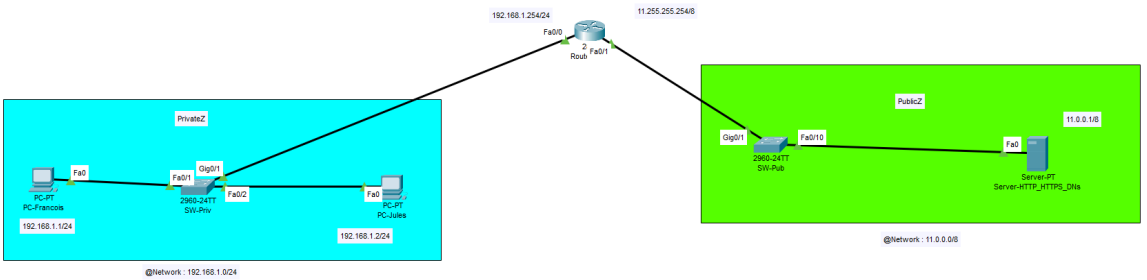
Pare-feu ZPF



Création des zones

Création des zones logiques permettant le filtrage des paquets

```
zone security [NAME zone]
```

Dans notre exemple on créer les deux zones correspondant au réseau privée et public de notre maquette :

```
zone security PrivateZ
zone security PublicZ
```

Création class-map

Défini les protocoles autorisés

```
class-map type inspect match-[any | all] [NAME class-map]
      match protocol [http | https | dns | ...]
```

On créer la class-map correspondant aux protocoles que l'on veut filtrer sur notre exemple (HTTP, HTTPS, DNS)

```
class-map type inspect match-any HTTP-TRAFFIC
 match protocol https
 match protocol dns
 match protocol http
```

Création policy-map

Définition du mode d'analyse ZPF (inspect | drop | pass) d'une class-map

On créer la policy map qui définira les protocoles de la class-map en mode inspect ou drop ou pass (dans l'exemple inspect)

```
policy-map type inspect PrivateZ-TO-PublicZ-PM
 class type inspect HTTP-TRAFFIC
  inspect
```

```
policy-map type inspect [NAME policy-map]
      class-type inspect [NAME class-map]
      inspect
```

Création zone pair

Association du sens d'analyse du flux (source et destination) + association policy-map

On créer une zone-pair qui permet de définir le sens de filtrage du flux (ici PrivateZ vers PublicZ)

```
zone-pair security PrivateZ-TO-PublicZ-ZP source PrivateZ destination PublicZ
 service-policy type inspect PrivateZ-TO-PublicZ-PM
```

```
zone-pair security [Name zone-pair] source [NAME zone] destination [NAME
Zone]
      service-policy type inspect [NAME policy-map]
```

Attribution des interfaces dans les zones

Définis les emplacements des zones dans notre réseau.

Pour finir on attribue sur les ports du routeur la zone correspondant

```
interface FastEthernet0/0
 ip address 192.168.1.254 255.255.255.0
 zone-member security PrivateZ
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 11.255.255.254 255.0.0.0
 zone-member security PublicZ
 duplex auto
 speed auto
```

```
int [gi | se] [N°]
      zone-member security [NAME zone]
```

Test du filtrage

Tester la communication sur les protocoles définis + retirer un protocole autorisé auparavant pour constater que désormais il est restreint + ping en continu (+ FTP pour tester car présent par défaut sur Packet Tracer)

cla