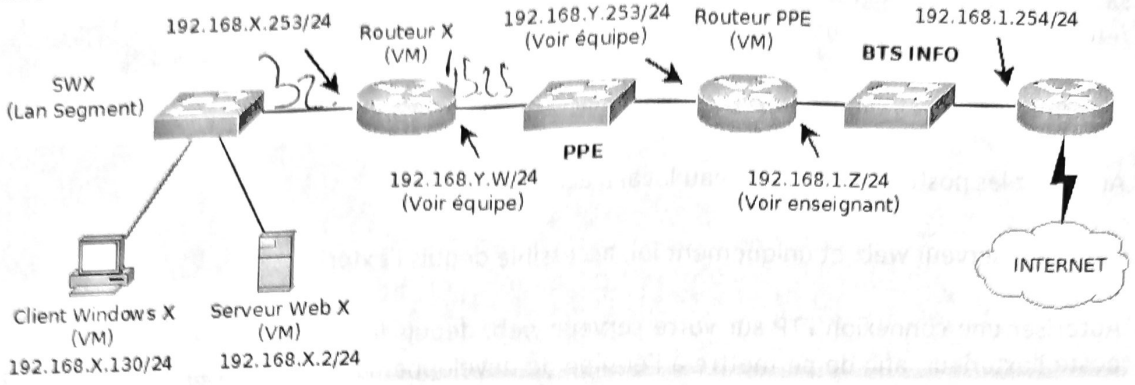
TP FILTRAGE

PRESENTATION

On considère votre infrastructure selon le schéma suivant :



Avant de commencer ce TP, vous devez disposer :

- de X et Y qui correspondent à des numéros de vlan qui vous ont été attribués.
- de W et Z qui correspondent à des adresses que vous aurez définies en concertation avec les personnes ad hoc.
- Un routeur RX avec 2 interfaces (administrable par ssh).
- Un serveur Web (ex : un serveur Apache/Linux) avec une page d'accueil personnalisée.
  Un PC X (Linux ou Windows) avec un client ssh (ex : putty).

Vous devez rendre un rapport contenant :

- Une introduction permettant de présenter vos objectifs.
- Des démonstrations :
  - État initial et scénario de test.
    État de ce qui fonctionne et ce que vous souhaitez obtenir.
  - Action.
    Commandes ou actions que vous mettez en œuvre pour répondre au besoin avec la copie d'écran pour le prouver.
  - Test de recette.
    Commandes ou actions que vous mettez en œuvre pour montrer que cela fonctionne avec la copie d'écran pour le prouver.
  - Tests de non-régression.
    Commandes ou actions que vous mettez en œuvre pour montrer que vos modifications n'ont pas nui au système avec la copie d'écran pour le prouver.
- Une conclusion permettant une rétrospective et un état de votre travail.

TRAVAIL A FAIRE

1. Fournir le schéma Visio de votre nouvelle infrastructure qui intègrera le serveur web dans une DMZ, et renseignez la matrice de communication.
   Vous ajouterez l'ensemble des informations que vous jugez utiles : adresses IP, Ports, ...

MATRICE DE COMMUNICATION

Communique avec ->	Internet (Wan)	CltWin1 (Ext)	Debian Routeur (Routeur)	Serveur Web (DMZ)	Serveur DHCP (Lan)	Debian2 (Lan)	CltWin7 (Lan)
CltWin1 (Ext)							
Debian Routeur							
Serveur Web (DMZ)							
Serveur DHCP (Lan)							
Debian2 (Lan)							
CltWin7 (Lan)							

2. Définir la politique de filtrage par défaut et mettre en œuvre une nouvelle politique en « liste blanche ».

3. Vous vous rendez compte que vous ne pouvez plus administrer votre routeur par SSH. Analysez la situation et remédier au problème.

4. Sauvegardez vos règles de filtrage est essentiel. Définissez une sauvegarde dans un fichier /etc/filtres.save, dont vous vérifierez la validité.

