TP Sécurité des réseaux

BRIZAI Olivier
THORAVAL Maxime

27 janvier 2011

Table des matières

1 Introduction **3**

2 Installation **4**

3 Configuration Inside **5**

3.1 Configuration du NAT 5

3.2 Règles de filtrage 6

4 Configuration DMZ **12**

4.1 Installation 12

4.2 Règles de filtrage 13

1 Introduction

Le but de ce TP est de mettre en place un réseau sécurisé à l'aide d'un firewall CISCO ASA.
Ci-dessous, le réseau que nous souhaitons obtenir (les règles de filtrage ne sont pas représentées).

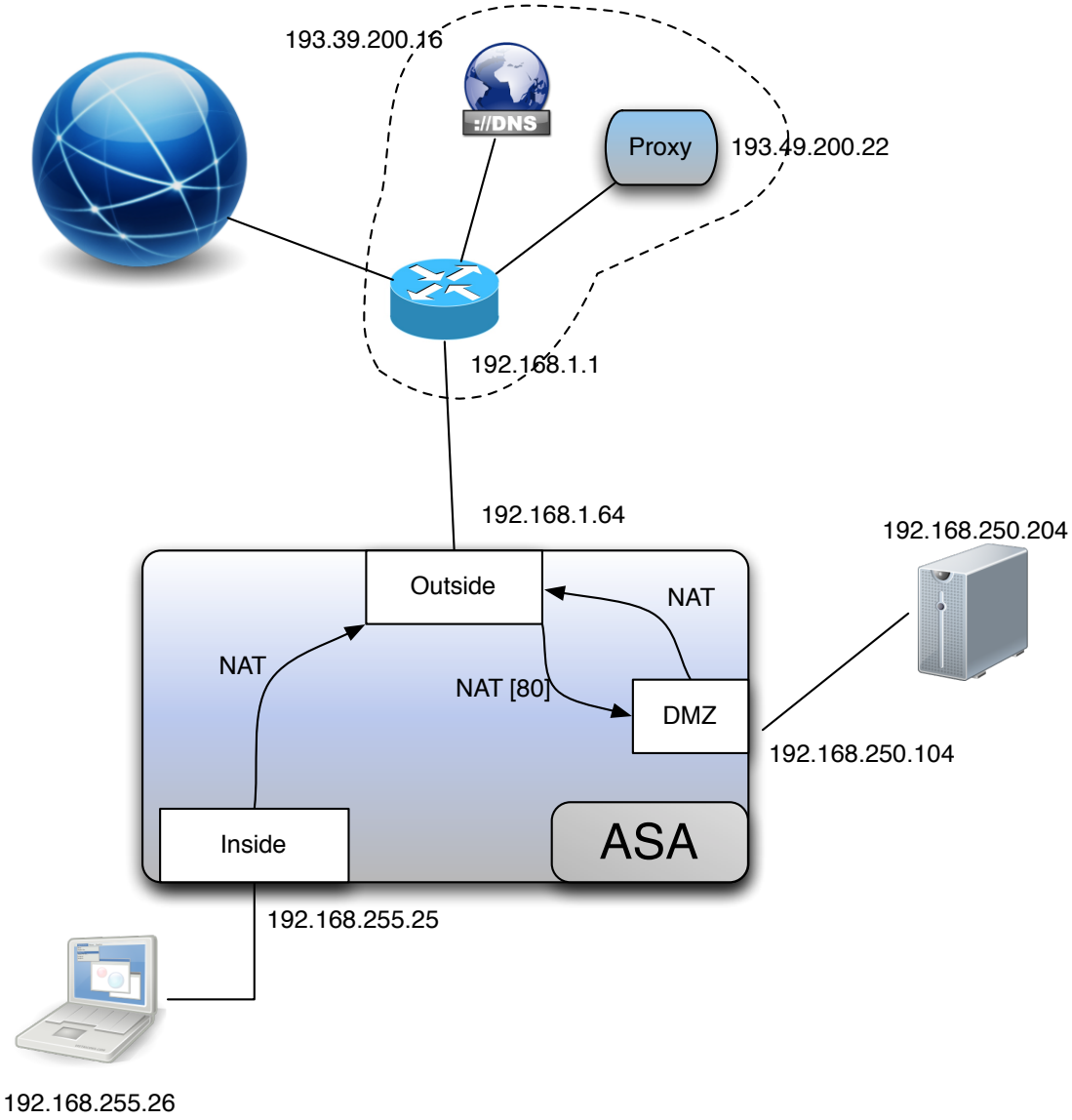

FIGURE 1 – Réseau à obtenir

2 Installation

Dans un premier temps, nous avons installé Ubuntu 9.04 (version client) sur notre PC. Celle-ci effectuée, nous réalisons les démarches suivantes, c'est à dire mise en place de Java ainsi que l'installation du paquet « Minicom ».

Nous lançons ensuite la commande **minicom -s** et définissons les divers paramètres afin de configurer le port console. Puis, nous définissons l'adresse *inside* de l'ASA. Nous pouvons maintenant, à partir de celle-ci, accéder à l'interface d'administration de l'ASA au sein de notre navigateur.
La figure ci-dessous présente l'accueil de celle-ci.

