COMPTE RENDU

DMZ multi-niveaux

Par Alexandre BEROT-ARMAND

BTS SIO 2

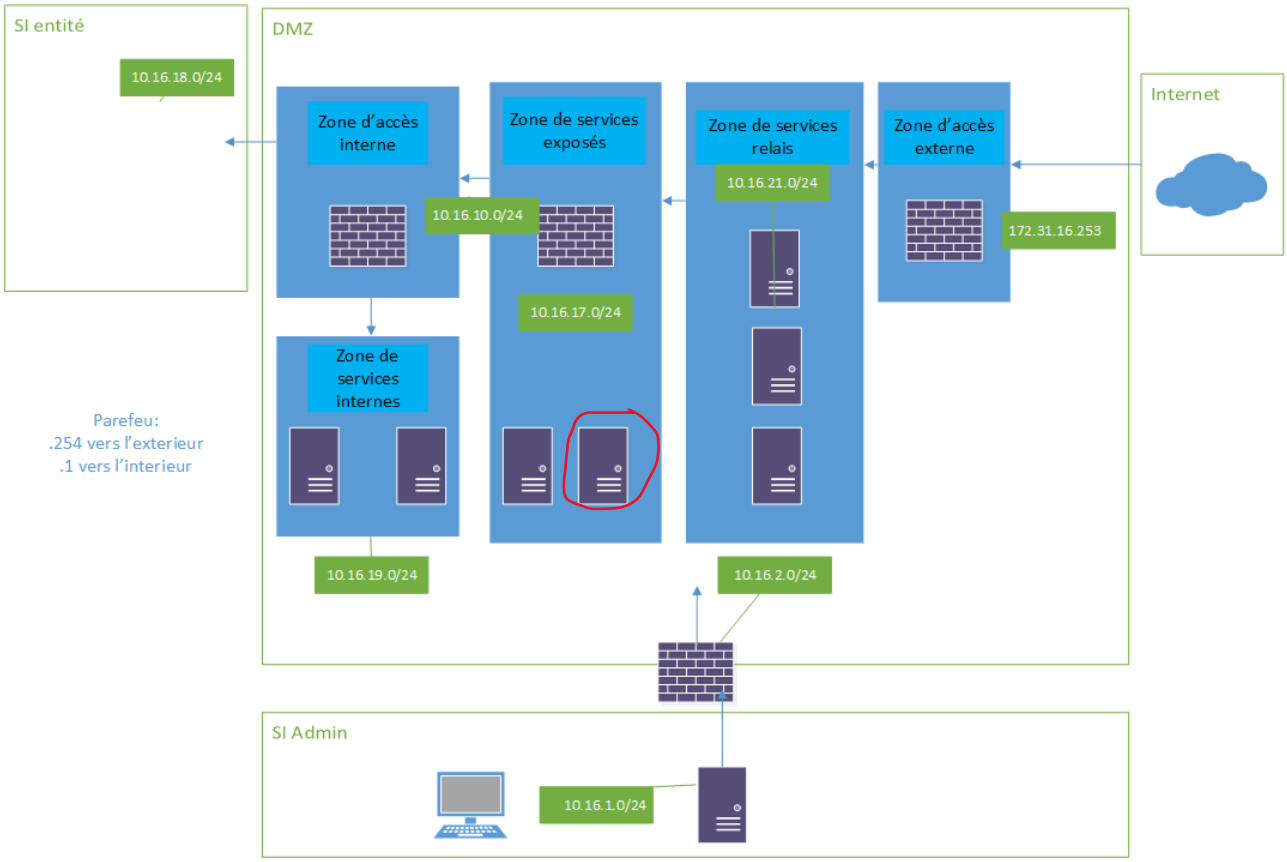
Lycée Louis PERGAUD

TABLE DES MATIERES

INTRODUCTION

Dans le TP précédent, nous avons vu comment faire une DMZ à un niveau pour ajouter un serveur Web accessible depuis l'extérieur du réseau.

Dans ce TP, nous allons augmenter le niveau de sécurité de la DMZ en lui rajoutant des niveaux.
Voici une image de la DMZ finale :



Le serveur entouré en rouge serait l'emplacement du serveur Web.

