

RAPPORT DU TP SML

The background features several blue 3D rectangular bars of varying heights and widths, arranged in a dynamic, overlapping fashion. Some bars are light blue, while others are a darker shade. In the top right corner, there is a small flag on a pole. At the bottom center, there are three vertical lines of different heights. The overall aesthetic is modern and geometric.

ACCLOMBESSI Bienvenu
Filière: Génie Logiciel à
IFRI

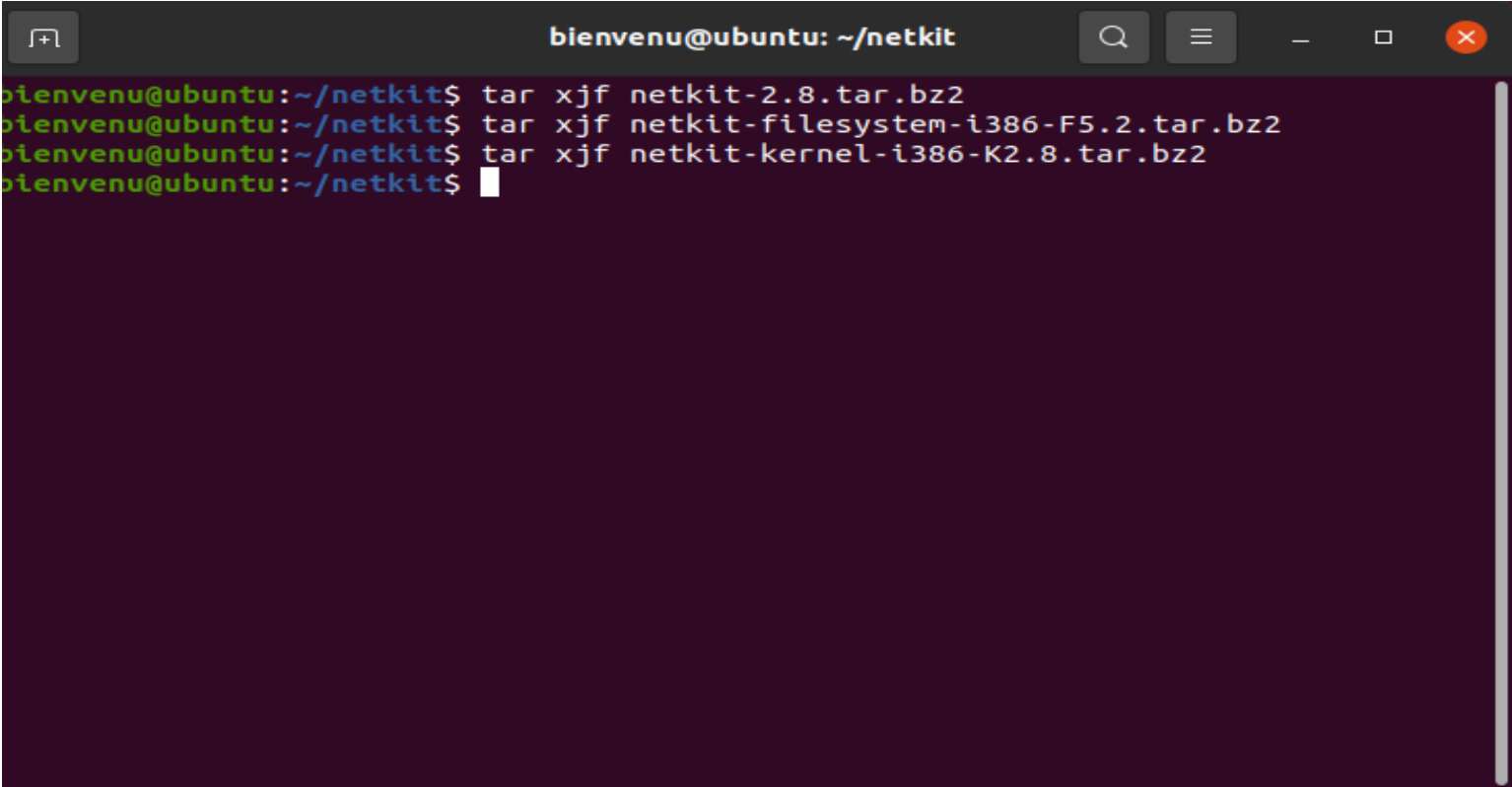
PARTIE 1 : ASPECT MATERIEL

Cette première partie consiste en l'installation de netkit, la création et la configuration des machines de notre architecture avec les différents tests réalisés pour vérifier la communication de nos machines à travers les Ping.