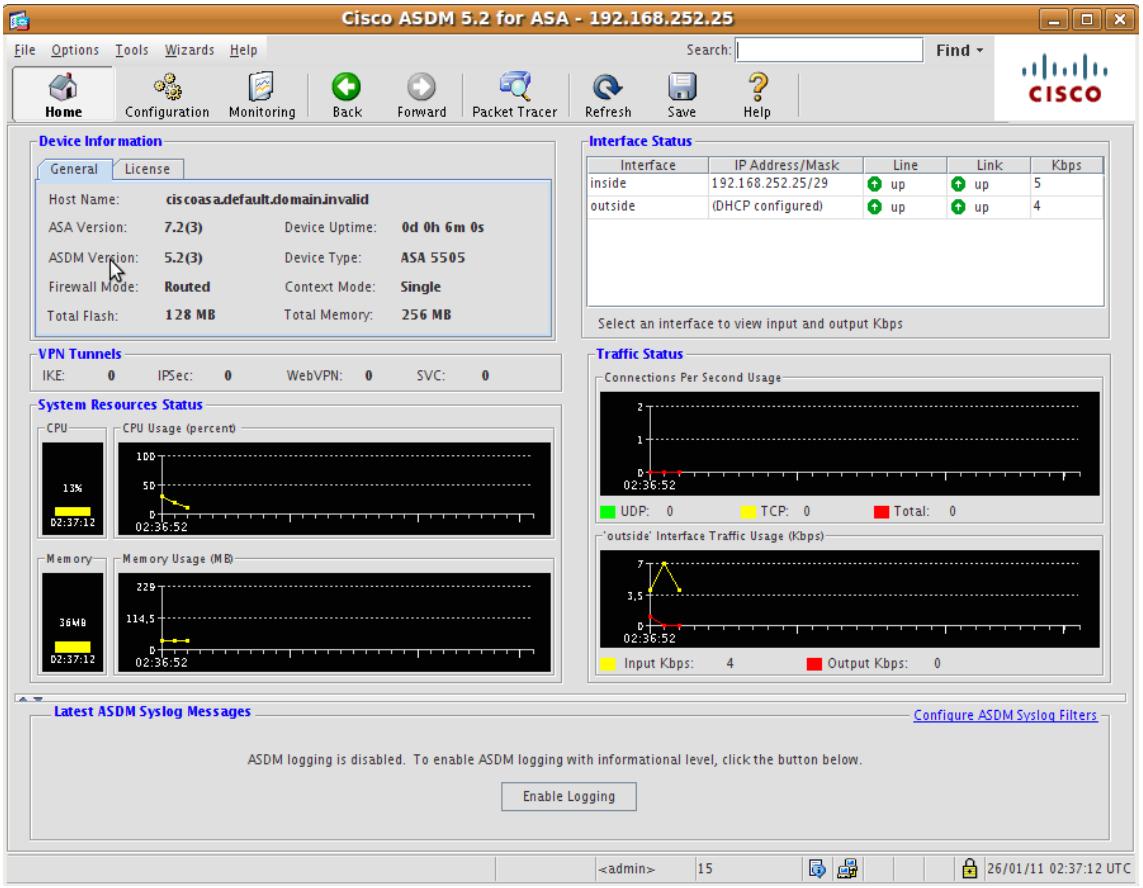

FIGURE 2 – Interface de configuration

Nous avons ensuite utilisé le « Wizard »de l'application pour mettre en place un certain nombres de paramètres tel que adresses IP (inside, outside, dmz) ou encore la répartition des interfaces du firewall (cf. figure ci-dessous).

Name	Switch Ports	Security Level	IP Address	Subnet Mask	VLAN
inside	Ethernet0/1, Ethernet0/2, Ethernet0/3, Ethernet0/4, Ethernet0/5, Ethernet0/6	100	192.168.252.25	255.255.255.248	vlan1
outside	Ethernet0/0	0	192.168.1.64	255.255.255.0	vlan2
dmz	Ethernet0/7	50	192.168.250.104	255.255.255.0	vlan3

FIGURE 3 – Configuration des interfaces

3 Configuration Inside

Dans cette partie, nous avons configuré notre firewall afin de permettre certaines actions à l'interface *inside*.

3.1 Configuration du NAT

Dans un premier temps, il nous a fallu configurer une règle de NAT afin de traduire l'adresse privée de l'interface *inside* en l'adresse publique de l'interface *outside*. Nous devons effectuer cette étape car il a été défini que les adresses privé (type 192.168.x.x) ne sont pas visibles sur internet. Ceci est dû au fait que nous arrivons à pénurie des adresse IPv4.
Ci-dessous, la configuration de notre NAT, pour le sous-réseau de lié à notre interface *inside* (192.168.252.24), nous lions l'adresse de l'interface *outside*.

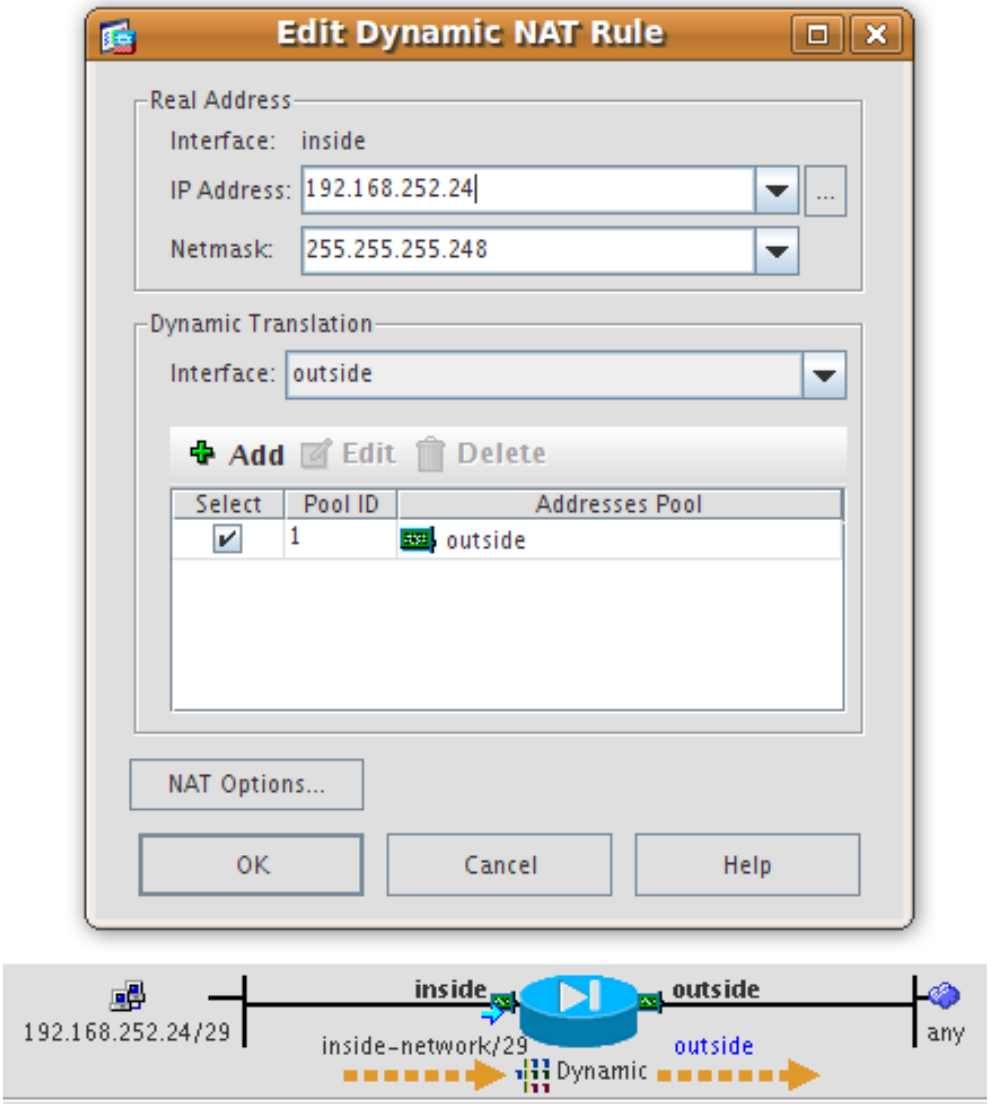

FIGURE 4 – Configuration du NAT

3.2 Règles de filtrage

Notre NAT crée, nous allons maintenant mettre en place des règles de filtrage afin de ne laisser passer que les paquets liés à des servies définis.

