

Compte rendu TP6

DMZ, NAT, RIPv2, Firewall

Introduction

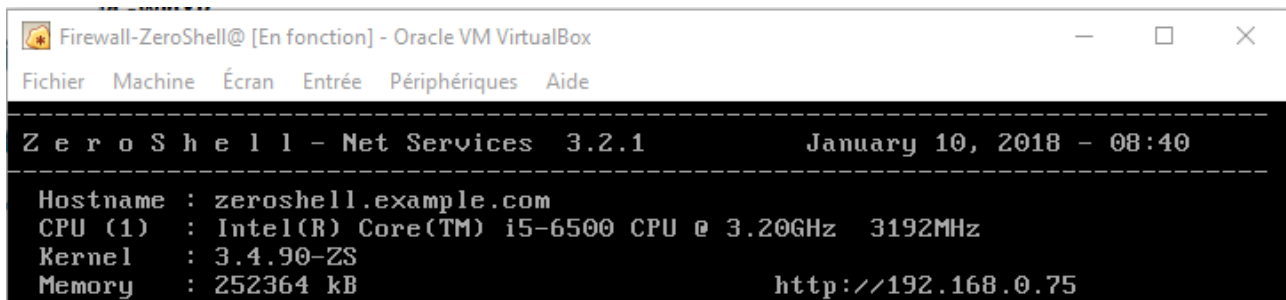
Lors de ce TP, nous avons pour objectif de configurer un réseau avec son DMZ virtuellement. Le but étant ensuite d'utiliser les commandes iptable NAT et de filtrage.

Table des matières

Partie I – Configuration de l’adressage du Firewall ZeroShell.....	4
Partie II – Configuration de l’adressage des autres machines.....	5
Partie III – Configuration de l’accès vers l’extérieur – NAT/PAT dynamique (masquerade).....	6
Partie IV – Configuration de l’accès extérieur aux serveurs – redirection de ports.....	8
Partie V – Mise en connexion de toutes les DMZ – routage RIPv2.....	10
Partie VI – Configuration des politiques de filtrage par défaut.....	11
Partie VII – Configuration complète du filtrage par Iptables.....	12

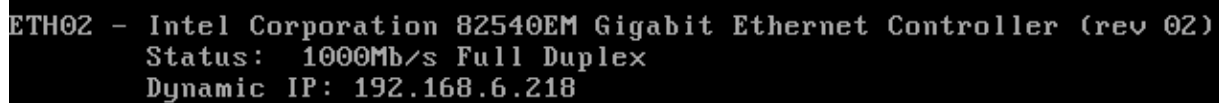
Partie I – Configuration de l'adressage du Firewall ZeroShell

1) Démarrez la machine « Firewall-ZeroShell » en cliquant dessus avec le bouton droit et en choisissant « Démarrer ».



```
Firewall-ZeroShell@ [En fonction] - Oracle VM VirtualBox
Fichier  Machine  Écran  Entrée  Périphériques  Aide
-----
Z e r o S h e l l - N e t S e r v i c e s   3.2.1           January 10, 2018 - 08:40
-----
Hostname : zeroshell.example.com
CPU (1)   : Intel(R) Core(TM) i5-6500 CPU @ 3.20GHz  3192MHz
Kernel   : 3.4.90-ZS
Memory    : 252364 kB                               http://192.168.0.75
```

