POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

INF8402
Sécurité des réseaux fixes et mobiles
Groupe 1

Lab3 – Configuration du pare feu par ligne de commandes

Soumis à : [redacted]

[redacted]

Le 18 novembre 2024

Table des matières

Note : pour toutes les manipulations nous sauvegarderons uniquement à la fin du laboratoire avec la commande : ***write memory*** et nous assumons également que nous serons en mode config tout le long pas besoin de faire à chaque fois ***configure terminal***

Q1) Quelle est la commande qui permet de fixer le niveau de sécurité de l'interface INSIDE à 100? (1 point)

La commande **security-level 100** permet de fixer le niveau de l'interface sélectionnée à 100

On entre en mode configuration, on sélectionne l'interface et on fait la commande

```
POLYFW01# configure terminal
POLYFW01(config)# int GigabitEthernet0
POLYFW01(config-if)# security-level 100
```

Figure 1.1 : Configuration du niveau de sécurité de l'interface INSIDE

```
POLYFW01(config-if)# sh running-confi int GigabitEthernet0
!
interface GigabitEthernet0
 nameif INSIDE
 security-level 100
 ip address 192.168.199.5 255.255.255.0
```

GigabitEthernet0	INSIDE	Enabled	100	192.168.199.5	255.255.255.0	H

Figure 1.2 : Preuve que la configuration est appliquée

Q2) Quelle(s) commande(s) permet(tent) de configurer l'interface GigabitEthernet2 telles que présentée dans le tableau 1? (2 points)

Les commandes suivantes permettent de réaliser les actions demandées : la première permet de sélectionner l'interface à configurer, la seconde définie la plage d'adresse de l'interface et la dernière le niveau de sécurité

```
POLYFW01(config-if)# int GigabitEthernet2
POLYFW01(config-if)# ip address 192.168.226.5 255.255.255.0
POLYFW01(config-if)# security-level 0
```

Figure 2.1 : Configuration de l'interface 2

```
POLYFW01(config-if)# sh running-confi int GigabitEthernet2
!
interface GigabitEthernet2
 shutdown
 no nameif
 security-level 0
 ip address 192.168.226.5 255.255.255.0
```

GigabitEthernet2		Disabled	0	192.168.226.5	255.255.255.0

Figure 2.2 : Preuve de la configuration

Q3) Il est possible de constater que l'interface GigabitEthernet2 ne possède pas de nom. Quelle commande permet de nommer l'interface GigabitEthernet2 à OUTSIDE? (1.5 points)

Étant donné que l'interface a déjà été sélectionner à la question 2, pour nommer l'interface il faut faire la commande

```
POLYFW01(config-if)# nameif OUTSIDE
```

Figure 3.1 : Nommer l'interface 2

```
POLYFW01(config-if)# sh running-confi int GigabitEthernet2
!
interface GigabitEthernet2
 shutdown
 nameif OUTSIDE
 security-level 0
 ip address 192.168.226.5 255.255.255.0
```

GigabitEthernet2	OUTSIDE	Disabled	0	192.168.226.5	255.255.255.0

Figure 3.2 : Preuve que l'interface est bien nommée

Q4) Encore sur ASDM, il est possible de constater que l'interface GigabitEthernet2 n'est pas activée. Quelle commande permet d'activer cette interface? (2 points)

Étant donné que l'interface a déjà été sélectionner à la question 2, pour activer l'interface il faut faire la commande :

```
POLYFW01(config-if)# no shutdown
```

Figure 4.1 : Commande pour activer interface

```
POLYFW01(config-if)# sh running-confi int GigabitEthernet2
!
interface GigabitEthernet2
 nameif OUTSIDE
 security-level 0
 ip address 192.168.226.5 255.255.255.0
```

GigabitEthernet2	OUTSIDE	Enabled	0	192.168.226.5	255.255.255.0

Figure 4.2 : Preuve que l'interface est active

```
POLYFW01(config-if)# int GigabitEthernet1
POLYFW01(config-if)# ip address 192.168.126.5 255.255.255.0
POLYFW01(config-if)# security-level 50
POLYFW01(config-if)# nameif DMZ
POLYFW01(config-if)# no shutdown
POLYFW01(config-if)# sh running-confi int GigabitEthernet1
```

