Rappel de l‘infrastructure réseau des deux compagnies A et B :



A faire pour la compagnie A et la compagnie B : les indications ne concernent que la compagnie A mais il faut aussi le faire pour la compagnie B si nécessaire

* en remplaçant x par 1 pour la compagnie A
* et x par 2 pour la compagnie B.

Dans la politique de filtrage/NAT « **compagnie\_X** », supprimez la règle de filtrage **Pass all** et ajoutez les règles de filtrage qui respecteront le cahier des charges suivant (utilisez les séparateurs en indiquant le rôle de chaque règle) :

## Trafics internes :

1. 1. Votre réseau interne doit pouvoir accéder aux serveurs de la DMZ (DNS, WEB (ports 80 et 808 pour le webmail), FTP et SMTP).

**Indications** :

Afin de réaliser votre politique de filtrage, allez dans le menu **Politique de sécurité => filtrage et NAT**.

## Trafics sortants :

1. Votre réseau interne, doit pouvoir naviguer sur les sites web d'Internet en HTTP et HTTPS, sauf sur les sites de la République de Corée (test avec [www.visitkorea.or.kr](http://www.visitkorea.or.kr)).
2. L’accès au site https://www.cnn.com doit être bloqué depuis le réseau interne, en utilisant un objet FQDN.
3. Un stagiaire, nouvellement arrivé dans l'entreprise, a l'interdiction d'effectuer la moindre requête FTP. L'adresse IP de sa machine (pc\_200) est 192.168.x.200.

**Indications** :

Au préalable, vous devrez créer un objet de type machine nommé **pc\_200**, portant l'adresse IP **192.168.x.200**.

1. Votre réseau interne doit pouvoir joindre les serveurs FTP et Web de l’autre compagnie.
2. Votre réseau interne doit pouvoir émettre un ping vers n'importe quelle destination.
3. Seul votre serveur DNS interne (172.16.x.10) est autorisé à résoudre vers l'extérieur.
4. Votre serveur de messagerie peut envoyer des mails vers le serveurs publié par l’autre entreprise.

## Trafics entrants :

1. L’autre entreprise peut joindre vos serveurs Web et FTP ; ces événements doivent être tracés.
2. Le serveur mail de l’autre entreprise est autorisé à transmettre des e-mails à votre serveur de messagerie.
3. L’autre entreprise est autorisée à pinger l'interface externe de votre firewall; ce type d’événement doit lever une alarme mineure.
4. L’autre entreprise peut se connecter à votre firewall : via l’interface web et en SSH. Ce type d’événement doit lever une alarme majeure.

**Indications** :



L’ensemble des flux est journalisé avec cette politique, les règles en **Passer** étant en TCP/UDP, les règles en **Passer** ou **Bloquer** pour ICMP ayant un mode de journalisation **verbeux**.

Pour autoriser l’autre entreprise à se connecter à votre firewall via l’interface web, il faut ajouter son adresse IP publique dans l’encadré **Accès aux pages d’administration du firewall** du menu **Système => Configuration =>** onglet **Administration du firewall** (pas d’alarme pour ce flux spécifique, donc).

Pour cette activité, vous devez considérer le réseau externe inter-entreprises comme un réseau public dans lequel aucune adresse IP privée n’est tolérée.

1. Désactivez les routes statiques ajoutées dans l’activité précédente.

**Indications** :

Désactivez les routes statiques vers les réseaux distants à partir du menu **Configuration => Réseau => Routage => Routage statique**. Si vous n’avez pas fait l’activité bonus **Objets**, créez deux nouveaux objets qui seront ensuite utilisés dans vos règles de NAT :

* srv\_ftp\_pub = 192.36.253.x2
* 0et srv\_mail\_pub = 192.36.253.x3.
1. Copiez la politique de filtrage/NAT **(10) Pass all** vers une autre politique vide en la renommant « **compagnie\_X** » (remplacez X par la lettre A ou B selon la compagnie). Ensuite, activez cette politique.

**Indications** :

Afin de construire votre politique, allez dans le menu **Politique de sécurité => Filtrage et NAT**. Copiez la politique **(10) Pass all** vers une politique vide en cliquant sur **Editer** ensuite **Copier vers**. Depuis le menu déroulant, sélectionnez la politique correspondante puis cliquez sur **Editer** puis **Renommer**.

1. Ajoutez une règle de NAT afin que les machines de vos réseaux internes puissent accéder au réseau externe sans que leur IP privée n’y soit vue. Ensuite, testez l’accès au réseau externe et l’accès à internet depuis votre **Débian graphique** (l’accès à internet est possible via la passerelle 192.36.253.1 si la translation est correctement configurée).
2. Vous disposez de 2 adresses IP publiques supplémentaires « 192.36.253.x2 » et « 192.36.253.x3 » réservées respectivement à vos serveurs FTP et MAIL situés en DMZ. Ajoutez les règles de NAT qui permettent de joindre chaque serveur depuis le réseau externe grâce à son adresse IP publique.
3. Ajouter une règle de NAT afin que votre serveur WEB situé en DMZ soit joignable grâce à une redirection de port via l’adresse IP publique portée par votre firewall « 192.36.253.x0 ».

**Indications** :

Ajoutez les règles de NAT suivantes :



Notez que la règle de NAT dynamique a été mise après les règles de NAT statiques. Dans le cas contraire, les serveurs FTP et SMTP souhaitant sortir sur Internet auraient après translation l’IP publique du firewall au lieu de leur IP publique dédiée. L’ordre du cahier des charges donné dans l’activité était donc à remettre en cause.

N'oubliez pas d'activer la politique et de valider les accès avec l’autre compagnie.

1. Tracez les règles de NAT pour les flux entrants.

**Indications** :

Les règles de NAT tracées sont dans le journal **Monitoring => Journaux d’audit => Filtrage**.

1. Avec l’autre entreprise, testez l'accès à l'ensemble des ressources (le serveur MAIL peut être testé à l’aide d’une commande TELNET) et confirmer le traçage des règles demandées dans les logs.

Bonus :

* Ajoutez une règle de NAT afin que les machines de votre réseau interne puissent accéder à vos serveurs en DMZ sans que leur adresse IP privée n’y soit vue.

**Indications** :

La règle de NAT permettant d’accéder aux serveurs e􀅶 DMZ sans que l’IP privée ne soit vue en DMZ est désactivée ci-dessus, et devra rester désactivée pour la suite des activités.

* Quels sont les avantages et inconvénients selon vous de translater les adresses depuis votre réseau interne vers votre DMZ, laquelle est aussi un réseau interne ?

**Indications** :

Si vous l’activez, le firewall qui la traite utilisera plus de performances (table NAT à maintenir), mais un éventuel attaquant ayant pris le contrôle d’un de vos serveurs en DMZ ne pourra pas connaître l’adresse IP du réseau local en capturant les paquets qui en proviennent puisqu’ils sont translatés.