Dans un premier temps, nous autorisations les flux TCP et UDP sur le port 53 (DOMAIN) qui sont à destination de 193.49.200.16 (adresse du serveur DNS de l'ENSICAEN).
Ci-dessous ces deux règles.

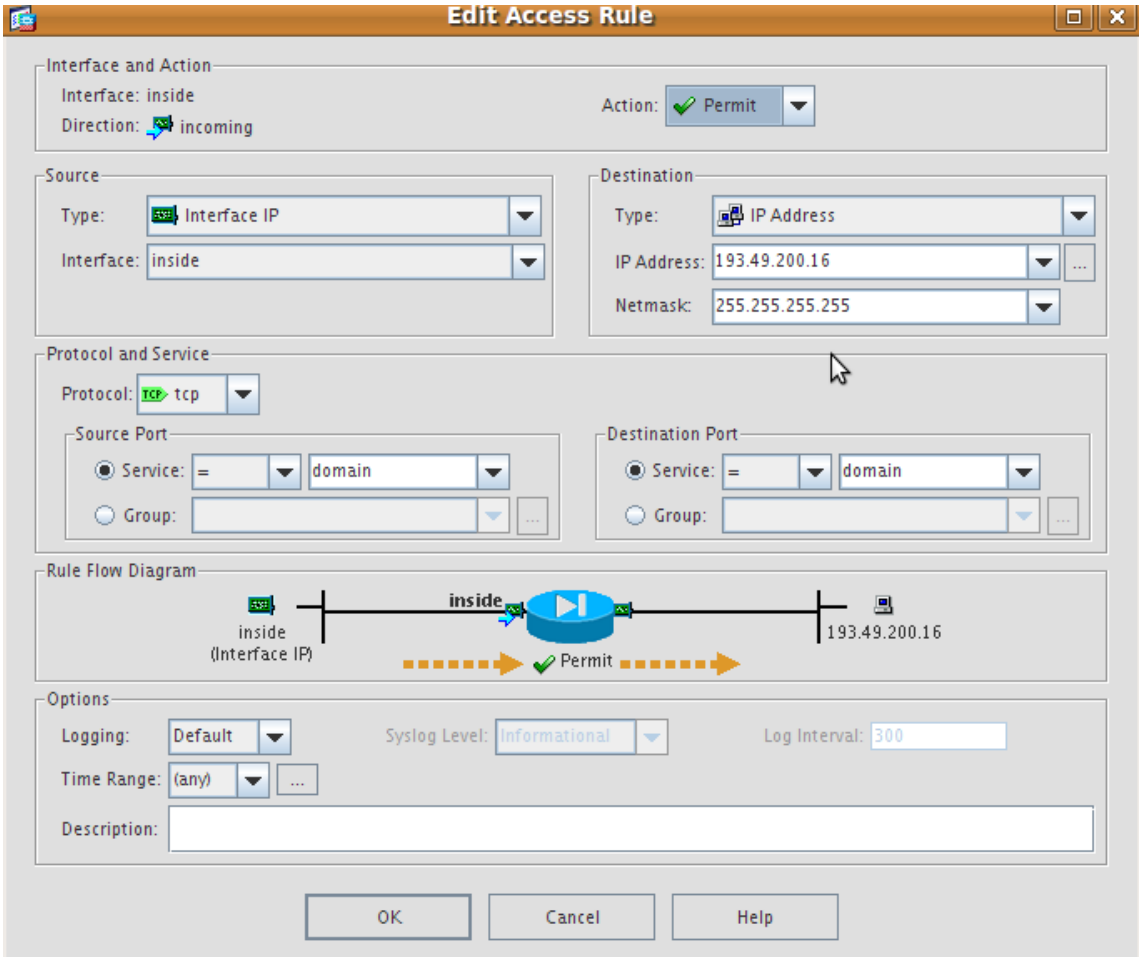

FIGURE 5 – Règle 1 : TCP DOMAIN

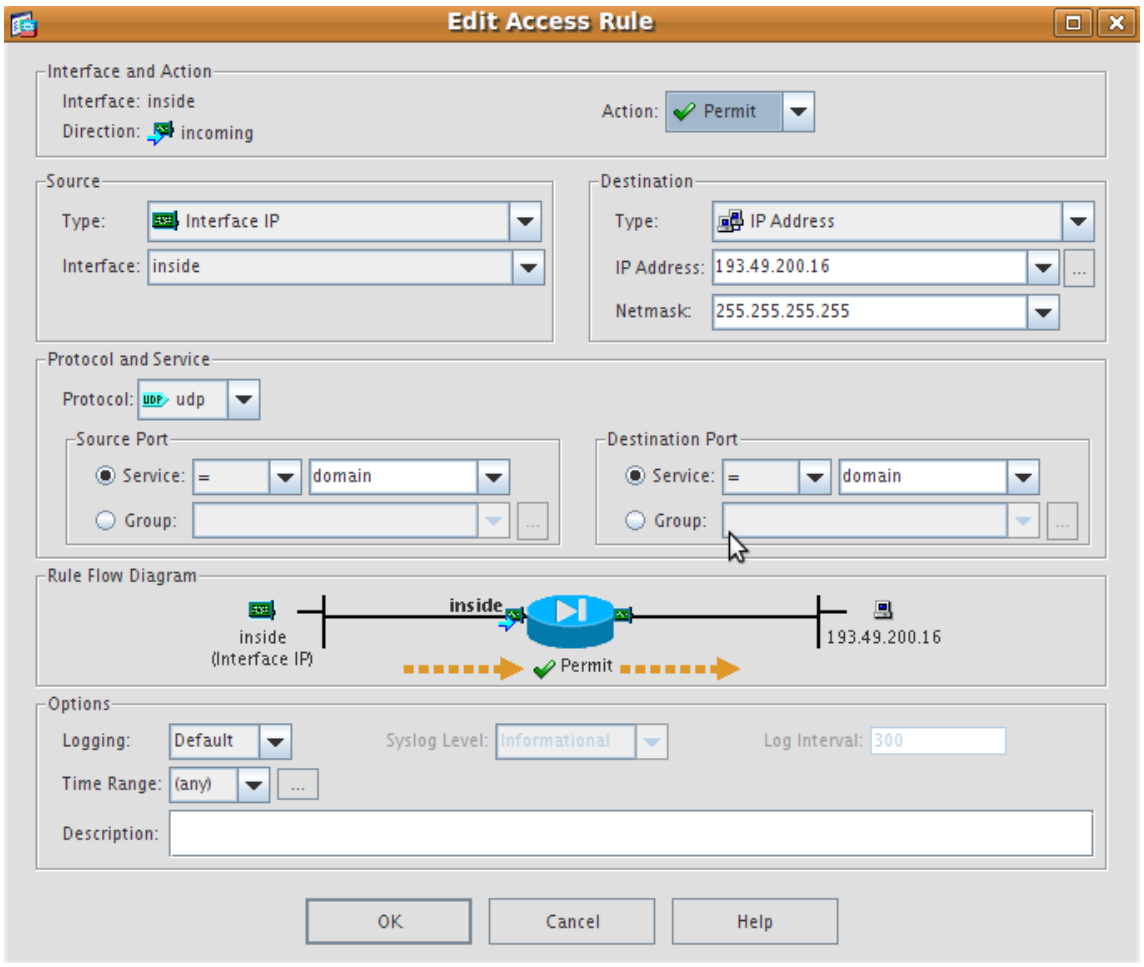