1-Installation de l'outil de simulation Netkit.

Etape 1 : Désarchiver les trois fichiers netkit zippés.

Après avoir téléchargés les fichiers zippés de NETKIT sur son site officiel, nous allons les désarchiver.

A terminal window titled 'bienvenu@ubuntu: ~/netkit' with standard window controls. It shows three lines of commands being executed to extract tarballs: 'tar xjf netkit-2.8.tar.bz2', 'tar xjf netkit-filesystem-i386-F5.2.tar.bz2', and 'tar xjf netkit-kernel-i386-K2.8.tar.bz2'. The prompt is 'bienvenu@ubuntu:~/netkit\$' and a cursor is visible on the last line.

```
bienvenu@ubuntu: ~/netkit
bienvenu@ubuntu:~/netkit$ tar xjf netkit-2.8.tar.bz2
bienvenu@ubuntu:~/netkit$ tar xjf netkit-filesystem-i386-F5.2.tar.bz2
bienvenu@ubuntu:~/netkit$ tar xjf netkit-kernel-i386-K2.8.tar.bz2
bienvenu@ubuntu:~/netkit$
```

Etape 2 : Lancer Netkit

Pour cela on exécute ces commandes pour définir des variables d'environnement:

(Voir la capture suivante)

```

bienvenu@ubuntu: ~/netkit/netkit
bienvenu@ubuntu:~/netkit/netkit$ export NETKIT_HOME=/home/bienvenu/netkit/netkit
bienvenu@ubuntu:~/netkit/netkit$ export PATH=$PATH:$NETKIT_HOME/bin
bienvenu@ubuntu:~/netkit/netkit$ export MANPATH=$NETKIT_HOME/man
bienvenu@ubuntu:~/netkit/netkit$ ./check_configuration.sh
> Checking path correctness... passed.
> Checking environment... passed.
> Checking for availability of man pages... passed.
> Checking for proper directories in the PATH... passed.
> Checking for availability of auxiliary tools:
    awk      : ok
    basename : ok
    date     : ok
    dirname  : ok
    find     : ok
    getopt   : ok
    grep     : ok
    head     : ok
    id       : ok
    kill     : ok
    ls       : ok
    lsof     : ok
    ps       : ok
    readlink : ok
    wc       : ok
    port-helper : ok
    tuncctl  : ok
    uml_mconsole : ok
    uml_switch : ok
passed.
> Checking for availability of terminal emulator applications:
    xterm      : found
    konsole    : found
    gnome-terminal : found
passed.
> Checking filesystem type... passed.
> Checking whether 32-bit executables can run... passed.

[ READY ] Congratulations! Your Netkit setup is now complete!
          Enjoy Netkit!
bienvenu@ubuntu:~/netkit/netkit$
```

Après avoir exécuté ces commandes nous avons vu [READY] qui montre que Netkit est bien démarré.

