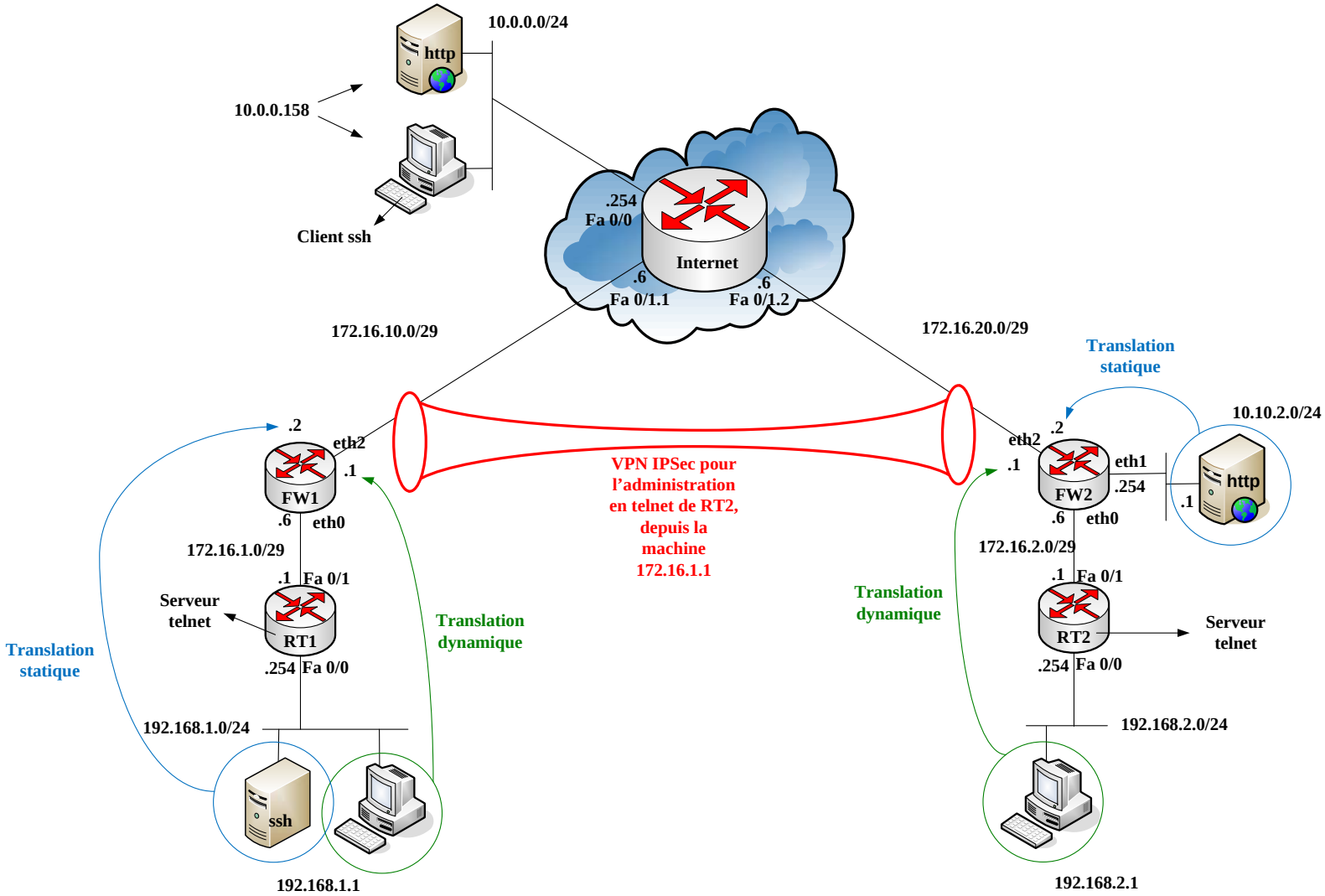
Utilisation des Firewalls : VPN IPSec



Objectif

- Mise en route d'un Firewall dans une configuration standard, c'est à dire :
  - à l'interface entre les domaines privé et public,
  - avec des clients internes qui veulent utiliser l'Internet,
  - avec des services internes à rendre publics,
  - avec un VPN d'interconnexion.

Matériel

- 2 ASA 5510
- 3 routeurs standards (28xx)
- 1 switch 2950 avec fonction VLAN
- 3 petits switch

Architecture logique

L'adressage des branches est choisi de manière à pouvoir ajouter autant de branches que désiré :

- réseau interne :192.168.x.0/24
- interconnexion interne : 172.16.x.0/29
- DMZ (si utilisé) : 10.10.x.0/24
- interconnexion à l'Internet : 172.16.x0.0/29

Un réseau représente les machines de l'Internet :

- 10.0.0.0/24

Les réseaux 10.0.0.0/24 et 172.16.x0.0/29 sont considérés comme publics

Architecture physique

Les segments d'interconnexion à l'Internet (172.16.x0.0/29) peuvent être assez nombreux (selon la quantité de matériel disponible). Ils sont donc réalisés avec le switch 2950, à l'aide des VLANs. Le routeur « Internet » est relié au 2950 par un lien en mode « trunk », et assure ainsi le routage entre les segments d'interconnexion, le réseau 10.0.0.0/24, et le réseau de l'UTT en 10.23.0.0/24 (non représenté sur le schéma).
Pour le segment x, le numéro de VLAN et le nom de la sous interface du routeur Internet sont égaux à x.
Les segments d'interconnexion interne (172.16.x.0/24) sont réalisés avec un câble droit qui relie directement le routeur x au firewall x.

