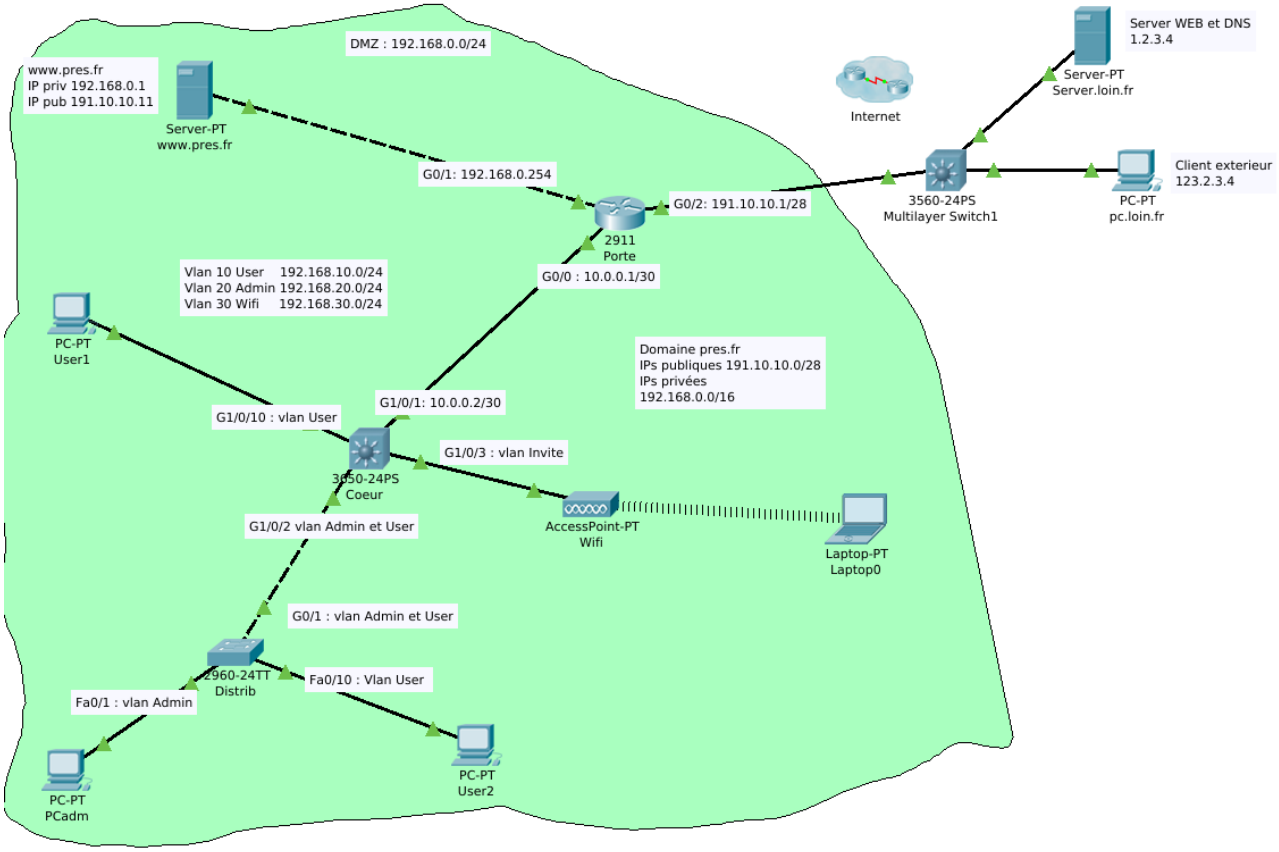
Exam - M1IF15 Réseau par la pratique

31 mai 2022

I Description du réseau



II Scénario

Vous devez configurer le réseau dans votre entreprise

II.1 Table d'adressage

Périphérique	Interface	Adresse IPV4	Masque Ipv4	Passerelle
Porte	G0/0	`10.0.0.1`	`255.255.255.252`	N/A
	G0/1	`192.168.0.254`	`255.255.255.0`	N/A
	G0/2	`191.10.10.1`	`255.255.255.240`	191.10.10.14
Coeur	G1/0/1	`10.0.0.2`	`255.255.255.252`	aquise par ospf
	G1/0/2	trunk vlan Admin et User	N/A	N/A
	G1/0/3	accès vlan Wifi	N/A	N/A
	G1/0/10 à 20	accès vlan User	N/A	N/A
	Vlan 10	`192.168.10.254`	255.255.255.0	N/A
	Vlan 20	`192.168.20.254`	255.255.255.0	N/A
	Vlan 30	`192.168.30.254`	255.255.255.0	N/A
Distrib	G0/1	trunk vlan Admin et User	`N/A`	N/A
	Fa 0/1 à 0/9	accès vlan Admin	N/A	N/A
	Fa 0/10 à 0/20	accès vlan User	N/A	N/A
	Vlan 20	`192.168.20.253`	255.255.255.0	192.168.20.254
www.pres.fr	NIC	`192.168.0.1`	`255.255.255.0`	192.168.0.254
PCAdmin	NIC	dans 192.168.20.0/24	acquis par DHCP	192.168.20.254
User1	NIC	dans 192.168.10.0/24	acquis par DHCP	192.168.10.254
User2	NIC	dans 192.168.10.0/24	acquis par DHCP	192.168.10.254
serveur.loin.fr	NIC	`1.2.3.4`	`255.255.255.0`	?
pc.loin.fr	NIC	`123.2.3.4`	`255.255.255.0`	?

III Configuration des périphériques de base

Q.III.1) - Effectuez les configurations suivantes sur `Porte`, `Coeur` et `Distrib`.

1(a) - Créez un utilisateur `root` de mot de passe **chiffré** `toto` avec les droits maximum.

1(b) - Désactivez la recherche DNS.