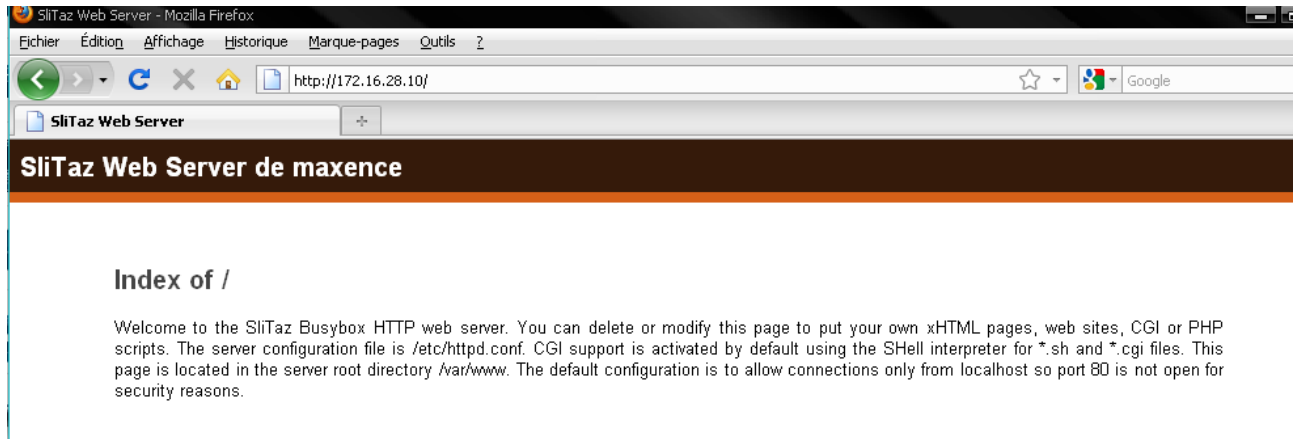
2) Notez cette adresse IP : c'est celle de l'interface extérieure de votre routeur, par laquelle on pourra vous joindre par la suite. elle est dynamique et changera à chaque fois que vous redémarrerez la machine virtuelle.



```
ETH02 - Intel Corporation 82540EM Gigabit Ethernet Controller (rev 02)
Status: 1000Mb/s Full Duplex
Dynamic IP: 192.168.6.218
```

Partie II – Configuration de l'adressage des autres machines

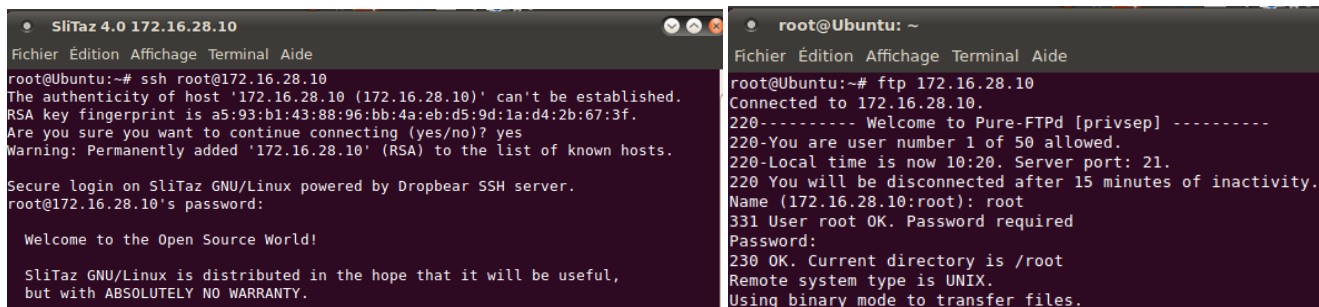
3) Vérifiez alors que vous pouvez bien accéder au site Web de votre DMZ.



Comment se comporte par défaut la machine «Firewall-ZeroShell» pour permettre cet accès ?

Réponse : Le firewall se comporte comme un routeur pour permettre cet accès.

4) Vérifiez depuis cette machine que vous pouvez alors accéder au serveurs SSH et FTP de la DMZ (avec le compte root/root)



Réponse : On peut accéder aux serveurs ssh et ftp.

Partie III – Configuration de l'accès vers l'extérieur – NAT/PAT dynamique (masquerade)

2)a) Commentez la table de routage obtenue. Y-a-t-il une route (passerelle) par défaut ? Comment a-elle été apprise ?