FIGURE 6 – Règle 1 : UDP DOMAIN

Maintenant, nous créons la règle autorisant le flux SSH (TCP sur le port 22) qu'importe le destinataire.

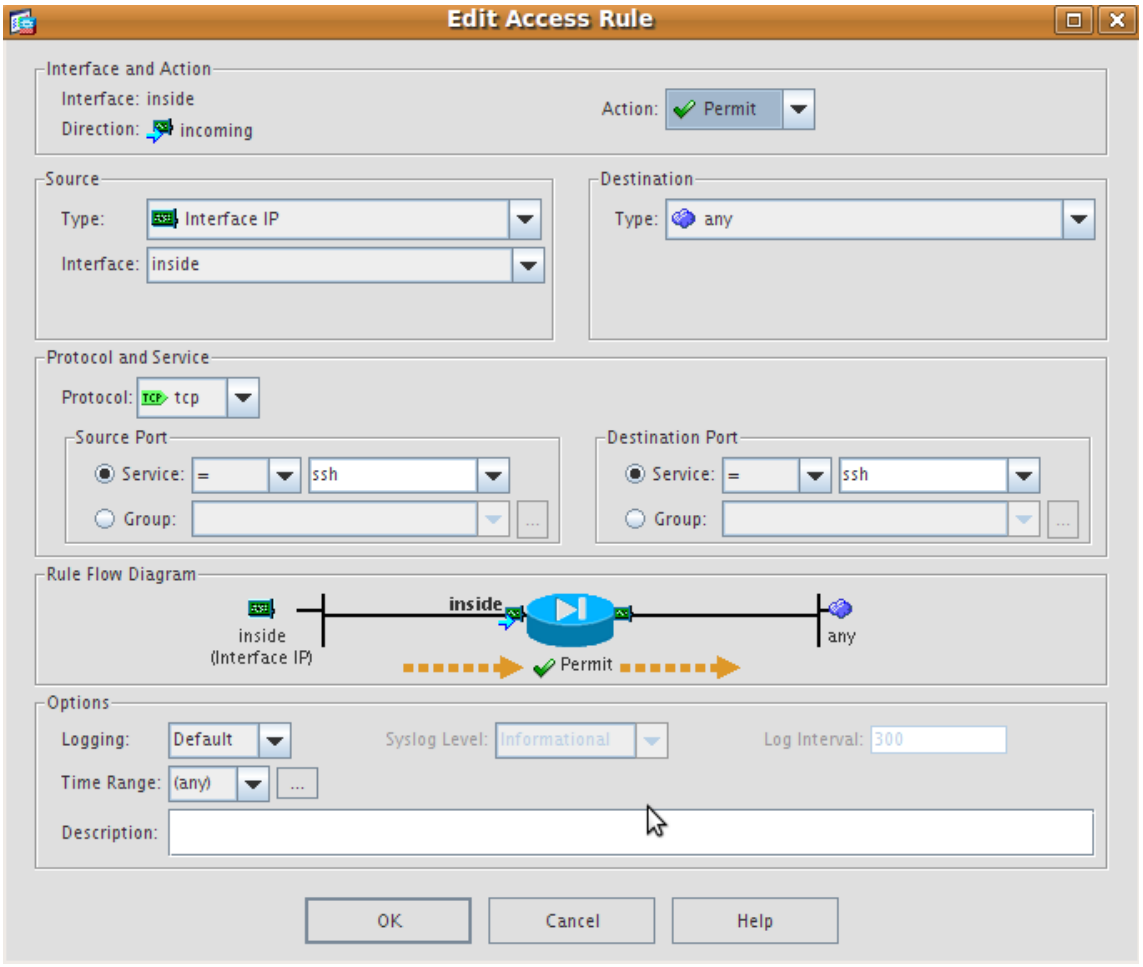

FIGURE 7 – Règle 2 : SSH

Puis la règle autorisant le flux HTTP (TCP sur le port 80) à destination de 193.49.200.22 (adresse du proxy de l'ENSICAEN).