Une suite de pare-feux successifs casse le flux venant d'internet, chacun protégeant une partie différente du réseau jusqu'à la plus critique soit le réseau interne.

INTERFACES

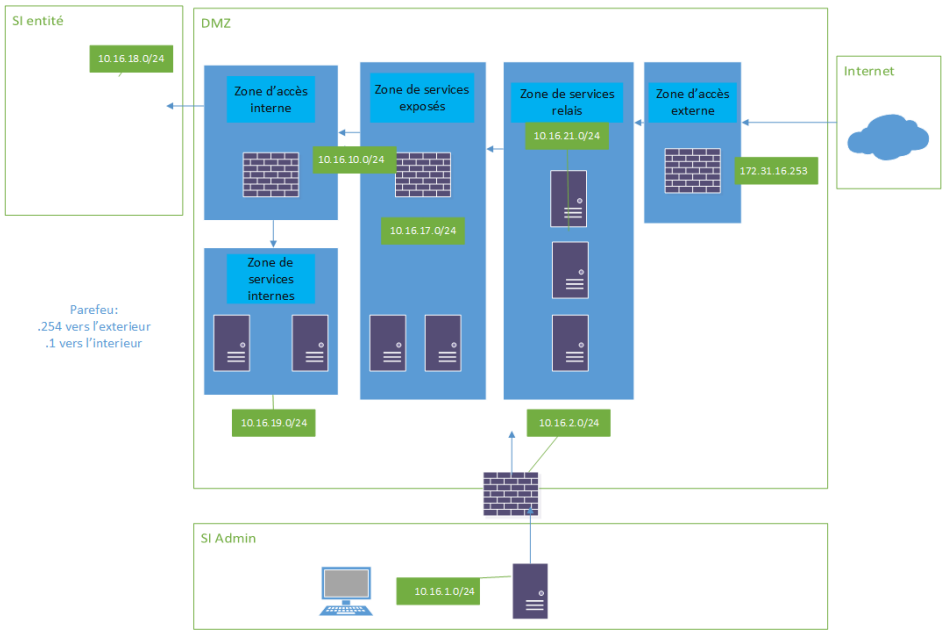
Pour la mise en œuvre de cette DMZ, il va falloir un certain nombre d'interfaces réseaux, une interface par partie soit :

-l'interface sortante vers internet (vmbr0),
-l'interface de la zone de relais de services (vmbr3),
-l'interface de la zone de services exposés (vmbr8),
-l'interface de la zone d'accès interne (vmbr4),
-l'interface de la zone de services internes (vmbr9),
-l'interface de la zone de SI entité (vmbr5),
-l'interface de la zone d'administration des firewalls (vmbr6),
-l'interface de la zone SI administration (vmbr7).

Chacune de ces interfaces couvrira donc un réseau local plus ou moins protégé de la DMZ ; excepté le vmbr0 qui est la sortie vers internet et le vmbr5 qui est le bridge d'entrée du SI entité.

REGLES DES PARE-FEUX

Reprenons l'image du réseau :



On peut voir qu'il y a 4 pare-feux dans cette DMZ :

- Celui de la zone d'accès externe (PF1)
- Celui de la zone de services exposés (PF2)
- Celui de la zone d'accès interne (PF3)
- Celui de la zone du SI administration (PF4)

Par défaut, il ne faut activer l'interface d'administration des pare-feux 1, 2 et 3 que sur l'interface vmbr6 (le réseau uniquement accessible via le SI Admin après le PF4). Cela a pour but d'interdire l'accès à la configuration aux utilisateurs lambda.

Ensuite il faut préparer les règles de NAT et de PAT en fonction de l'emplacement des services. Pour le serveur web situé dans la zone de services exposés, il faut faire un PAT qui redirige les requêtes « http » de la zone d'accès externe à la zone de services exposés puis au serveur en question.

CONFIGURATION PHYSIQUE DES PARE-FEUX

Nous n'allons pas expliquer l'installation ni comment configurer un Pfsense mais vous trouverez ici les configurations physiques des 4 pare-feux.