ROUTING TABLE

☒ Static

☒ Dynamic

☒ Auto

Destination	Netmask	Type	Metric	Gateway	Interface	Flags	State	Source
DEFAULT GATEWAY	0.0.0.0	Net	0	192.168.6.254	ETH02	UG	Up	Auto
172.16.28.0	255.255.255.0	Net	0	none	ETH01	U	Up	Auto
192.168.0.0	255.255.255.0	Net	0	none	ETH00	U	Up	Auto
192.168.6.0	255.255.255.0	Net	0	none	ETH02	U	Up	Auto
192.168.250.0	255.255.255.0	Net	0	none	VPN99	U	Up	Auto

Réponse : La première route est la route par défaut et elle a été apprise dynamiquement.

b) Expliquez le type de translation d'adresse ainsi définie et son effet sur les paquets des machines du LAN ou de la DMZ à destination de l'extérieur

Réponse : Le type de translation est MASQUERADE, les paquets provenant du LAN ou de la DMZ verront leurs adresses source se transformer en l'adresse de eth02 pour accéder à l'extérieur.

3) Quelle entrée a été ajoutée dans la table Iptables nat ? Dans quelle chaîne Iptables se trouve-t-elle ? Donnez la commande Iptable correspondante que vous auriez pu taper en ligne de commande pour obtenir ce résultat.

Port Forwarding and Source NAT (NAT)

```
Chain PREROUTING (policy ACCEPT 17 packets, 2567 bytes)
pkts bytes target      prot opt in      out     source      destination

Chain POSTROUTING (policy ACCEPT 2 packets, 120 bytes)
pkts bytes target      prot opt in      out     source      destination
 810 57635 SNATVS    all  --  *       *       0.0.0.0/0   0.0.0.0/0
   1   328 MASQUERADE  all  --  *       ETH02    0.0.0.0/0   0.0.0.0/0

Chain SNATVS (1 references)
pkts bytes target      prot opt in      out     source      destination
```

Réponse : iptable -t nat -A POSTROUTING -o eth02 -j MASQUERADE

4) Lancez un navigateur sur les machines « PC-Ubuntu », « PC-WinXP » , « Server-SliTaz » et vérifiez que vous pouvez aller sur Internet

Réponse : Ils se connectent.

Partie IV – Configuration de l'accès extérieur aux serveurs – redirection de ports

1)b) Quelle entrée a été ajoutée dans la table Iptables nat ? Dans quelle chaîne Iptables se trouve-t-elle ? Donnez la commande Iptable correspondante que vous auriez pu taper en ligne de commande pour obtenir ce résultat.

Port Forwarding and Source NAT (PAT)

Refresh
Close

Chain PREROUTING (policy ACCEPT 1 packets, 256 bytes)

pkts	bytes	target	prot	opt	in	out	source	destination
0	0	DNAT	tcp	--	ETH02	*	0.0.0.0/0	0.0.0.0/0 tcp dpt:80 to:172.16.28.

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)

pkts	bytes	target	prot	opt	in	out	source	destination
984	69170	SNATVS	all	--	*	*	0.0.0.0/0	0.0.0.0/0
165	11263	MASQUERADE	all	--	*	ETH02	0.0.0.0/0	0.0.0.0/0

Chain SNATVS (1 references)

pkts	bytes	target	prot	opt	in	out	source	destination
------	-------	--------	------	-----	----	-----	--------	-------------

Réponse : iptables -t nat -A PREROUTING -i eth02 -p tcp --dport 80 -j DNAT --to-destination 172.16.28.0:80

2) Ouvrez un navigateur depuis une autre machine physique Windows 10 (de votre voisin) et essayez d'afficher le site Web de votre DMZ. Par quelle adresse IP de votre machine ZeroShell pouvez-vous y parvenir ? Pourquoi ? Expliquez.