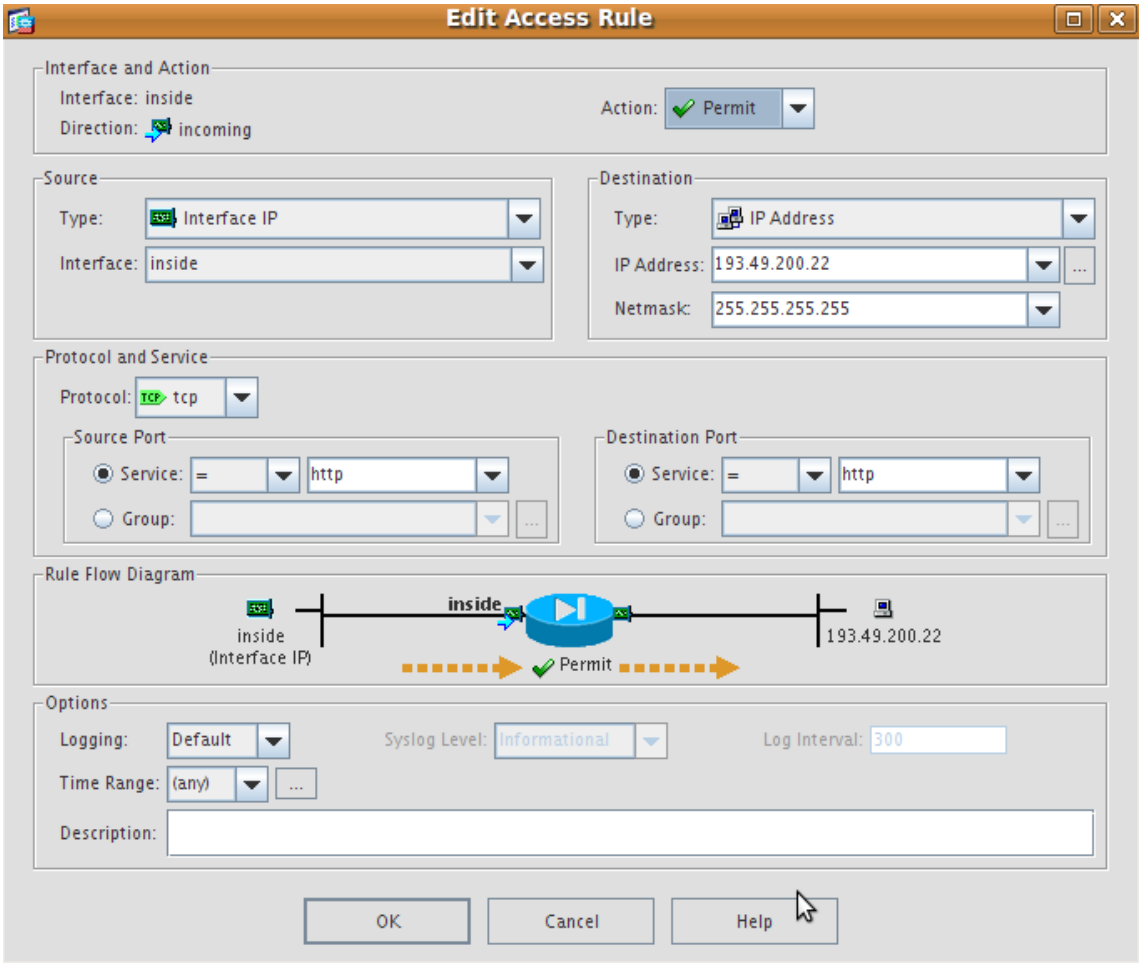

FIGURE 8 – Règle 3 : HTTP

Enfin, nous autorisons le flux à destination d'un proxy (TCP sur le port 3128 = port du proxy de l'école). Bien entendu, nous nous restreignons une nouvelles fois à l'adresse du proxy de l'ENSICAEN.