Figure 4.3 : Configuration DMZ

```
POLYFW01(config-if)# sh running-confi int GigabitEthernet1
!
interface GigabitEthernet1
 nameif DMZ
 security-level 50
 ip address 192.168.126.5 255.255.255.0
```

GigabitEthernet1	DMZ	Enabled	50	192.168.126.5	255.255.255.0

Figure 4.4 : Preuve configuration DMZ

Q5) Quelle(s) commande(s) permet(tent) de créer un NAT pour permettre à tous les utilisateurs des réseaux « INSIDE » d'aller vers internet. (2 points)

Pour faire la règle NAT, on commence par créer un objet pour les adresses source à translater, ensuite on attribue un sous réseau à l'objet et enfin on crée la règle avec la commande nat

```
POLYFW01(config)# object network INSIDE-NET
POLYFW01(config-network-object)# subnet 192.168.199.0 255.255.255.0
POLYFW01(config-network-object)# nat (INSIDE,OUTSIDE) dynamic interface
```

Figure 5.1 : Crée la règle NAT

```
POLYFW01(config-network-object)# sh nat

Auto NAT Policies (Section 2)
1 (INSIDE) to (OUTSIDE) source dynamic INSIDE-NET interface
    translate_hits = 29, untranslate_hits = 0
```

"Network Object" NAT (Rule 1)					
1	INSIDE	OUTSIDE	INSIDE-NET	any	any

Figure 5.2 : Preuve que la règle est bien créée

Q6) Quelle commande permet d'ajouter une route statique? (1.5 points) N'oubliez pas de préciser ces paramètres dans votre commande : « OUTSIDE », IP Address « 0.0.0.0 » (Any), Netmask « 0.0.0.0 », Gateway IP « serveur WINS de l'interface VMnet8 ».

Pour créer cette route statique, on utilise la commande route en précisant l'interface de destination les ip source, le masque et enfin l'ip de la passerelle

```
POLYFW01(config)# route OUTSIDE 0.0.0.0 0.0.0.0 192.168.142.2
```

Figure 6.1 : Création d'une route statique

En faisant la commande sh route on obtient :

```
S*    0.0.0.0 0.0.0.0 [1/0] via 192.168.142.2, OUTSIDE
```

OUTSIDE	0.0.0.0	0.0.0.0	192.168.142.2	1	None

Figure 6.2 : Preuve que la route a bien été créée

Q7) À ce stade, vous devriez avoir internet sur la machine window 10. De la même façon, donnez accès à internet à la machine Metasploit. Vous devez expliciter toutes les commandes à l'aide de captures d'écran. Montrez que vous avez accès à Internet en utilisant l'outil curl.

a) Quelle configuration statique avez-vous utilisé? Vous pouvez présenter la configuration que vous avez utilisez dans le fichier /etc/network/interfaces (2 points)

Sur la machine Metasploit j'ai fait la commande ***sudo nano etc/network/interfaces*** pour modifier l'ip en statique et le résultat est le suivant

```
auto eth0
        #iface eth0 inet dhcp
        iface eth0 inet static
                address 192.168.126.100
                netmask 255.255.255.0
                gateway 192.168.126.5
```

J'ai également modifié le dns avec la commande ***sudo nano etc/resolv.conf***

```
search localdomain
nameserver 192.168.28.2
nameserver 8.8.8.8
nameserver 8.8.4.4
```

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:9f:76:fa
          inet addr:192.168.126.100  Bcast:192.168.126.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe9f:76fa/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:107 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:14224 (13.8 KB)
          Interrupt:17 Base address:0x2000
```

Figure 7.1 : Configuration réseau de la machine Metasploit

b) Quelle commande NAT permet à tous les utilisateurs du réseau « DMZ» d'aller vers internet? (2 points)

Pour aller sur internet depuis DMZ on suit la même démarche que pour INSIDE on crée un objet network et on crée la ègle NAT comme suit :