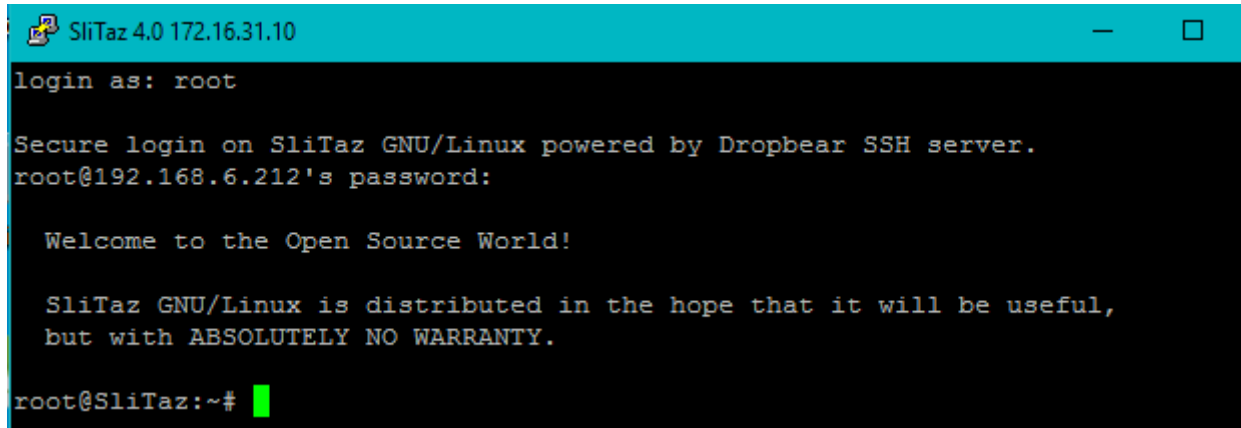
Réponse : On peut y parvenir par l'adresse publique de l'eth02. C'est grâce au mécanisme de translation que l'on adresse publique.

SliTaz Web Server didier

Index of /

Welcome to the SliTaz Busybox HTTP web server. You can delete or modify this page to put your own xHTML pages, web sites, CGI or PHP scripts. The server configuration file is /etc/httpd.conf. CGI support is activated by default using the SHell interpreter for *.sh and *.cgi files. This page is located in the server root directory /var/www. The default configuration is to allow connections only from localhost so port 80 is not open for security reasons.

3)b) Vérifiez l'accès SSH avec Putty et l'accès FTP avec FileZilla à votre serveur depuis la machine Windows 10 de votre voisin Vérifiez également depuis votre PC Windows 10 que vous pouvez accéder aux serveurs SSH et FTP des autres étudiants

A screenshot of a terminal window titled "SliTaz 4.0 172.16.31.10". The terminal shows the following text: "login as: root", "Secure login on SliTaz GNU/Linux powered by Dropbear SSH server.", "root@192.168.6.212's password:", "Welcome to the Open Source World!", "SliTaz GNU/Linux is distributed in the hope that it will be useful, but with ABSOLUTELY NO WARRANTY.", and "root@SliTaz:~#". The prompt "root@SliTaz:~#" is followed by a green cursor.

```
SliTaz 4.0 172.16.31.10
login as: root

Secure login on SliTaz GNU/Linux powered by Dropbear SSH server.
root@192.168.6.212's password:

Welcome to the Open Source World!

SliTaz GNU/Linux is distributed in the hope that it will be useful,
but with ABSOLUTELY NO WARRANTY.

root@SliTaz:~#
```

Partie V – Mise en connexion de toutes les DMZ – routage RIPv2

1)a) Pourquoi n'ajoute-t-on pas aussi l'interface ETH00 (comparer les adresses réseaux des LANs Intérieurs des différents étudiants) ?
Cochez la case pour l'interface ETH01. Pourquoi fait-on cela (rechercher sur Internet « rip passive interface ») ?

Réponse : L'interface ET00 est la même pour tout le monde donc il n'est pas nécessaire de l'ajouter . Le RIP passive interface est une commande qui permet d'empêcher les envois depuis cette interface. On le fait pour qu'aucun paquet ne soit créé depuis les serveurs de la DMZ.

b) Attendez que les d'autres étudiants aient fait la même chose et que RIP ait convergé jusqu'à voir apparaître les routes vers les réseaux DMZ des autres étudiants en dessous.

