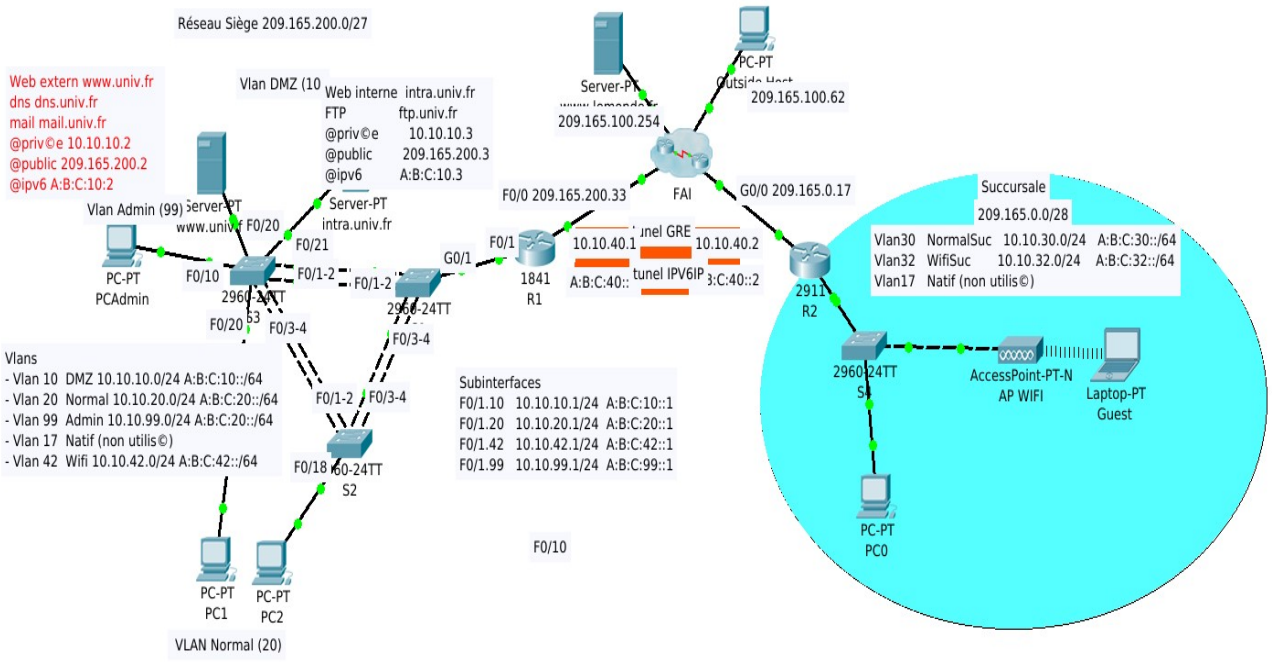
Packet Tracer – TP Issus du PacketTracer du chapitre 1.4.1.2

Topologie



Scénario

Vous devez installer le réseau dans une succursale de votre entreprise. Cette dernière devra être reliée par un tunnel GRE au siège ce qui lui permettra d'utiliser les mêmes adresses privées que le reste de l'entreprise.

Conditions requises

Remarque : bien que cela ne soit pas obligatoire, l'ajout d'un étiquetage supplémentaire à la topologie peut vous aider dans la réalisation de cette tâche. Tous les noms et mots de passe tiennent compte des majuscules.

Table d'adressage

Périphérique	Interface	Adresse IPv4	Masque	Passerelle par défaut
		Remarques		
R1	F0/0	209.165.200.33	255.255.255.252	209.165.200.34
	F0/1.10	10.10.10.1	255.255.255.0	N/A
	F0/1.20	10.10.20.1	255.255.255.0	N/A
	F0/1.42	10.10.42.1	255.255.255.0	N/A
	F0/1.99	10.10.99.1	255.255.255.0	N/A
R2	G0/0	209.165.0.17	255.255.255.252	209.165.0.18
	G0/1.30	10.10.30.1	255.255.255.0	NA
	G0/1.32	10.10.32.1	255.255.255.0	NA
S4	Vlan 39	10.10.39.12	255.255.255.0	10.10.39.1
	Fa0/1-24	Acces au vlan 30		
	Gi 0/1	Liaison avec le routeur		
	Gi 0/2	Accès au vlan 32 (Wifi)		
www.univ.fr	Fa0	10.10.10.2	255.255.255.0	10.10.10.1
		A:B:C:10::2	/64	A:B:C:10::1
	nat	209.165.200.2	255.255.255.224	
Intra.univ.fr	Fa0	10.10.10.3	255.255.255.0	10.10.10.1
		A:B:C:10::3	/64	A:B:C:10::1
		209.165.200.3	255.255.255.224	
PCAdmin	Fa0	10.10.99. 21	255.255.255.0	10.10.99.1
PC1	Fa0	10.10.20. 21	255.255.255.0	10.10.20.1
PC2	Fa0	10.10.20. 22	255.255.255.0	10.10.20.1
Www.lemonde.fr	Fa0	209.165.100.254	?	?
Outside Host	Fa0	209.165.100.62	255.255.255.0	209.165.100.1
PC0	Fa0	10.10.30. ?	255.255.255.0	10.10.30.1

Le réseau de la succursale comporte 2 vlans : 30 et 32 (Wifi). Les vlans et le routage inter vlans sont configurés. Vous devez mettre en place le serveur DHCP, la traduction d'adresse, les tunnels pour les adresses ipv4 et ipv6 ainsi que des ACL pour protéger le réseau.

