).
* Configurez le Wifi en utilisant le port du switch Gi0/2, le SSID **invite** et l'authentification WPA2-PSK et la la clef partagée **totototo**
* Ce dernier doit de plus proposer 3 pools DHCP utilisez les nom **POOLNORM, POOLADM et POOLWifi**
* Conservez 50 adresses en début de plage pour les matériels utilisant une adresse statique
* Donnez le serveur DNS (10.10.10.3) et la passerelle par défaut via DHCP.
* Vérifiez le bon fonctionnement sur Pctest et Portable de manière à utiliser DHCP (pour les 2 Vlan Normal et Admin, vous pouvez changer le port de connexion de PcTest).

À ce stade vous devriez avoir 49 points et les PC doivent pouvoir pinguer leur passerelle et l'adresse public du routeur SaintEtienne (209.42.100.1).

**Configuration OSPF**

Vous devez configurer le protocole OSPF sur SaintEtienne pour qu'il échange des informations avec Lyon. Les 2 routeurs sont reliés avec un tunnel GRE qui leur donne une pseudo interface **tun0** dont l'adresse est sur le réseau 10.1.1.0/30**.** Via cette insterface ils peuvent échanger des mises à jour ospf. Lyon est configuré pour utiliser OSPF en monozone sans mot de passe.

* Configurez ospf sur St Etienne avec le numéro de processus 1 en mettant l'interface tun0 dans l'aréa 0.
* Vous devez exporter les informations de toutes les interfaces de SainEtienne mais n'envoyez pas de mise à jour OSPF sur les vlans internes.
* SaintEtienne ne doit pas anoncer de route par défaut ni le réseaux de liaison avec le FAI (*attention, cela ferait tomber le tunnel GRE*).

A ce stade la résolution de nom doit fonctionner et vous devriez avoir 56 points.

**Nat et ACL**

Vous devez mettre en place le NAT et les ACLs afin que vos machines puissent communiquer avec l'extérieur.

* Méttez un place la translation d'adresse
	+ en utilisant un pool nommé PNAT et contenant les adresses 209.42.100.2 à 10 ;
	+ en utilisant une ACL simple numérotée **1** pour définir les adresses à traduire ;
	+ en permettant le partage de connexion avec plus de 10 Pcs internes.
* Vous devez protéger votre réseau en :
	+ En interdisant les paquets à destination du vlan d'administration s'il proviennent du vlan Wifi (vous devez proposer une ACL étendue numéroté 150, avec le moins de règles possible et la plus précise possible et l'appliquer dès la sortie du reseau Wifi).
	+ En interdisant à tout paquet de pénétrer le réseaux depuis l'extérieur sauf si c'est le retour d'un paquet tcp ou icmp provenant de l'intérieur du réseau et sauf s'il est à destination du routeur SaintEtienne ou d'une des adresses public utilisées (pour cette question, utilisez une ACL étendue nomée **AIN** et autorisant l'accès aux adresses 209.165.100.61 et 209.42.100.0/28, nommez votre inspection **INSAIN**).