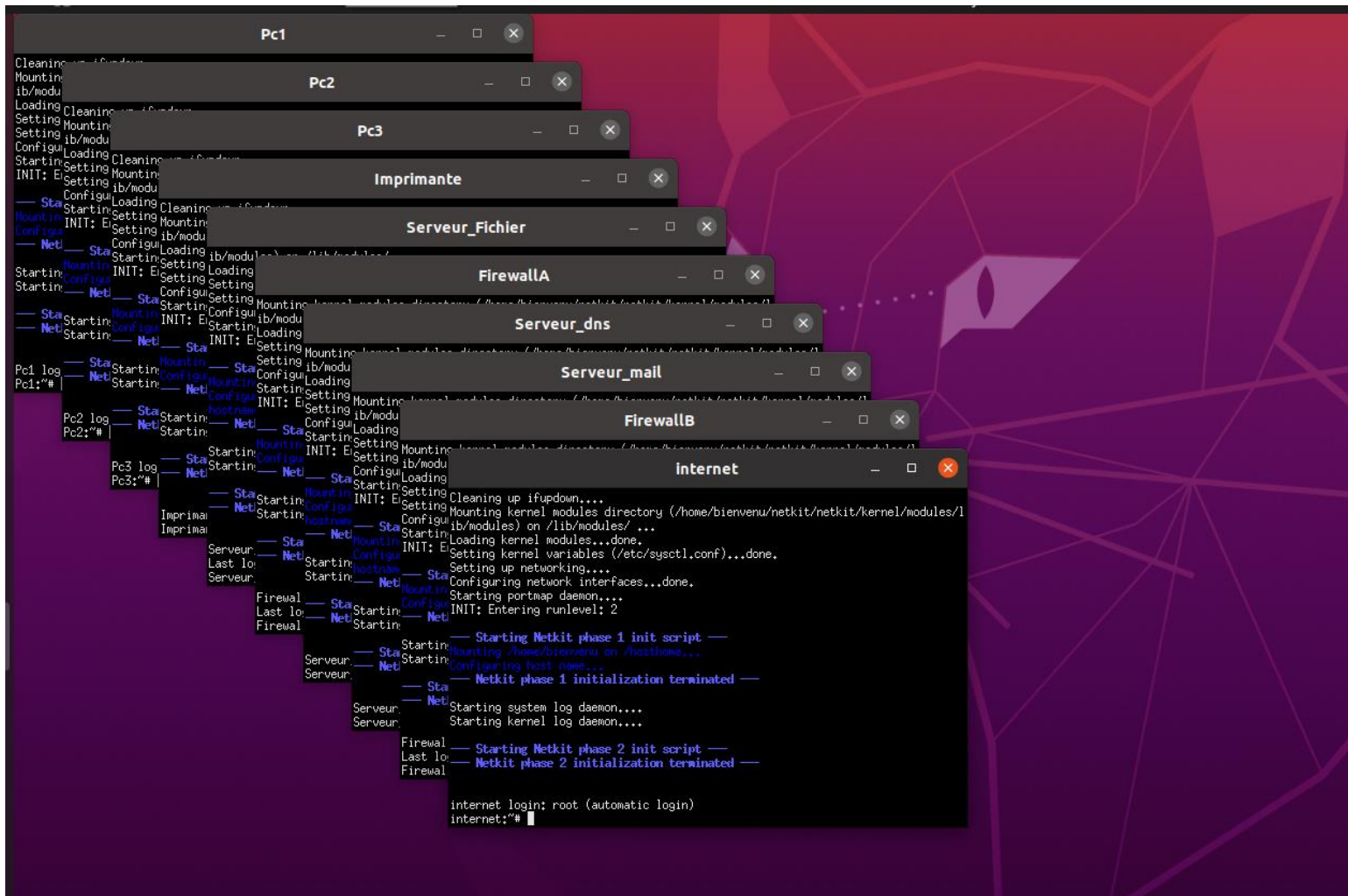
2. Création des différentes ressources de l'architecture tout en configurant leurs interfaces telles que proposées sur l'architecture du système d'information.

Etape1 : Création des différentes ressources de l'architecture.

Pour cela nous allons utiliser la commande VSTART de Netkit qui permet de créer des machines.

On obtient des machines du réseau:

Notre architecture comporte trois réseaux : Le réseau local qui contient trois PC (PC1, PC2, PC3) un serveur de fichier nommé serveur fichiers et une imprimante; La DMZ qui comporte deux serveurs: serveur_dns et serveur_mail puis Internet simulé ici par un PC nommé internet et l'autre nommé internet2 afin de vérifier après la communication entre les machines de l'internet. On a ensuite deux firewalls le premier qui relie le réseau local à la DMZ nommé firewallA et l'autre qui relie internet à la DMZ, (firewallB).