1(c) - Activez les logs synchrones.

1(d) - Activez ssh, créer une clef de 2048 bits.

1(e) - Utilisez la base de données d'utilisateur local pour la connection à distance.

1(f) - Imposez ssh comme seul moyen de se connecter à distance.

IV Wifi

Le wifi utilise les caractéristiques suivantes :
— SSID : `invite`
— Sécurité : `Wpa2 PSK`
— Mot de passe : mdP1nV1tE

Q.IV.1) - Configurez le Wifi pour l'AP `Wifi` et le portable `Laptop0`.

V Vlan

Sur `Coeur` et `Distrib` il y a 3 vlans :
— `User` vlan 10
— `Admin` vlan 20
— `Wifi` vlan 30
C'est le switch niveau 3 `Coeur` qui s'occupe du routage inter vlan Les configurations vlan sont normalement fonctionnelles

VI Dhcpv4

`Coeur` va fournir les adresses et les configurations de base pour les 3 vlans.

Q.VI.1) - Activez le dhcp sur `Coeur`.

Q.VI.2) - Faites en sorte de ne pas distribuer les 5 dernières adresses des 3 vlans

Q.VI.3) - Appelez les pools respectivement `poolUser`, `poolAdmin` et `poolWifi`.

Q.VI.4) - En plus des adresses fournissez aux clients le domaine `pres.fr`, le dns `1.2.3.4` et le routeur par défaut.

Q.VI.5) - Testez le fonctionnement du DHCP sur `User1`, `User2` et `PCAdmin`.

VII Routage OSPF

`Coeur` et `Porte` doivent s'échanger leurs routes via le protocole `OSPF`. Vous n'utiliserez qu'une seule zone.

Q.VII.1) - Configurez la zone OSPF sur `Coeur` et `Porte`.

1(a) - Utilisez l'ID de processus **1** sur `Porte` et **2** sur `Coeur`.

1(b) - Affectez les IDs de routeurs 1.1.1.1 (`Porte`), 2.2.2.2 (`Coeur`).

