Objectifs pédagogiques :

L’objectif de ce TP est de se familiariser avec un firewall.

Objectifs du TP :

* Gestion des zones
* Gestion des règles

Configuration d’un firewall

**Attention, ne pas toucher la configuration. (Ne pas lancer le wizard). On bidouillera plus tard.**

Groupez vous par 4.

Avant de commencer : autoriser les requêtes de PING dans le pare-feu de votre ordinateur (voir slides).

Connexion à un firewall : Connectez vous sur un des ports entre 0/2 et 0/6.

Quelle adresse IP, masque Gateway vous donne le serveur DHCP du firewall ?

Connectez vous au serveur Web du firewall (Re : ne pas toucher la conf, ne pas lancer le wizard). (Je vous laisse trouver l’adresse IP, et le mot de passe par défaut). Attention, l’interface graphique marche mal sur Firefox….

Dans Network -> Interfaces -> List :

* Comment sont regroupés les interfaces ? (ie : les ports Ethernet)
* A quelle zone est attribué le port 0/0 ? Idem pour 0/1 ?
* Quels sont les interfaces qui peuvent configurer le firewall ?
* Quels sont les moyens de configurer le firewall ?
* Essayé de vous connecter en Telnet

Dans Policy -> Policies :

* Quelle est la règle définie ?
* Attention, il y a une règle sous jacente : Tout ce qui n’est pas clairement indiqué, est interdit !

Dans Policy -> Policy Éléments -> Services -> Predefined :

* Cherchez la règle HTTPS
* Quels est le « transport » utilisé ?
* Quels sont les ports qui doivent être « ouverts » pour laisser passer un flux HTTPS ?

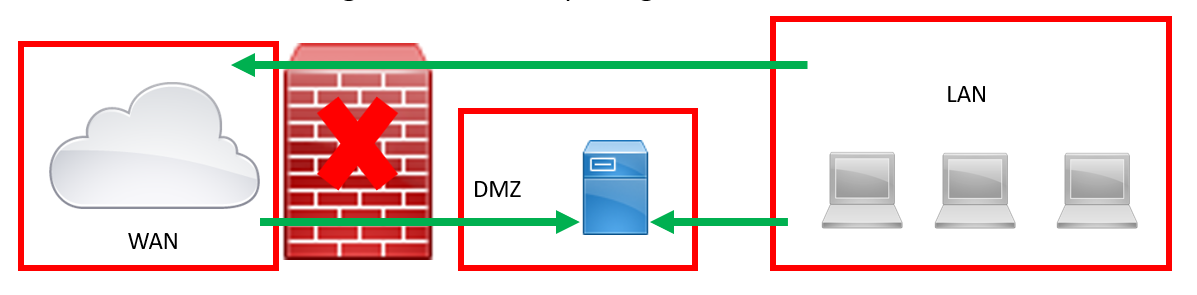
Blobby Volley, le retour

Le problème :

L’entreprise Balonron souhaite monter un réseau de blobby volley. Ils veulent que le serveur soit accessible depuis le WAN et le LAN mais ils ne veulent pas qu’il puisse y avoir de communication WAN <-> LAN . Le serveur va donc se retrouver en DMZ.

Blobby Volley est relativement simple : il n’a pas besoin que du port UDP 1234 pour fonctionner.

Le schéma réseau est le suivant :



Conception :

1. WAN (untrust) : Le RIR vous a attribué l’adresse 2.7.113.69
2. DMZ : Définissez un nom de sous réseau + masque
3. LAN (Trust) : Conservez le plan d’adressage défini dans le firewall

Configuration de l’architecture :

1. WAN : Dans la liste des interfaces, Définissez l’adresse IP/masque (Utilisez /8 même si je ne comprends pas encore pourquoi ….)
2. DMZ : Dans la liste des interfaces, définissez l’adresse IP de l’interface ainsi que son masque
3. Ajouter une règle pour permettre des requêtes PING depuis la zone trust (LAN) vers DMZ
4. Ajouter une règle pour permettre des requêtes PING depuis la zone trust (LAN) vers WAN
5. Ajouter une règle pour permettre des requêtes PING depuis la zone WAN vers DMZ
6. Vérifier que la communication passe.
7. Tester le ping depuis WAN vers LAN, DMZ vers WAN et DMZ vers LAN

Affinage des règles :

1. Créer un nouveau service dans les policy (Policy -> Policiy éléments -> Services -> Custom). Il s’appellera Blobby Volley. Définissez le port de destination 1234 en UDP
2. Dans les règles, ajouter le service Blobby Volley de façon à permettre de jouer à Blobby volley LAN -> DMZ et WAN -> DMZ
3. Jouer !

Fin de l’histoire

Désactiver la règle de PING dans votre firewall

Faire un reset du Juniper (En telnet : reset)

Pour aller plus loin

Trouver comment réaliser du port forwarding (PAT) pour utiliser l’adresse WAN du routeur pour jouer à blobby.