```
POLYFW01# configure terminal
POLYFW01(config)# object network DMZ-NET
POLYFW01(config-network-object)# subnet 192.168.126.0 255.255.255.0
POLYFW01(config-network-object)# nat (DMZ,OUTSIDE) dynamic interface
```

Figure 7.2 : Configuration de la règle NAT pour DMZ

Note la configuration du réseau DMZ a été faite plus haut à la question 4

Validons maintenant que nous avons bien accès à internet à partir des machines Windows et Metasploit

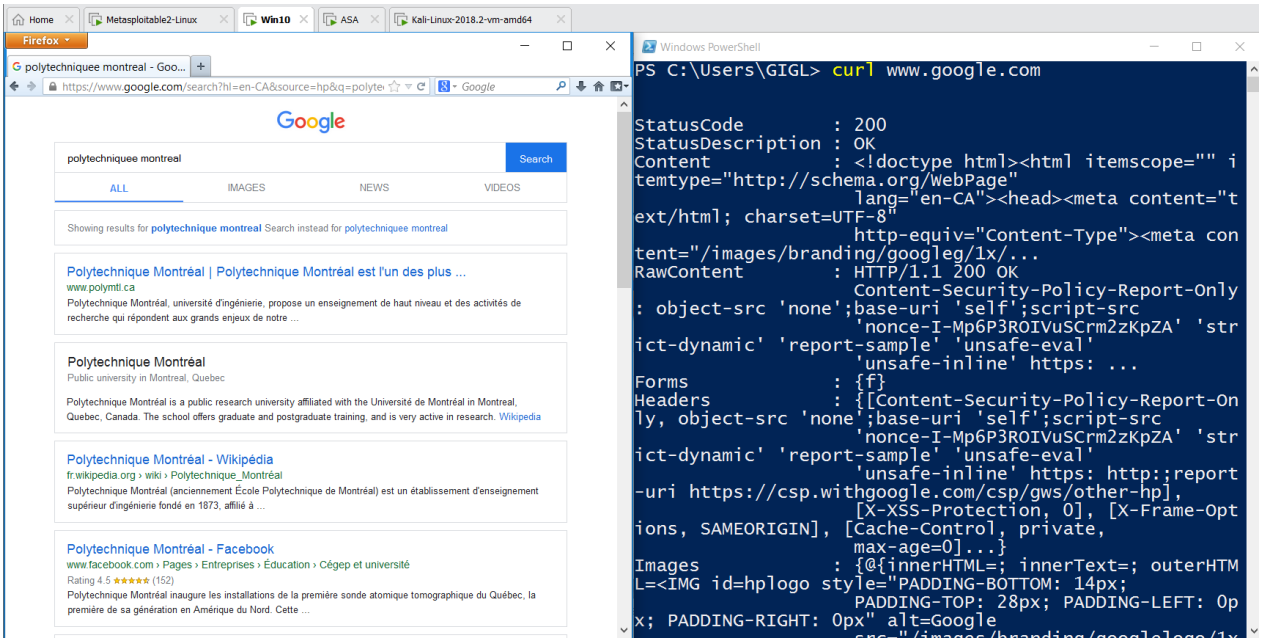

Figure 7.3 : Preuve d'accès à internet sur machine Windows

```
msfadmin@metasploitable:~$ curl www.polymtl.ca
<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx</center>
</body>
</html>
msfadmin@metasploitable:~$
```

