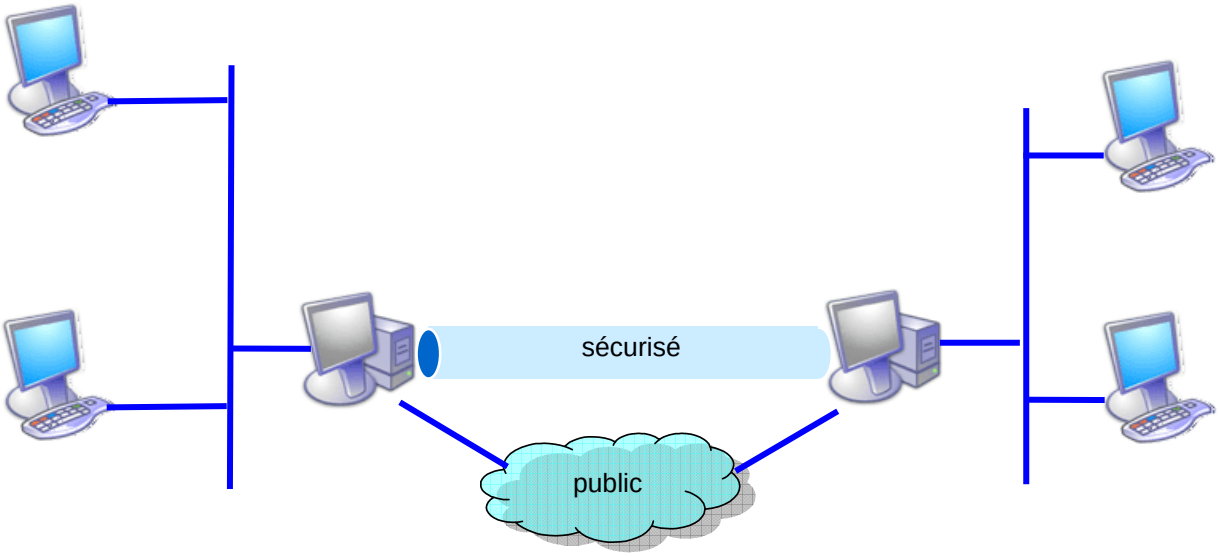
TP Sécurité : Pare-feu et IPSec

But du TP : Mettre en œuvre d'une architecture sécurisée avec pare-feu et IPSec

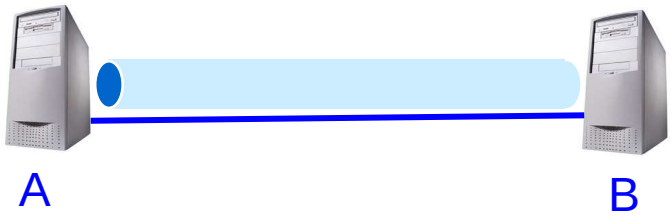
- **Topologie générale du réseau :** Deux réseaux locaux sont interconnectés via 2 routeurs A et B par un réseau public non sécurisé. On souhaite mettre en œuvre une solution de connexion sécurisée pour les routeurs et/ou les stations des réseaux locaux.



Etape A : Création routeurs et configuration IP

Remarque préliminaire : Les étapes de ce TP sont volontairement un peu moins détaillés que précédemment, ne pas hésiter à prendre des initiatives pour obtenir les réponses aux questions. Le TP peut être réalisé en binôme, chacun créant les MV à une extrémité de la liaison IPSec.

Copier la machine FreeBsd62… en …\IPSECA et en …\IPSECB



Configurer l'un après l'autre les 2 routeurs IPSecA et IPSecB :

- Connexion des cartes réseaux : les liaisons entre les MV IPSec seront réalisées en mode Pont sous VMWare.
- Les adresses IP seront assignées statiquement aux interfaces et seront choisies dans la plage **10.0.X.0/26** pour les interfaces publiques (Choisir un **X** différent pour chaque binôme).
  - Un schéma récapitulant toutes les informations de configuration DOIT absolument être maintenu à jour en parallèle des configurations …

- Installer et tester une application client/serveur UDP (netcat ou autre).

Remarque bis : Les MV connectées en mode Pont/10.0.X.0 dans le réseau local du Dpt communiquent entre elles, mais ne permettent pas d'accéder aux autres adresses locales ou distantes. Si vous deviez mettre à jour la MV, passez l'interface ne mode NAT/DHCP, puis revenez en mode Pont/10.0.X.0 une fois la mise à jour effectuée.

- La communication est elle possible ? Capturez les trames dans lesquelles on voit le message passer en clair dans le réseau public

Etape B : Mise en place d'un pare-feu

- Charger le module ipfw.ko dans le noyau des routeurs A et B. Les modules sont dans le répertoire /boot/kernel et peuvent être dynamique chargés et déchargés du noyau FreeBsd sans nécessiter le reboot du système.
- Mettre en place les règles qui autorisent les communications UDP sur A et B, mais filtrent toutes les autres communications (commande *ipfw*)
- Attention, lors de l'activation du pare-feu, toutes les communications sont interdites par défaut.

