GSB

DMZ

Version <1.0>

Mise en place d'une DMZ

Historique des révisions

Date	Version	Description	Auteur
11/03/2016	<1.0>	Rédaction de la documentation initiale	Brice Harismendy, Julien Legrand

Table des matières

Mise en place d'une DMZ

1. Introduction

Nous allons mettre en place une DMZ permettant au personnel d'accèder au serveur GSB avec plus de sécurité. Cela passe par le rajout d'un routeur à la configuration existante qui servira de pare-feu avec notamment une ACL qui devra autorisé les ports web mais empêcher tout autre accès.

1.1 Contexte du projet

Ici, un reponsable technique GSB souhaite mettre en place une DMZ sur son réseau afin de sécuriser l'accès aux serveur nottament le service Web.

1.2 Objectifs du document

L'objectif de ce document est donc d'expliquer comment mettre en place et tester une zone démilitarisée, et d'offrir une démarche à suivre pour la mise en place.

1.3 Portée

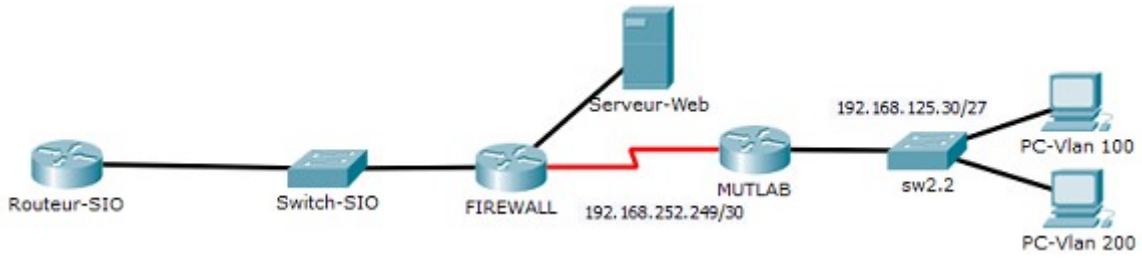
Ce document est adressé aux techniciens informatique de GSB.

1.4 Définitions, Acronymes et Abréviations

DMZ : zone démilitarisée (de l'anglais "demilitarized zone”)
ACL : "Access-List"

2. Éléments de configuration

2.1 schéma réseau



2.2 Modification du routeur MUTLAB

Nous allons modifier la configuration actuelle du routeur MUTLAB pour ajouter un autre routeur qui nous servira de pare-feu.

Voici les modifications à réaliser :

2.2.1 Déplacer l'IP du réseau de sortie sur la carte serial 0 :

```
MUTLAB(config)#no interface fastEthernet 0/1.1
MUTLAB(config)#int S0/1/0
MUTLAB(config-if)#ip address 192.168.252.249 255.255.255.252
MUTLAB(config-if)#no shutdown
MUTLAB(config)#exit
```

2.2.2 On enlève le réseau 28 de rip

```
MUTLAB(config)#router rip
MUTLAB(config-router)#version 2
MUTLAB(config-router)#no network 192.168.28.0
```

2.2.3 Ajout du nouveau réseau a la configuration rip

```
MUTLAB(config-router)#network 192.168.252.248
```

2.2.4 Changement de la route par défaut :

```
MUTLAB(config)#no ip route 0.0.0.0 0.0.0.0 192.168.28.254
```

```
MUTLAB(config)#ip route 0.0.0.0 0.0.0.0 192.168.252.250
```

2.3 Configuration du pare-feu

Nous allons maintenant configurer notre routeur avec une DMZ intégrée.

2.3.1 Configuration du nouveau routeur :

```
Router>en
Router#conf t
Router(config)#int fa0/1
Router(config-if)#no sh
Router(config)#int fa0/1.1
Router(config-subif)#encapsulation dot1Q 28
Router(config-subif)#ip address 192.168.28.253 255.255.255.0
Router(config-subif)#exit
Router(config)#int fa0/1.27
Router(config-subif)#encapsulation dot1Q 27
Router(config-subif)#ip address 192.168.27.253 255.255.255.0
Router(config-subif)#exit
```

2.3.2 Ajout de la route dans rip :

```
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#net
Router(config-router)#network 192.168.28.0
Router(config-router)#no auto-summary
Router(config-router)#end
```

2.3.3 Ajout de la route par défaut

```
Router#conf t
Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.28.254
Router(config)#end
```

2.3.4 Configuration du nom du routeur :

```
Router#conf t
Router(config)#hostname FIREWALL
```

2.3.5 Configuration de la connexion entre les deux routeurs :

```
FIREWALL(config)#int S0/1/0
FIREWALL(config-if)#ip address 192.168.252.250 255.255.255.252
FIREWALL(config-if)#no shutdown
```

```
FIREWALL(config-if)#exit
```

2.3.6 Ajout du réseau a rip :

```
FIREWALL(config)#router rip
FIREWALL(config-router)#version 2
FIREWALL(config-router)#network 192.168.252.248
FIREWALL(config-router)#network 192.168.27.0
FIREWALL(config-router)#network 192.168.28.0
FIREWALL(config-router)#end
```