Services nécessaires

- Machine Internet (10.0.0.158) : client web, client ssh (putty), serveur web
- RT1 : client telnet, serveur telnet (console d'administration)
- 192.168.1.1 : client telnet, client web, serveur ssh
- 10.10.2.1 : serveur web
- RT2 : serveur telnet (consle d'administration)
- 192.168.1.1 : client web

Mise en œuvre

Etape 1 Configuration de base

- Réaliser l'architecture physique :
  - utiliser des couleurs différentes pour chaque branche
  - ne pas oublier le 2950 qui n'apparaît pas sur le schéma logique
  - vérifier l'état des liens avec les LEDs sur les interfaces des équipements
- Création des segments d'interconnexion :
  - créer les VLANs sur le 2950
  - activer 802.1q sur le lien vers le routeur « Internet »
- Activation des interfaces :
  - paramétrer les adresses IP des équipements réseau, et des ordinateurs
  - vérifier l'état des liens avec les LEDs sur les interfaces des équipements
- Résolution du routage (sans protocole de routage car non souhaitable dans ce cas) :
  - configurer la passerelle sur chaque ordinateur
  - RT1 : passerelle
  - FW1 : route vers 192.168.1.0/24 et passerelle par défaut
  - même chose pour la branche 2 (et toutes les autres)
  - remarque : le routeur Interne ne connaît que les réseaux «publics », c'est-à-dire 172.16.x0.0/29 et 10.0.0.0/24, il ne routera pas de paquets à destination des 192.168.x.0/24 ni vers 10.10.x.0/24
- Activation des services :
  - sur les machines
  - sur les routeurs

A la fin de cette étape, aucune communication n'est possible à travers les firewalls.

Etape 2 Communications sortantes vers l'Internet

- Sur FWx : réaliser la translation dynamique des machines du réseau 192.168.x.0/24 vers l'adresse 172.16.x0.1 (celle de l'interface eth2 de FWx)

Essayer en faisant une requête web depuis 192.168.x.1 vers 10.0.0.158

Etape 3 Publication de services

- Réaliser la translation statique du service web de 10.10.2.1 vers l'adresse 172.16.20.2
- Appliquer l'ACL qui autorise l'entrée de requêtes web vers 172.16.20.2 dans FW2

Essayer en faisant une requête web depuis 10.0.0.158 vers 172.16.20.2

- Réaliser la translation statique du service ssh de 192.168.1.1 vers l'adresse 172.16.10.2
- Appliquer l'ACL qui autorise l'entrée de requêtes ssh vers 172.16.10.2 dans FW1

Essayer en lançant le client ssh putty sur 10.0.0.158, vers 172.16.10.2

Etape 4 Réalisation de l'interconnexion

- Sur FW1 : créer une ACL pour désigner les flux qui doivent passer dans le VPN (permit tcp 192.168.1.0 0.0.0.255 host 172.16.2.1 eq telnet)

- Sur FW2 : créer une ACL pour désigner les flux qui doivent passer dans le VPN (permit tcp host 172.16.2.1 eq telnet 192.168.1.0 0.0.0.255)
- Sur FW1 et FW2 :
    - créer une SA ISAKMP
    - créer une SA IPSec
    - créer une table des VPNs en désignant le FW distant par son adresse IP
    - lier les SAs et l'ACL à ce VPN
    - appliquer cette table des VPNs à l'interface outside

  Essayer depuis une fenêtre de commande de 192.168.1.1 en lançant un telnet vers 172.16.2.1

Etape 5 Jouer avec cette architecture

Session cliente sortante :

- établir une session http depuis 192.168.1.1, vers 10.0.0.158
- pour cela il faut :
    - résoudre le problème du routage
    - réaliser la translation dynamique des clients vers l'interface « outside » du firewall

Session cliente entrante :

- ouvrir un client ssh sur 10.0.0.158 et lancer une requête vers 172.16.10.2, cela permet la prise de contrôle de la machine 192.168.1.1
- pour cela, il faut :
    - résoudre le problème du routage
    - réaliser la translation statique du service ssh de 192.168.1.1 vers 172.16.10.2
    - appliquer une ACL qui laisse entrer les requêtes ssh par l' « outside » du firewall

Session privée entre les deux branches, à travers l'Internet :

- depuis une console sur 192.168.1.1, lancer un telnet sur 192.168.1.254, on a maintenant le contrôle du routeur RT1,
- depuis RT1, lancer un telnet sur 172.16.2.1, on gagne ainsi le contrôle de RT2 à travers le VPN (communication chiffrée par le VPN, et non pas par telnet), pour cela, sur chaque firewall :
    - créer l'ACL qui capte le flux à faire passer dans le VPN
    - créer les Sas ISAKMP et IPSec
    - créer la table des VPNs, et faire les liens avec l'ACL et les Sas
    - appliquer la table des VPNs à l'interface « outside » du firewall