Le Firewall Admin :

```
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on FW-Admin ***

 WAN (wan)       -> vtnet0     -> v4: 10.16.2.1/24
 LAN (lan)       -> vtnet1     -> v4: 10.16.1.254/24
```

Le Firewall Interne :

```
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on FW-Interne ***

 WAN (wan)       -> vtnet0     -> v4: 10.16.10.1/24
 LAN (lan)       -> vtnet1     -> v4: 10.16.18.254/24
 OPT1 (opt1)     -> vtnet2     -> v4: 10.16.2.252/24
 OPT2 (opt2)     -> vtnet3     -> v4: 10.16.19.254/24
```

Le Firewall Intermédiaire :

```
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> vtnet0     -> v4: 10.16.21.1/24
 LAN (lan)       -> vtnet1     -> v4: 10.16.10.254/24
 OPT1 (opt1)     -> vtnet2     -> v4: 10.16.2.253/24
 OPT2 (opt2)     -> vtnet3     -> v4: 10.16.17.254/24
```

Le Firewall Externe :

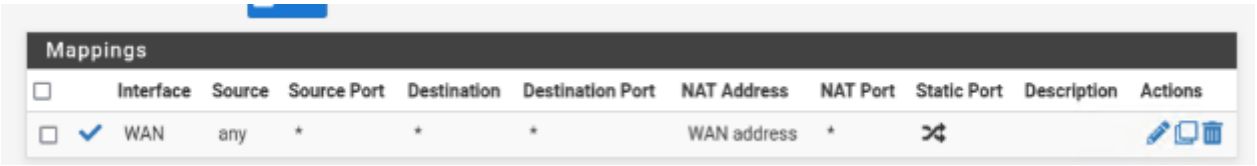
```
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on FW-Externe ***

 WAN (wan)       -> vtnet0     -> v4: 172.31.16.253/24
 LAN (lan)       -> vtnet1     -> v4: 10.16.21.254/24
 OPT1 (opt1)     -> vtnet2     -> v4: 10.16.2.254/24
```

CONFIGURATION DU PARE-FEU ADMIN

La configuration de ce pare-feu est relativement rapide.

Pas besoin de route, simplement un NAT Outbound pour avoir accès à l'extérieur :

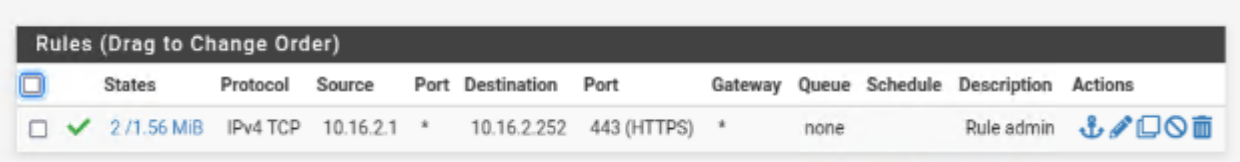


Cela suffira à donner l'accès à la machine Debian admin afin d'avoir accès aux autres firewalls.

CONFIGURATION DU PARE-FEU INTERNE

Le pare-feu interne est le deuxième à être configuré.
On commence par lui donner une route :

Ce firewall passera donc par le pare-feu intermédiaire.
Ensuite il faut autoriser l'administration du firewall via OPT1 (le LAN admin) avec une règle :



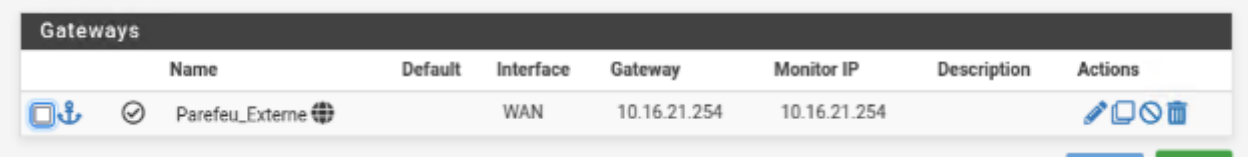
Et après une vérification de fonctionnement, il faut faire une règle d'interdiction d'accès à la configuration pour le réseau LAN :

Et la configuration est terminée.