2.3.7 Ajout du nouveau réseau :

2.3.7.1 Configuration de l'accès au routeur en TELNET :

```
FIREWALL(config)#line vty 0 4
FIREWALL(config-line)#transport input telnet
FIREWALL(config-line)#password P@ssw0rd
FIREWALL(config-line)#login local
FIREWALL(config-line)#exit
FIREWALL(config)#service password-encryption
FIREWALL(config)#enable secret P@ssw0rd
FIREWALL(config)#end
```

2.3.7.2 Configuration du NAT :

```
FIREWALL(config)#access-list 1 permit 192.168.125.0 192.255.255.255
```
(on regroupe ici tout les réseaux 125.0/27)
```
FIREWALL(config)#ip nat inside source list 1 interface fa0/1.1 overload
FIREWALL(config)#int fa0/1.1
FIREWALL(config-subif)#ip nat inside
FIREWALL(config-subif)#end
```

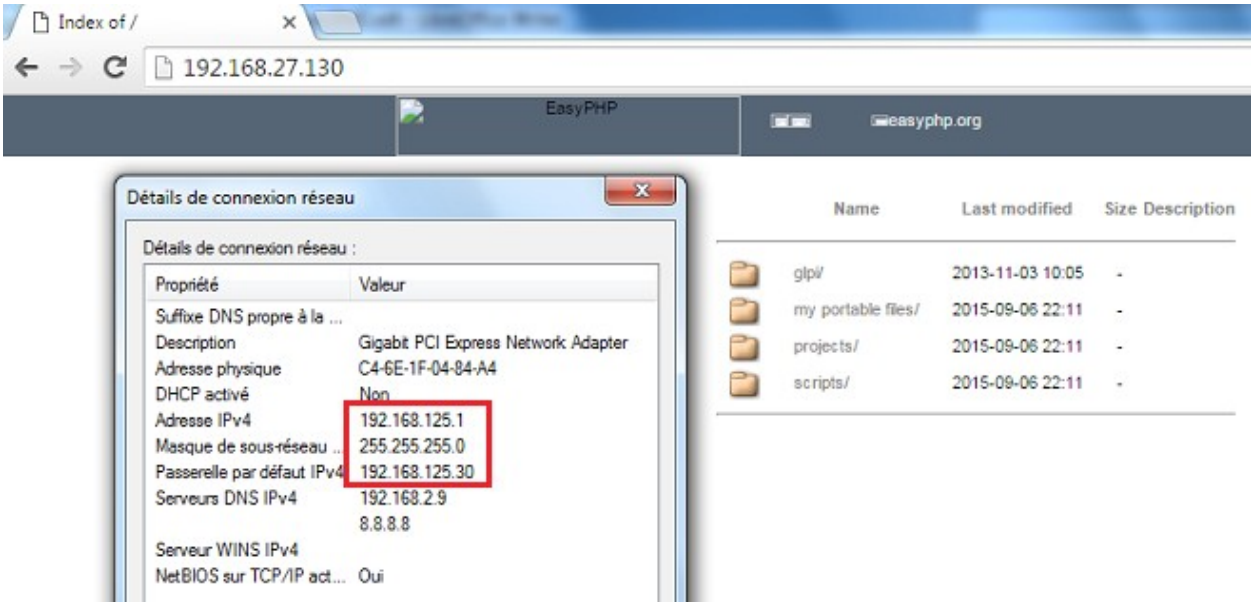
2.3.8 Configuration de la DMZ

(les ";" servent à mieux distinguer les adresses, à ne pas entrer)
```
FIREWALL(config)#access-list 100 permit 80 192.168.125.0 ; 0.0.0.31
192.168.27.0 ; 0.0.0.255
FIREWALL(config)#access-list 100 permit 80 192.168.125.32 ; 0.0.0.31
192.168.27.0 ; 0.0.0.255
FIREWALL(config)#access-list 100 permit tcp 192.168.125.0 ; 0.0.0.31
192.168.27.0 ; 0.0.0.255 eq 443
FIREWALL(config)#access-list 100 permit tcp 192.168.125.32 ; 0.0.0.31
192.168.27.0 ; 0.0.0.255 eq 443
FIREWALL(config)#access-list 100 deny any any
FIREWALL(config)#end
FIREWALL(config)#int fa0/1.27
FIREWALL(config-if)#ip access-group 100 in
```

Nous avons ouvert les ports 80 et 443 pour n'autoriser que le service Web.

3. Tests / Validations

Nous arrivons donc bien à accéder à la page web depuis un PC dans les vlans 100 et 200. Mais on ne peut pas accéder à cette page web depuis un autre réseau, de plus, tout les autres services sont désactivés.



4. Conclusion

Pour conclure, la DMZ permet de sécuriser l'accès au site web GSB, en autorisant uniquement les vlans 100 et 200 à y accéder. Le problème ou la limite de cette configuration est le coûts d'un routeur supplémentaire, mais aussi la connection est de ce fait dépendante de deux routeurs. On pourrait éventuellement installer une solution moins coûteuse comme l'ajout d'une interface réseau au routeur existant, ou bien utiliser un serveur PfSense.