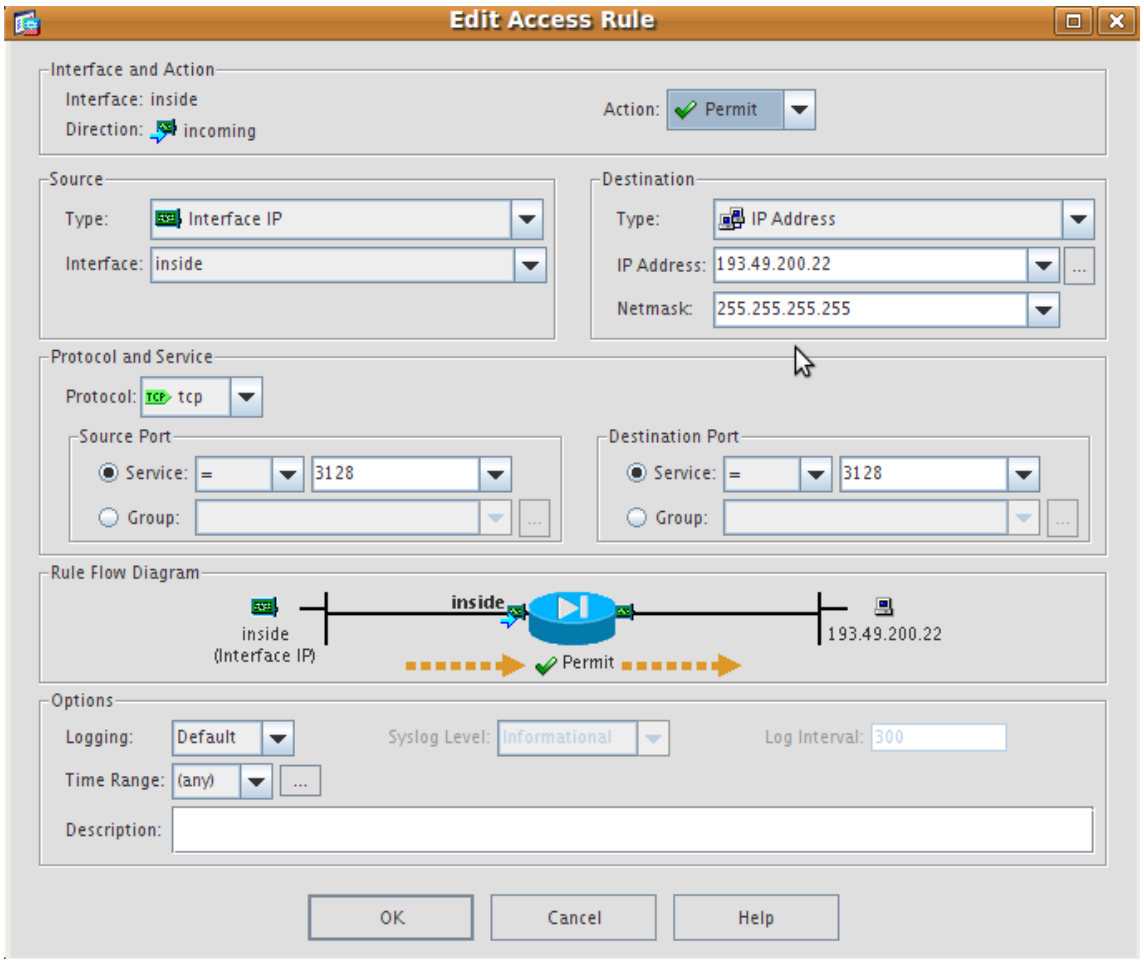

FIGURE 9 – Règle 4 : Proxy

Nous sommes maintenant censé pouvoir accéder au routeur de l'école (adresse 192.168.1.1). Pour le vérifier, nous lançons la commande **ping** sur son adresse. On remarque que nous n'avons pas de retour de cette commande. Afin de vérifier l'erreur, nous allons regarder le *monitoring* de notre firewall. Ceci va nous permettre de suivre son activité. Après analyse des traces, nous avons pu comprendre l'échec de la commande **ping**. En effet, elles nous informent que les paquets de type ICMP ne sont pas autorisés à destination de l'interface *inside*. Afin de résoudre ce problème, nous devons rajouter une nouvelle règle de filtrage que nous avons défini de la manière ci-dessous.

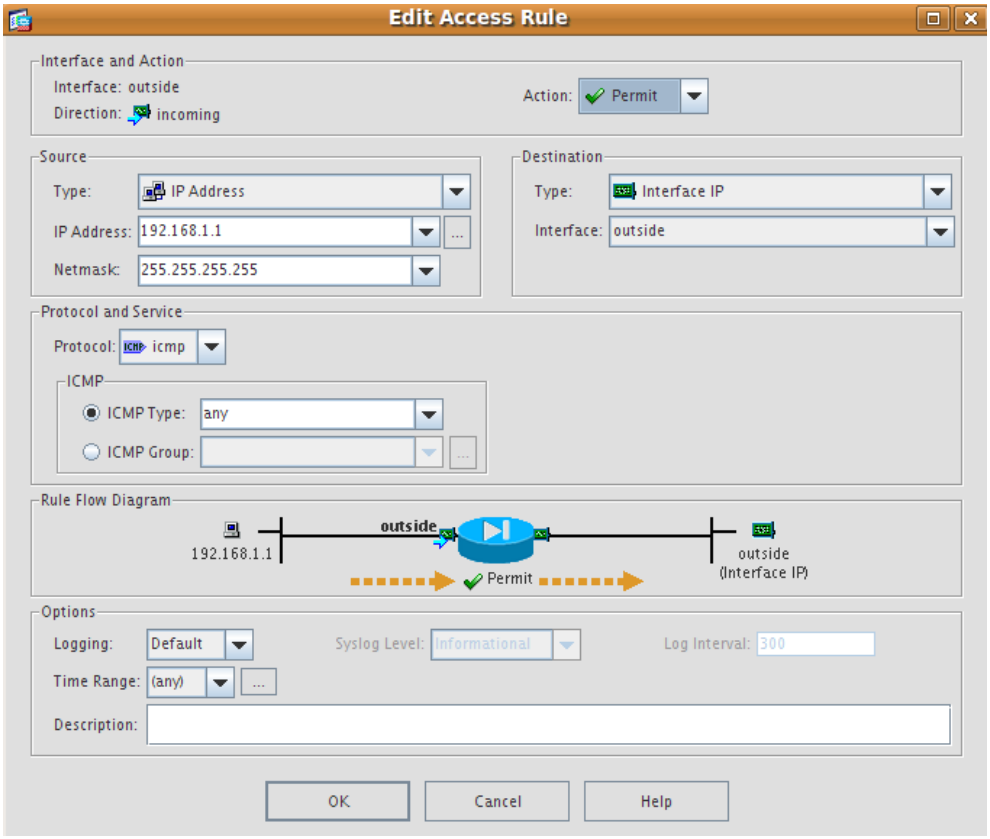

FIGURE 10 – Filtrage ICMP pour autoriser le retour de ping

Cette règle mise en place, nous lançons une nouvelles fois la commande **ping**. Comme visible sur la figure ci-dessous, il n'y a plus d'échec.

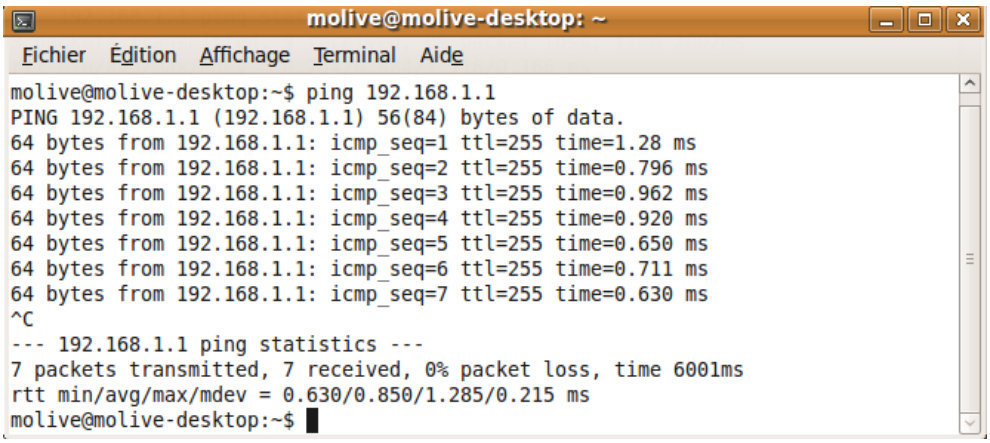

FIGURE 11 – Résultat ping

4 Configuration DMZ

4.1 Installation

Nous souhaitons maintenant configurer la DMZ. Dans un premier temps, nous installons « Ubuntu 9.0.4 server » sur le PC relié à l'interface DMZ du firewall. Lors de l'installation, nous indiquons que nous souhaitons avoir par défaut les services suivants : un serveur SSH et un serveur web (LAMP).

L'installation terminée, nous allons maintenant configurer les informations réseau de notre serveur. Nous renseignons son adresse IP (192.168.250.204), le masque associé et enfin le routeur (ici il s'agit de l'adresse de l'interface *dmz* de notre firewall).
Afin de mettre en place ces informations, nous allons modifier le fichier */etc/network/interfaces* de la sorte :

```
1 auto eth0
2 iface eth0 inet static
3     address 192.168.250.204
4     netmask 255.255.255.0
5     gateway 192.168.250.104
```

4.2 Règles de filtrage

Comme pour notre interface *inside*, nous allons devoir indiquer un certain nombre de règles de filtrage pour autoriser différents service.