- La service UDP est il sécurisé par le pare-feu ?

Etape C : Mise en place d'un VPN IPSec en mode transport

Remarque ter: le manuel n'étant pas totalement installé sur les MV, consulter

http://www.freebsd.org/doc/fr_FR.ISO8859-1/books/handbook

- Vérifier si le noyau des MV inclut IPSec, sinon recompiler le noyau FreeBSD avec les options IPSEC et IPSEC_ESP.
- Mettre en place les associations et les politiques de sécurité pour une liaison A-B sécurisée avec authentification (et chiffrement) : configuration manuelle des clés.

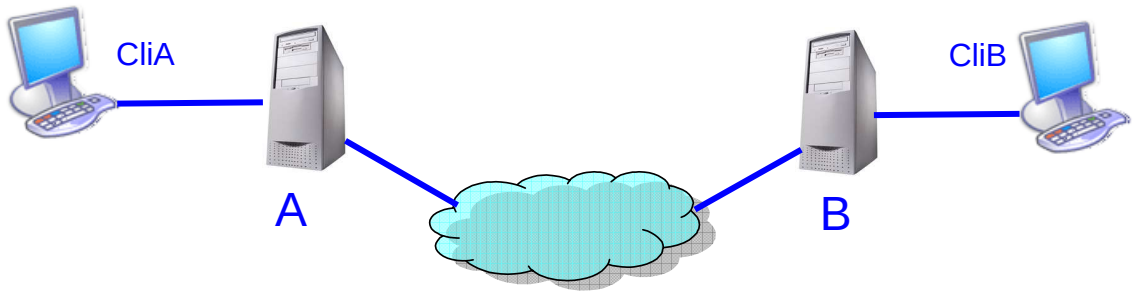
- En quoi la communication entre A et B est-elle sécurisée ? Le service UDP bénéficie-t-il de ce VPN ? Capturez les trames qui montrent les messages échangés.

Etape D : Communication entre 2 réseaux locaux

Créer les MV CLIA et CLIB

Configurer l'un après l'autre les 2 clients CliA et CliB et utiliser le mode NAT pour les liaisons CliA-A et CliB-B.

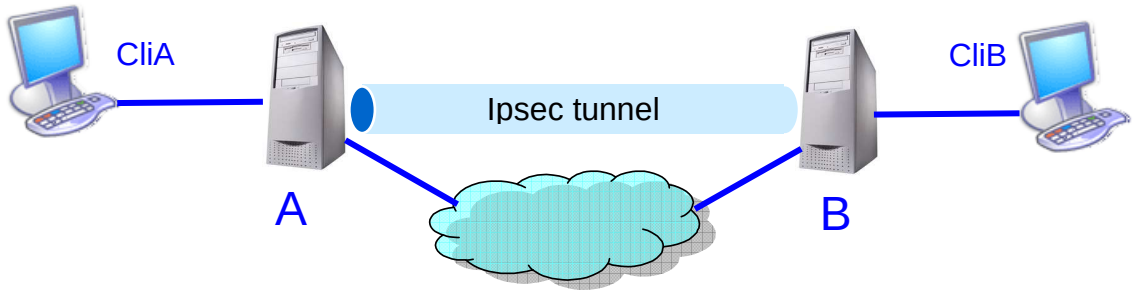
- les adresses IP dans les réseaux privés seront choisies dans les plages 10.0.X.64/26 et 10.0.X.128/26.
- supprimer le pare-feu
- mettre en place de routes statiques nécessaires à la communication entre CliA et CliB (ICMP, service UDP ou apache/lynx)



➢ Mettre à jour le schéma avec toutes les adresses IP/Masque et le routes.

Etape E : Mise en place d'un VPN IPSec en mode tunnel

- Mettre en place le tunnel IPSEC garantissant l'authentification et la confidentialité en mode tunnel entre A et B pour les 2 réseaux locaux.



➢ Quelles applications peuvent bénéficier de cette sécurité ? Capturez les trames qui montrent qu'aucun message ne transite en clair (ICMP, service UDP ou apache/lynx).
➢ Quelle configuration faudrait-il déployer pour éviter la configuration manuelle des clés ?
➢ Quelle configuration de pare-feu faut-il déployer pour empêcher *ping* et *traceroute* mais autoriser le service UDP.

- **Conclusion générale et comparaison des approches ssh et IPSec pour la création de communications sécurisées.**

DOSSIER A RENDRE :

Vous rédigerez étape par étape un dossier dans lequel vous indiquerez les résultats obtenus à chaque étape, (copies d'écran, trames, schémas) et les réponses aux éventuelles questions.
Le dossier sera nommé *S51_TP3_<Nom1_Nom2>*.pdf (ex : *S51_TP3_Muller_Dupont.pdf*) et sera envoyé par mail (*S51_TP3_Muller_Dupont.zip* → *Dominique.Grad@urs.u-strasbg.fr*) pour le **dimanche 27 janvier 08 au plus tard.**