Learned by RIP								Make Static	Refresh
	Destination	Netmask	Type	Metric	Gateway	Learned From	State	Time	
<input type="radio"/>	172.16.7.0	255.255.255.0	Net	2	192.168.6.221	192.168.6.221	Up	02:36	
<input type="radio"/>	172.16.29.0	255.255.255.0	Net	2	192.168.6.220	192.168.6.220	Up	02:29	
<input type="radio"/>	172.16.31.0	255.255.255.0	Net	2	192.168.6.212	192.168.6.212	Up	02:51	
<input type="radio"/>	172.16.33.0	255.255.255.0	Net	2	192.168.6.197	192.168.6.197	Up	02:54	
<input type="radio"/>	172.16.48.0	255.255.255.0	Net	2	192.168.6.215	192.168.6.215	Up	02:42	
<input type="radio"/>	172.16.62.0	255.255.255.0	Net	2	192.168.6.194	192.168.6.194	Up	02:41	

2) Depuis le serveur SliTaz de votre DMZ, ouvrez le navigateur et vérifiez que vous pouvez joindre le serveur SliTaz d'un des réseaux apparus par son adresse IP.



Index of /

Welcome to the SliTaz Busybox HTTP web server. You can delete or modify this page to put your own xHTML pages, web sites, CGI or PHP scripts. The server configuration file is /etc/httpd.conf. CGI support is activated by default using the SHell interpreter for *.sh and *.cgi files. This page is located in the server root directory /var/www. The default configuration is to allow connections only from localhost so port 80 is not open for security reasons.

Partie VI – Configuration des politiques de filtrage par défaut

2) Que cela signifie-t-il ?

Réponse : Tout paquet traversant la machine ZeroShell est accepté et non rejeté ou détruit.

Partie VII – Configuration complète du filtrage par Iptables

Réponse :

Avant de commencer, vérifions s'il n'y a pas des commandes qui sont faites par défaut :

- d) Rien à faire car par défaut l'intérieur ne peut pas aller vers le public.
- f) Par défaut, c'est déjà autorisé.
- j) Aucune redirection donc rien à faire.

FORWARD									
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)									
pkts	bytes	target	prot	opt	in	out	source	destination	
1	0	0 DROP	all	--	ETH01	ETH00	0.0.0.0/0	0.0.0.0/0	
2	0	0 REJECT	tcp	--	ETH00	ETH01	0.0.0.0/0	0.0.0.0/0	state NEW tcp dpt:22 reject-with icmp-port-unreachable
3	0	0 REJECT	tcp	--	ETH02	ETH01	0.0.0.0/0	0.0.0.0/0	state NEW tcp dpt:20 reject-with icmp-port-unreachable
4	0	0 REJECT	tcp	--	ETH02	ETH01	0.0.0.0/0	0.0.0.0/0	state NEW tcp dpt:21 reject-with icmp-port-unreachable
5	0	0 DROP	udp	--	ETH00	*	192.168.0.2	0.0.0.0/0	udp dpt:53
6	0	0 REJECT	tcp	--	ETH02	ETH01	0.0.0.0/0	0.0.0.0/0	state NEW tcp dpt:22 reject-with icmp-port-unreachable
7	0	0 ACCEPT	tcp	--	ETH01	ETH02	0.0.0.0/0	0.0.0.0/0	state ESTABLISHED
8	0	0 REJECT	tcp	--	ETH01	ETH02	0.0.0.0/0	0.0.0.0/0	reject-with icmp-port-unreachable
9	0	0 REJECT	icmp	--	ETH01	ETH00	0.0.0.0/0	0.0.0.0/0	reject-with icmp-port-unreachable
10	0	0 ACCEPT	icmp	--	ETH00	ETH01	0.0.0.0/0	0.0.0.0/0	

OUTPUT									
Chain OUTPUT (policy ACCEPT 88 packets, 50157 bytes)									
pkts	bytes	target	prot	opt	in	out	source	destination	
1130	847K	SYS_OUTPUT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	
0	0	0 DROP	icmp	--	*	ETH02	0.0.0.0/0	0.0.0.0/0	

Correspondance des commandes :

- b) C'est la commande 8.
- c) C'est la commande 2
- e) Ce sont les commandes 3,4,6 pour chaque port 20-21 FTP -22 SSH
- g) C'est la commande 7
- h) C'est la commande dans output
- i) C'est la commande 9
- k) C'est la commande 5

Pour les vérifications, je n'ai pas eu le temps, excusez-moi.

Conclusion

A l'issue de ce TP, nous savons configurer un réseau et sa DMZ et aussi utiliser des interfaces de mises en place de filtre et de translation d'adresse NAT.