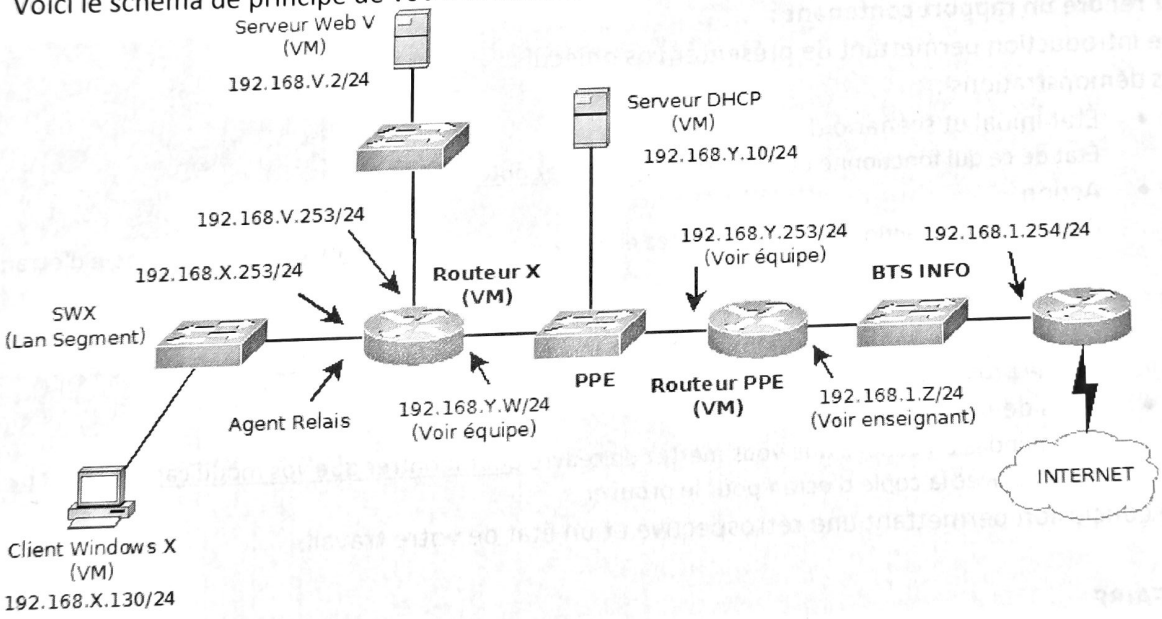
5. Autorisez les postes clients du réseau local à accéder à votre serveur web.

6. Autorisez les postes clients du réseau local à accéder à Internet.

7. Rendre le serveur web, et uniquement lui, accessible depuis l'extérieur.

8. Autoriser une connexion FTP sur votre serveur web, depuis les postes du réseau LAN et depuis un seul poste l'extérieur, afin de permettre à l'équipe de développement d'alimenter le site Internet du serveur Web.

9. (Bonus) Vous disposez d'un LAN personnel (X) et d'une DMZ personnelle (V) qui vous ont permis de réaliser individuellement de TP.
Le serveur DHCP doit être en Production dans un Vlan spécifique (ici dans le Vlan de PPE : Y). Il est configuré pour adresser chacune des zones personnelles (et notamment X).
N'étant pas dans le même réseau que les Lan personnels, il doit donc se faire seconder par un agent relais.
Voici le schéma de principe de votre architecture :



La création d'un nouveau poste en adressage dynamique dans votre Lan personnel est-elle fonctionnelle ? Analysez et remédiez au problème.

10. (Bonus) Bonnes pratiques.
    a) Comment supprime-t-on des règles ?

    b) Le serveur web peut-il faire les mises à jour de son OS ?

    c) Est-il possible de pinger le routeur ?

    d) Quels outils vous permettraient de faciliter la tâche de gestion des règles de filtrage ?