1(c) - Empêchez la transmission des mises à jour du routage sur les interfaces ne comportant pas de routeur et la liaison vers l'extérieur.

1(d) - Demandez à `Porte` d'etre le routeur de sortie.

VIII Network Addresse Translation (NAT)

Configurez les fonctions NAT/PAT sur `Porte` (voir A.4)

Q.VIII.1) - Configurez une traduction d'adresse statique pour le serveur `www.pres.fr`

1(a) - Utilisez `192.168.0.1` comme adresse interne.

1(b) - Utilisez `192.10.10.11` Comme adresse publique.

1(c) - Activez la traduction pour tous les ports de `www.pres.fr`.

Q.VIII.2) - Configurez la traducion pour toutes les autres machines du réseau interne.

2(a) - utilisez un pool d'adresses nommé `poolNat` et utilisant la plage `191.10.10.2` à `191.10.10.9`.

2(b) - Traduisez les adresses de tout le réseau `192.168.0.0/16`.

2(c) - Utilisez une acl standard de numéro 1.

2(d) - Faites en sorte que plus de 30 machines puissent se connecter à internet simultanément.

IX ACL

Pour les ACL, consultez l'annexe A.1

Q.IX.1) - Protégez l'entrée du réseau `Admin` par une ACL étendue nomée `adminAcl`.

1(a) - Placez l'ACL en entrée du réseau `Admin`

1(b) - Autorisez les réponses aux pings, ainsi que les packets tcp dont le status est `established`.

1(c) - Interdisez tous les autres paquets IP.

Q.IX.2) - Protégez l'entrée de votre réseau par une ACL nommée `outAcl`.

2(a) - Autorisez les pacquets vers le site web de `www.pres.fr`.

2(b) - Autorisez les paquets udp qui proviennent d'un serveur DNS à l'extérieur.

2(c) - Placez l'ACL à l'entrée de votre réseau.

X Firewall à état

L'acl `outAcl` doit normalement interdire à aux machine du réseau d'accéder au serveur distant. En effet, la sortie vers l'extérieur est maintenant autorisée, mais la réponse du serveur est refusée. Pour que la discussion entre l'interieur et l'extérieur soit de nouveau possible il faut donc faire en sorte d'ouvrir le firewall pour les réponse à des requetes en provenance de l'interieur. Pour cela, il est necessaire pour le firewall de se modifier automatiquement. En effet, ce dernier doit maintenir un état des paquets sortant pour autoriser le retour.

Cela est fait sous la forme d'un inspection, c'est a dire que le routeur de sortie va espionner les paquets sortant et automatiquement modifier l'ACL d'entrée afin d'autoriser le retour, voir A.3

Q.X.1) - Creez une inspection sur `Porte` appelée `outIns`. Elle doit concerner les paquets `ICMP`, `TCP` et `UDP`.

Q.X.2) - Placer l'inspection en sortie du réseau afin de modifier l'ACL `outAcl`.

A Liste de Contrôle d'Accès ACL

A.1 ACL standard

Configuration d'une ACL standard : Le numéro utilisé doit être inférieur à 99

```
Router(config)# access-list access-list-number
        {permit | deny | remark remark} source [source-wildcard] [log]
Router(config)# no access-list acces-list-number
Router(config-if)# ip access-group {access-list-number | access-list-name}
        {in | out}
Router# show access-lists [acces-list-number | NAME]
```

Configuration d'une ACL standard nommée :

```
Router(config)# ip access-list standard NAME
Router(config-std-nacl)# sequence-number [permit|deny|remark]
        source [source-wildcard] [log]
Router(config-if)# ip access-group access-list-name {in | out}
Router# show access-lists [NAME]
```