Configuration de DHCP

Vous devez activer un serveur DHCP ipv4 sur R2 pour attribuer les adresses sur les vlans 30 et 32

- Pour les pools DHCP utilisez les noms **DHCP30** et **DHCP32**
- Conservez 20 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.
- Modifier la configuration de PC0 de manière à utiliser DHCP

Installation du Wifi

Vous devez installer une borne légère dans un vlan dédié (le 32). Les utilisateurs devront obtenir automatiquement une adresse via le serveur DHCP.

- Configurez la borne pour utiliser le SSID **User**, l'authentification WPA2-PSK et la clef « motdepasse » avec le chiffrement TKIP.
- À partir de ce moment si vous configurez le portable Guest, il doit obtenir une adresse et être capable de « pinguer » la passerelle 10.10.32.1

Adresse IPV6

Le routeur a déjà des adresses ipv6, les machines peuvent obtenir une adresse automatiquement mais pas les autres infos (domain, dns ...). Vous devez configurer deux pool DHCPV630 et DHCPV632 pour cela. LA configuration dhcp ne fonctionne pas très bien sous packettracer, vous devez vous référer au lexique des commandes pour que cela fonctionne.

- Utilisez deux pool locaux d'adresses :
  - POOLADD30 avec le préfix A:B:C:30:1::/80
  - POOLADD32 avec le préfix A:B:C:32:1 ::/80
- Créez deux pool :
  - DHCPV630 utilisé par l'interface Gi 0/1.30 et proposant le bon préfix
  - DHCPV632 utilisé par l'interface Gi 0/1.32 et proposant le bon préfix
- Configurez les deux pools pour donner le serveur DNS A:B:C:10::2 et le domaine univ.fr

Tunnel

Le réseau de la succursale ne peux pas contacter les serveurs principaux. En effet, les adresses privées ou ipv6 ne sont pas routées par le réseau externe qui relie les 2. Vous allez donc mettre en place 2 tunnels :

- Un tunnel numéro 0, de type gre, pour transporter les paquets du réseau 10.10.0.0/16 entre les 2 routeurs. Vous utiliserez comme source et destinations les adresses publiques des 2 routeurs (209.165.200.33 pour R1 et 209.165.0.17 pour R2). Et les adresses 10.10.40.1 pour R1 et 10.10.40.2 pour R2. Remarque, sous packet tracer, la commande « tunnel source »
- Un tunnel numéro 1, de type ipv6ip, pour transporter les paquets ipv6. Avec pour ce tunnel les adresses A:B:C:40::1 et A:B:C:40::2.

Attention, il y a une ACL pour protéger l'entrée sur le réseau de R1. Il faut la modifier pour que cela fonctionne. Vous placerez deux règles en début de liste.

- Une règle pour autoriser les paquets GRE de R2 vers R1

- Une règle pour autoriser les paquets IP de R2 vers R1

A la fin, les machines de la succursale doivent pouvoir contacter les serveurs de la DMZ en ipv6 et ipv4

NAT

Vous devez mettre en place la traduction d'adresse pour permettre aux machines du réseau de contacter l'extérieur.

- Utilisez le PAT sur un pool d'adresses POOLNAT contenant les adresses 209.165.0.10 à 14
- Utilisez une ACL numérotée 1 pour reconnaitre les adresses à traduire (contenant les 2 vlans 30 et 32).

Normalement, PC0 doit pouvoir lire la page web du serveur www.lemonde.fr

ACL étendues

Vous allez sécuriser le réseau en limitant les droits depuis le réseau WIFI. Créez une ACL (OUTWIFI) à placer en sortie du vlan 32 permettant (attention, on sort d'un réseau en entrant dans un routeur) :

- de laisser passer les réponses au ping ;
- de laisser passer les requêtes vers les port www (80, tcp), https (443, tcp), ssh (22, tcp), dns (53, tcp+udp) et tous les ports supérieurs à 1024 ;
- de laisser passer les requêtes vers l'extérieur mais pas celles vers tous les réseaux 10.10.0.0/16.

Normalement, le portable doit pouvoir contacter le serveur www.lemonde.fr, il peut être pingué depuis PC0 mais ne peux pas le pinguer.

ACL à état

A priori, aucun paquet ne doit entrer dans le réseaux sauf s'il est associé aux tunnel. Cependant, le fait de bloquer un paquet entrant bloque aussi la réponse à un paquet provenant du réseau 10.10.0.0/16. Il faut donc utiliser un système capable de garder trace des sessions légitimes qui sont sorties du réseau pour autoriser automatiquement leur retour.

- Ajoutez une ACL étendue nommée ACLOUT qui n'autorise que les paquets ip ou gre de R1 vers R2.
- Vérifiez que PC0 ne contacte plus le serveur extérieur (préciser dans le rapport comment vérifier cela).
- Ajoutez une inspection de ce qui sort pour tcp, udp ou icmp et vérifiez que cela re-fonctionne.
- Vous avez utilisé une ACL étendue pour faire cela. Mais la règle étant simple, on aurait pu utiliser une ACL standard. Par contre, si vous faite cela, le système CBAC ne fonctionnera plus. Pourquoi selon vous ?

© UCBL & CISCO