Dans un premier temps, nous souhaitons que toutes les requêtes HTTP provenant de l'interface *inside* à destination de la *dmz* puissent être transmises. Ci-dessous, la règle liée.

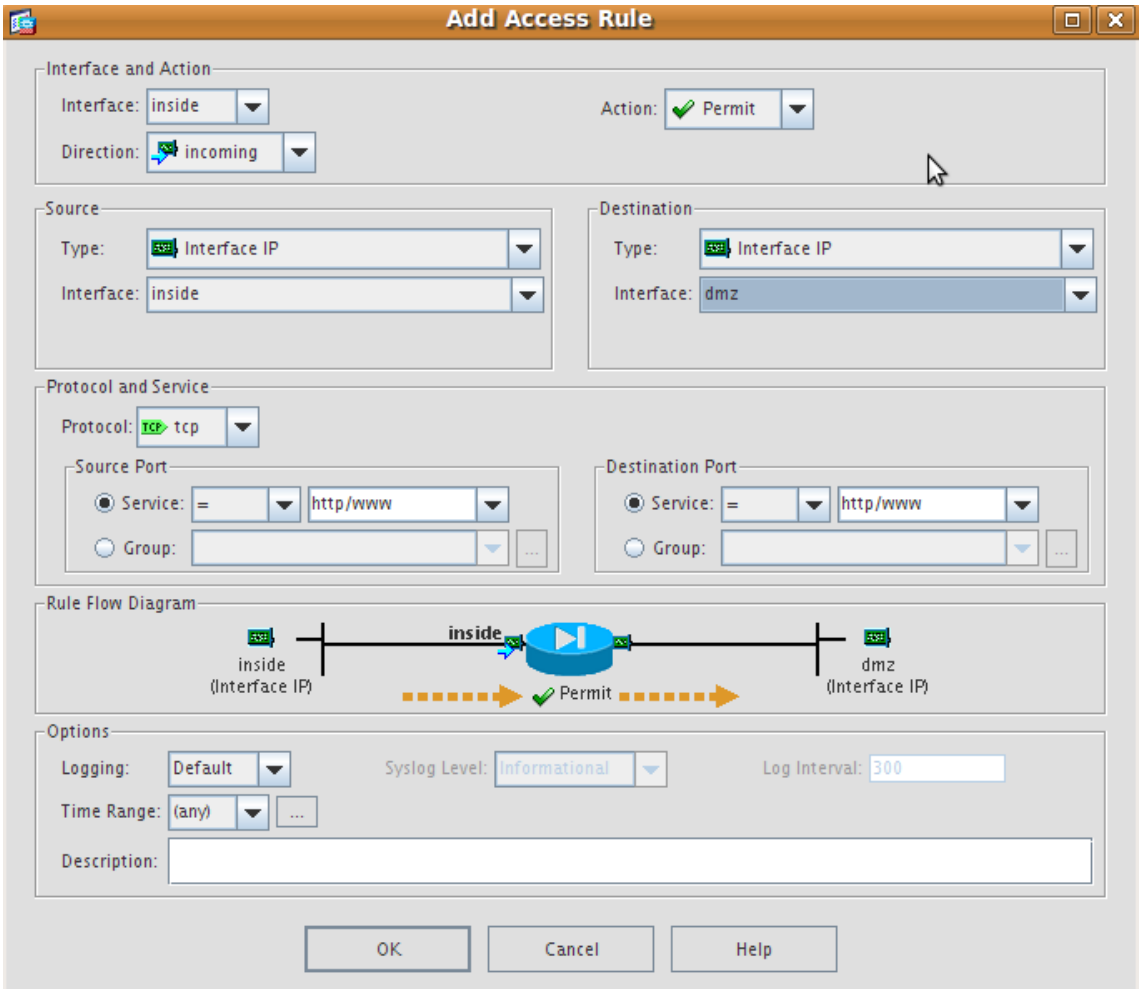

FIGURE 12 – Règle 1 : HTTP inside vers dmz

Nous souhaitons aussi que les requêtes HTTP externes puissent être reçu par la *dmz*, dans ce cas, nous devons définir une nouvelle règle autorisant ces flux entre l'interface *outside* et la *dmz*.