```
msfadmin@metasploitable:~$ curl curl horde.polymtl.ca
curl: (6) Couldn't resolve host 'curl'
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://horde.polymtl.ca/">here</a>.</p>
</body></html>
msfadmin@metasploitable:~$ _
```

Figure 7.4 : Preuve d'accès à internet sur la machine Metasploit

Q8) Quelle(s) commande(s) permet(tent) à Kali Linux d'accéder à Internet?

a) Quelle configuration statique avez-vous utilisé? Vous pouvez présenter la configuration que vous avez utilisez dans le fichier /etc/network/interfaces (2 points)

La configuration réseau de la machine kali a été complété depuis l'interface graphique je suis allé dans Wired Connected puis dans Wired Settings puis dans settings enfin dans ipv4 et j'ai appliqué la configuration suivante :

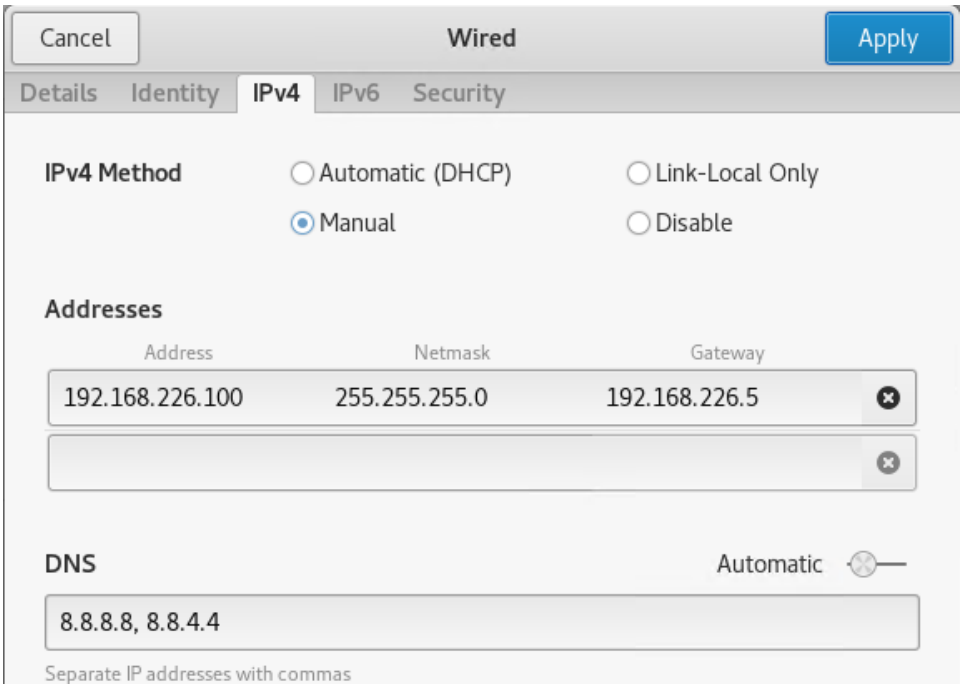

Figure 8.1 : Configuration réseau de la machine kali

b) Quelle commande NAT permet à tous les utilisateurs du réseau « OUTSIDE » d'aller vers internet? (2 points)

Pour permettre aux utilisateur d'outside d'aller vers internet on a créé une règle nat comme dans les 2 derniers cas

```
POLYFW01(config)# object network OUTSIDE-NET
POLYFW01(config-network-object)# subnet 192.168.226.0 255.255.255.0
POLYFW01(config-network-object)# nat (OUTSIDE,OUTSIDE) dynamic interface
```

Figure 8.2 : Règle NAT pour permettre à OUTSIDE d'aller sur internet

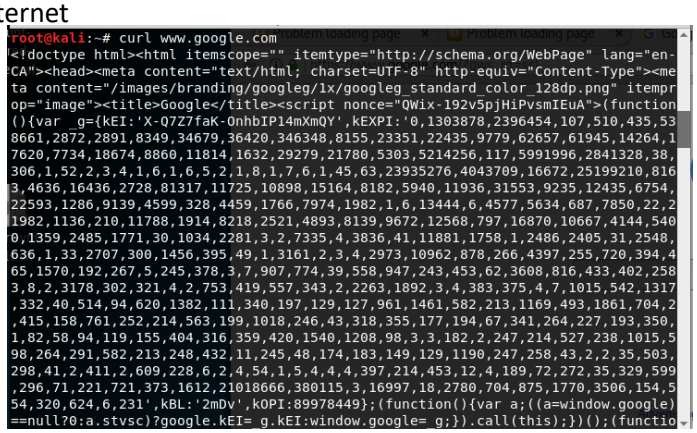

Figure 8.2 : Preuve que la machine Kali a accès

c) Quelle commande permet d'activer la communication entre deux hôtes d'une même interface afin qu'ils puissent communiquer entre eux? (2 points)

Pour activer la communication dans la même interface faire les commandes ci-dessous et enregistrer les modifications ensuite avec ***write memory***

```
POLYFW01(config)# configure terminal
POLYFW01(config)# same-security-traffic permit intra-interface
POLYFW01(config)# exit
POLYFW01# write memory
Building configuration...
Cryptochecksum: b21e86ac af8ccd04 21078a55 b3504fa6

2724 bytes copied in 0.20 secs
[OK]
```

Figure 8.3 : Activation de la communication intra interface