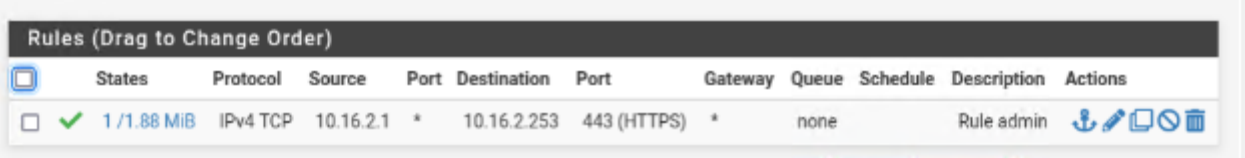
CONFIGURATION DU PARE-FEU INTERMEDIAIRE

Après l'interne, on configure le pare-feu externe.

Dans le même principe, on commence par la route :



Puis on autorise la configuration via OPT1 (Lan admin) :

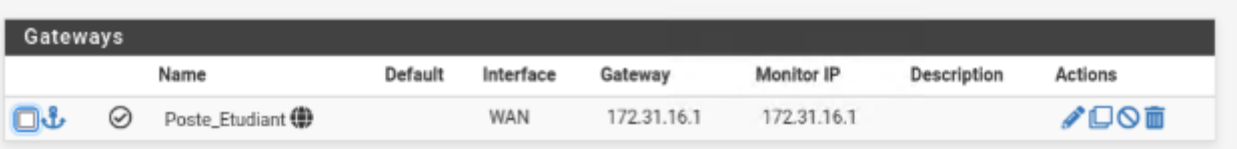


Et pour finir, l'interdiction d'accès à la config via le LAN (après vérification) :

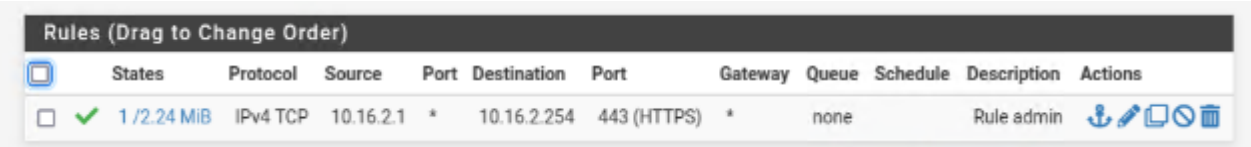
Et la configuration est terminée pour le moment.

CONFIGURATION DU PARE-FEU EXTERNE

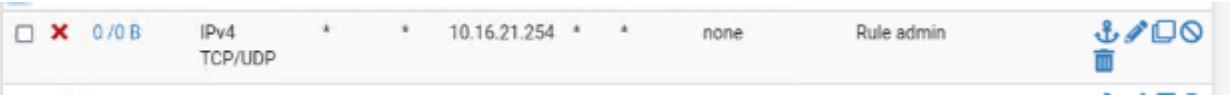
Le dernier pare-feu à être configuré est le pare-feu externe de la même façon que les autres. D'abord la route :



Puis l'autorisation de configuration pour OPT1 (Lan admin) :