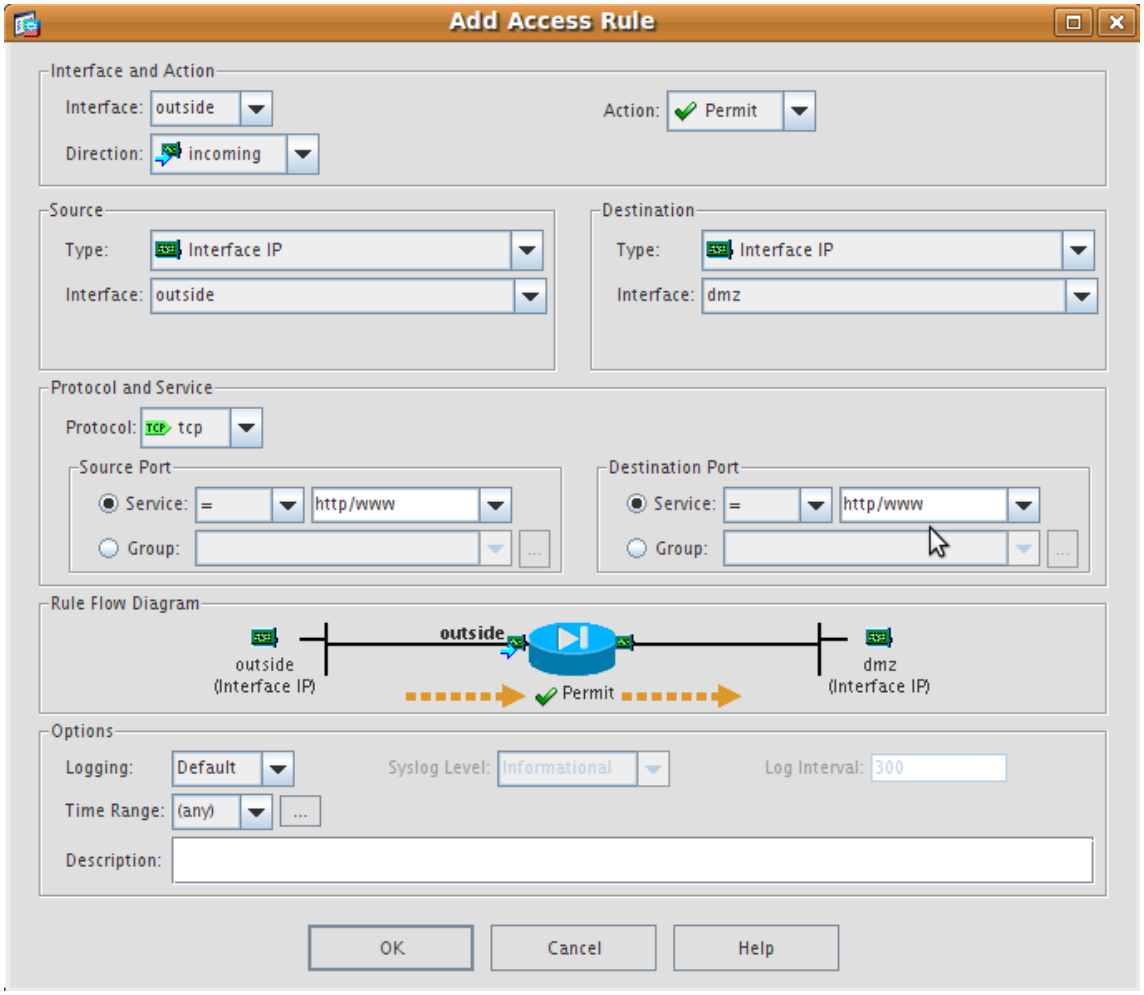

FIGURE 13 – Règle 1 : HTTP outside vers dmz

Enfin, nous faisons de même pour les requêtes SSH.

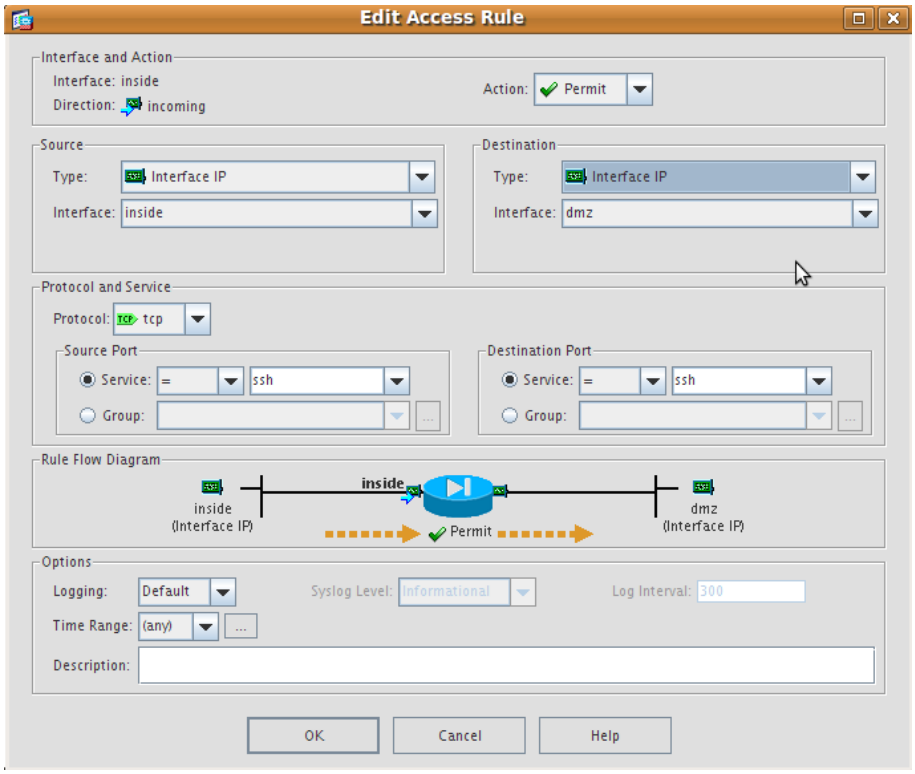

FIGURE 14 – Règle 2 : SSH inside vers dmz

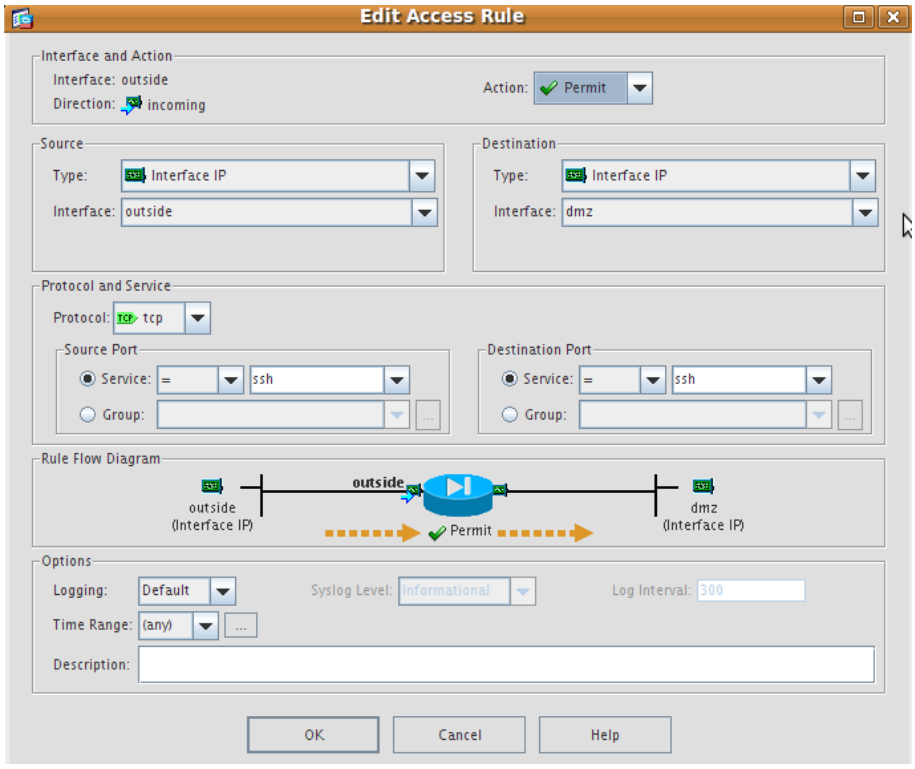

FIGURE 15 – Règle 2 : SSH outside vers dmz