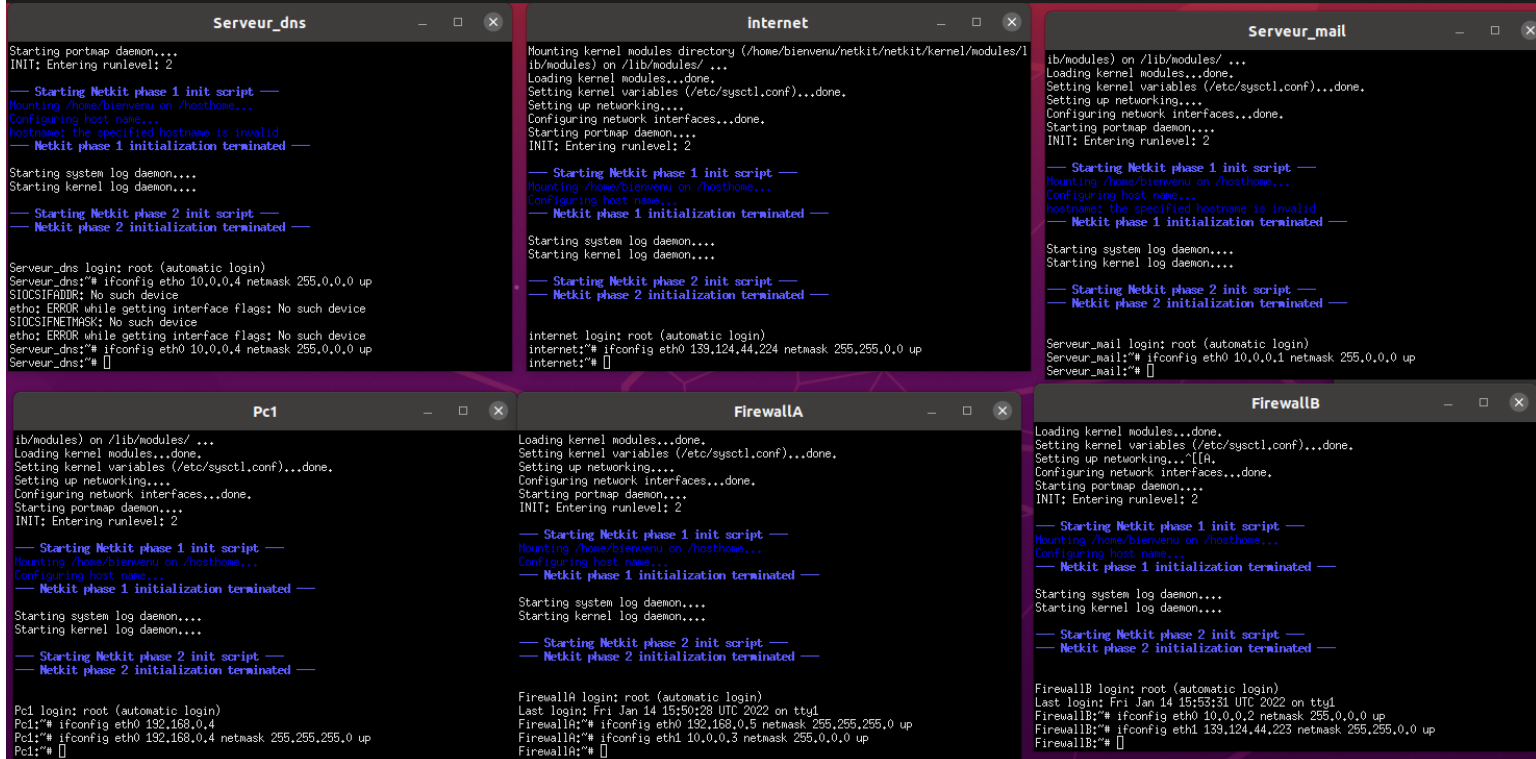


Toutes les machines sont démarrées, alors configurons ces machines pour permettre la communication entre ces dernières ;

Etape2 : Configuration des interfaces de chaque machine.