A.2 ACL étendue

Configuration d'une ACL étendue : les Acls étendues utilisent un numéro supérieur à 100.

```
Router(config)# access-list access-list-number {permit | deny | remark}
         protocol source [source-wildcard]
             [operator operand] [port port-number or name]
         destination [destination-wildcard
             [operator operand] [port port-number or name] [established]
Router(config)# access-list access-list-number {permit | deny}
         protocol source source-wildcard
         destination destination-wildcard
         {eq | neq | gt | lt | range} protocol-number [established]
Router(config-if)# ip access-group {access-list-number | access-list-name}
         {in | out}
Router# show access-lists [acces-list-number | NAME]
```

Configuration d'une ACL étendue nommée :

```
Router(config)# ip access-list extended NAME
Router(config-ext-nacl)# sequence-number [permit | deny | remark]
         protocol source [source-wildcard]
         destination [destination-wildcard]
         {eq | neq | gt | lt | range} protocol-number [established]
Router(config-if)# ip access-group access-list-name {in | out}
Router# show access-lists [NAME]
```

A.3 ACL dynamique

A.3.1 Context Based Access Control (CBAC)

Associée à une ACL étendu, cela permet de tracer les sessions (tcp, udp, telnet...) qui demanderont un retour et de leur ouvrir l'accès. Très utile pour configurer un pare-feu ou tout peut sortir mais rien rentrer.

```
Router(config)# ip inspect name nom {tcp|udp|icmp|...}
Router(config)# ip access-list extended 100
Router(config-ext-acl)# !! uniquement avec une ACL étendue
Router(config-ext-acl)# deny ip any any
Router(config)# interface Serial 0/0/0
Router(config-in)# ip access-group 100 in
Router(config-in)# ip inspect nom
```

Il est possible d'inspecter plusieurs protocoles et de placer l'inspection sur une autre interface. Par contre, comme le CBAC modifie la règle d'ACL pour ajouter une permission sur les paquets correspodant avec protocole, ip source, ip destination, port source et port destination, cela n'ouvre que les ACL étendues.

A.4 fonctionnement du nat

Pour mettre en place le nat sur le routeur, il faut d'abord identifier les interfaces internes et externes du réseau. Pour cela, dans la configuration de chaque interface concernée, il faut utiliser :

```
Router(config)# interface type number
Router(config)# ! pour les interface internes
Router(config-if)# ip nat inside
Router(config)# interface type number
Router(config)# ! pour les interface externes
Router(config-if)# ip nat outside
```

Ensuite en mode configuration
Configuration de la traduction statique :

```
Router(config)# ip nat inside source static local-ip global-ip
```

Configuration de la redirection de port :

```
Router(config)# ip nat inside source static protocol
         local-ip port global-ip port
```

Configuration de NAT dynamique sans surcharge de port :

```
Router(config)# ip nat pool NAME start-ip end-ip
         {netmask netmask | prefix-length prefix-length}
Router(config)# access-list access-list-number permit
         source [source-wildcard]
Router(config)# ip nat inside source list access-list-number pool NAME
```

Configuration de la surcharge NAT *première configuration possible* (utilisant l'adresse de l'interface de sortie) :

```
Router(config)# access-list access-list-number permit
         source [source-wildcard]
Router(config)# ip nat inside source list access-list-number
         interface interface overload
```

Configuration de la surcharge NAT *deuxième configuration possible* (utilisant un pool d'adresse) :

```
Router(config)# access-list access-list-number permit
         source [source-wildcard]
Router(config)# ip nat pool NAME start-ip end-ip
         {netmask netmask | prefix-length prefix-length}
Router(config)# ip nat inside source list access-list-number
         pool NAME overload
```

Dans les deux configurations, le mot clef `overload` déclanche la surcharge
Visualisation et dépannage de NAT :

```
Router# show ip nat translations [verbose]
Router# show ip nat statistics
Router(config)# ip nat translation timeout timeout-seconds
Router# clear ip nat translation *
Router# clear ip nat translation inside global-ip local-ip [outside
local-ip global-ip]
Router# clear ip nat translation protocol inside global-ip global-port
local-ip local-port [outside local-ip local-port global-ip global-port]
Router# debug ip nat [detailed]
```