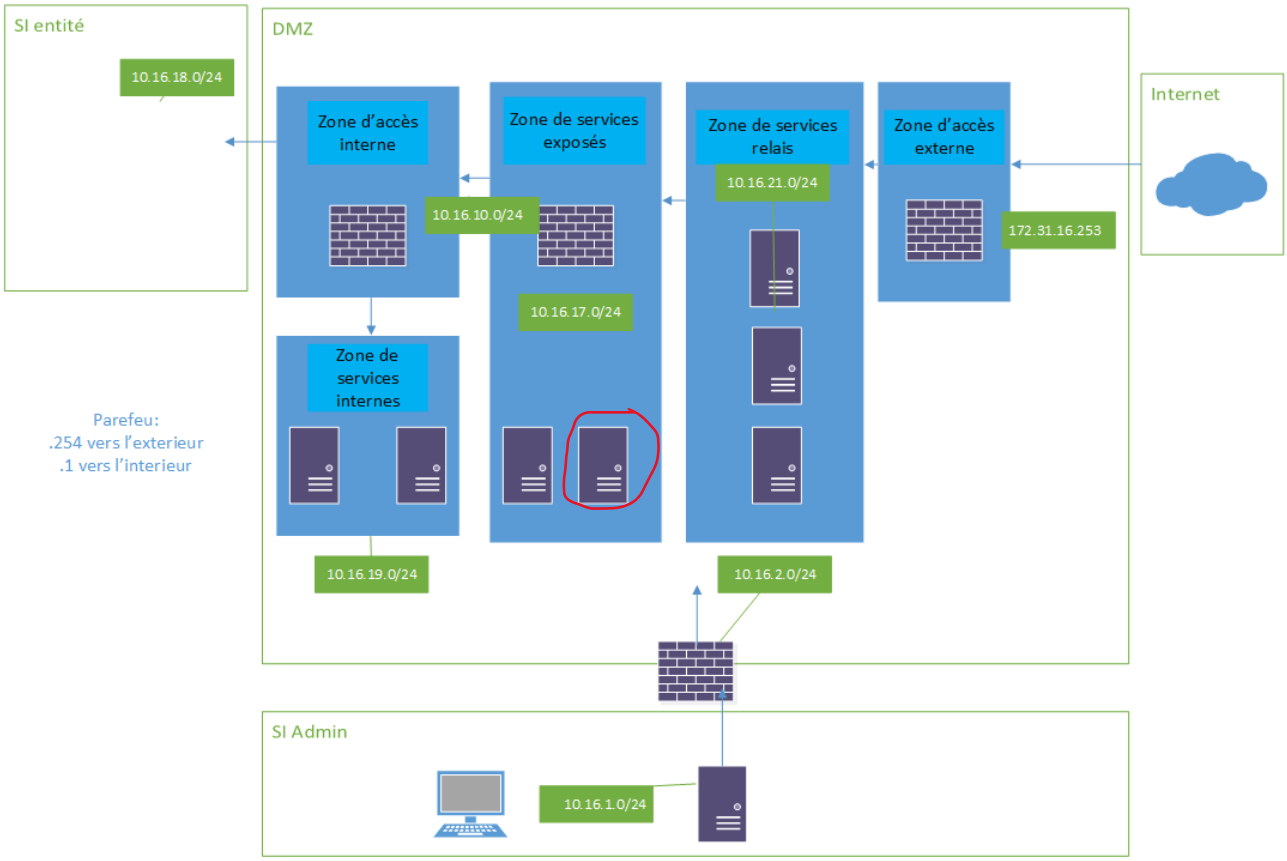
Puis la règle d'interdiction de configuration pour le LAN :



Et la configuration minimale est terminée pour l'ensemble des pare-feux

CONFIGURATION DE LA DMZ POUR UN ACCES AU SERVEUR WEB

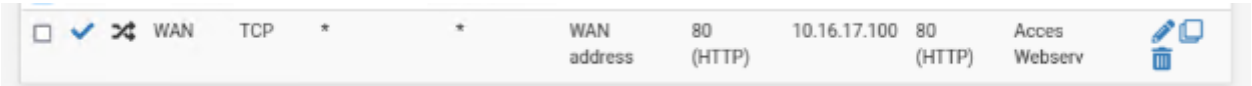
Reprenons encore une fois notre schéma réseau pour bien comprendre ce qu'il faut faire :



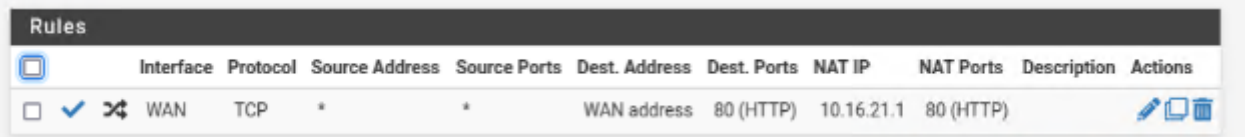
Le serveur WEB est entouré en rouge. On voit donc qu'il faut faire une redirection de port (depuis le port HTTP 80, mais on pourrait aussi ouvrir le port 443 pour l'HTTPS) depuis le firewall externe en passant par le firewall intermédiaire pour finalement avoir accès au serveur WEB depuis l'extérieur de la DMZ.

Nous passerons sur la façon de créer un serveur WEB.

Commençons par la configuration PAT du pare-feu intermédiaire (toujours de l'intérieur vers l'extérieur) :



Ensuite nous ajoutons une configuration PAT similaire sur le pare-feu externe :



Une fois cette configuration réalisée, on peut faire le test via une machine externe et voir que maintenant, le port 80 du Firewall externe amène bien au serveur WEB dans la zone de service exposé :