Configurer les machines avec les commandes (Exemple pour PC1) :

- `ifconfig eth0 192.168.0.4 netmask 255.255.255.0 broadcast 192.168.0.255 up .`



On vient de faire la configuration de l'adresse IP de chaque machine selon ces interfaces.

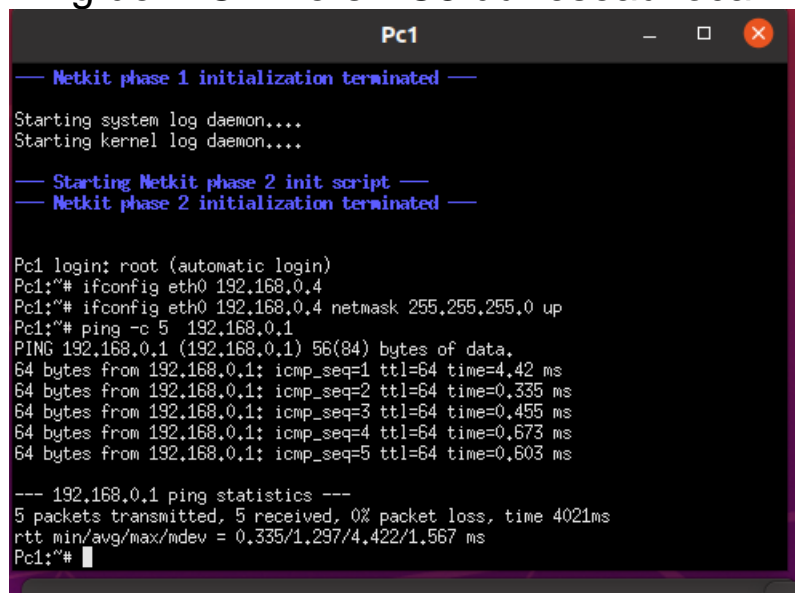
3. Vérification de la communication entre les machines.

a-Configuration (voir 2-Etape2)

b-Vérification de la communication entre les machines du réseau local

Pour cela nous allons ping :

➤ Ping de PC1 vers PC3 du réseau local



Tous les paquets envoyés sont reçus

Ce qui montre que il y'a interconnexion entre les machines du réseau local.

C-Vérification de la communication entre les machines de la DMZ

➤ Ping entre serveur mail et serveur DNS

```

Serveur_mail
hostname: the specified hostname is invalid
--- Netkit phase 1 initialization terminated ---

Starting system log daemon....
Starting kernel log daemon....

--- Starting Netkit phase 2 init script ---
--- Netkit phase 2 initialization terminated ---

Serveur_mail login: root (automatic login)
Serveur_mail:~# ifconfig eth0 10.0.0.1 netmask 255.0.0.0 up
Serveur_mail:~# ping -c 5 10.0.0.4
PING 10.0.0.4 (10.0.0.4) 56(84) bytes of data:
64 bytes from 10.0.0.4: icmp_seq=1 ttl=64 time=2.68 ms
64 bytes from 10.0.0.4: icmp_seq=2 ttl=64 time=0.392 ms
64 bytes from 10.0.0.4: icmp_seq=3 ttl=64 time=0.335 ms
64 bytes from 10.0.0.4: icmp_seq=4 ttl=64 time=0.304 ms
64 bytes from 10.0.0.4: icmp_seq=5 ttl=64 time=0.578 ms

--- 10.0.0.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4022ms
rtt min/avg/max/mdev = 0.304/0.859/2.688/0.919 ms
Serveur_mail:~#
```

Tous les paquets sont reçus
Ce qui montre que il y'a interconnexion entre les machines du DMZ.

C-Vérification de la communication entre les machines du domaine de collision C (internet).

```

internet2
64 bytes from 192.168.0.4: icmp_seq=1 ttl=62 time=10.5 ms
64 bytes from 192.168.0.4: icmp_seq=2 ttl=62 time=1.11 ms
64 bytes from 192.168.0.4: icmp_seq=3 ttl=62 time=1.16 ms
64 bytes from 192.168.0.4: icmp_seq=4 ttl=62 time=1.29 ms

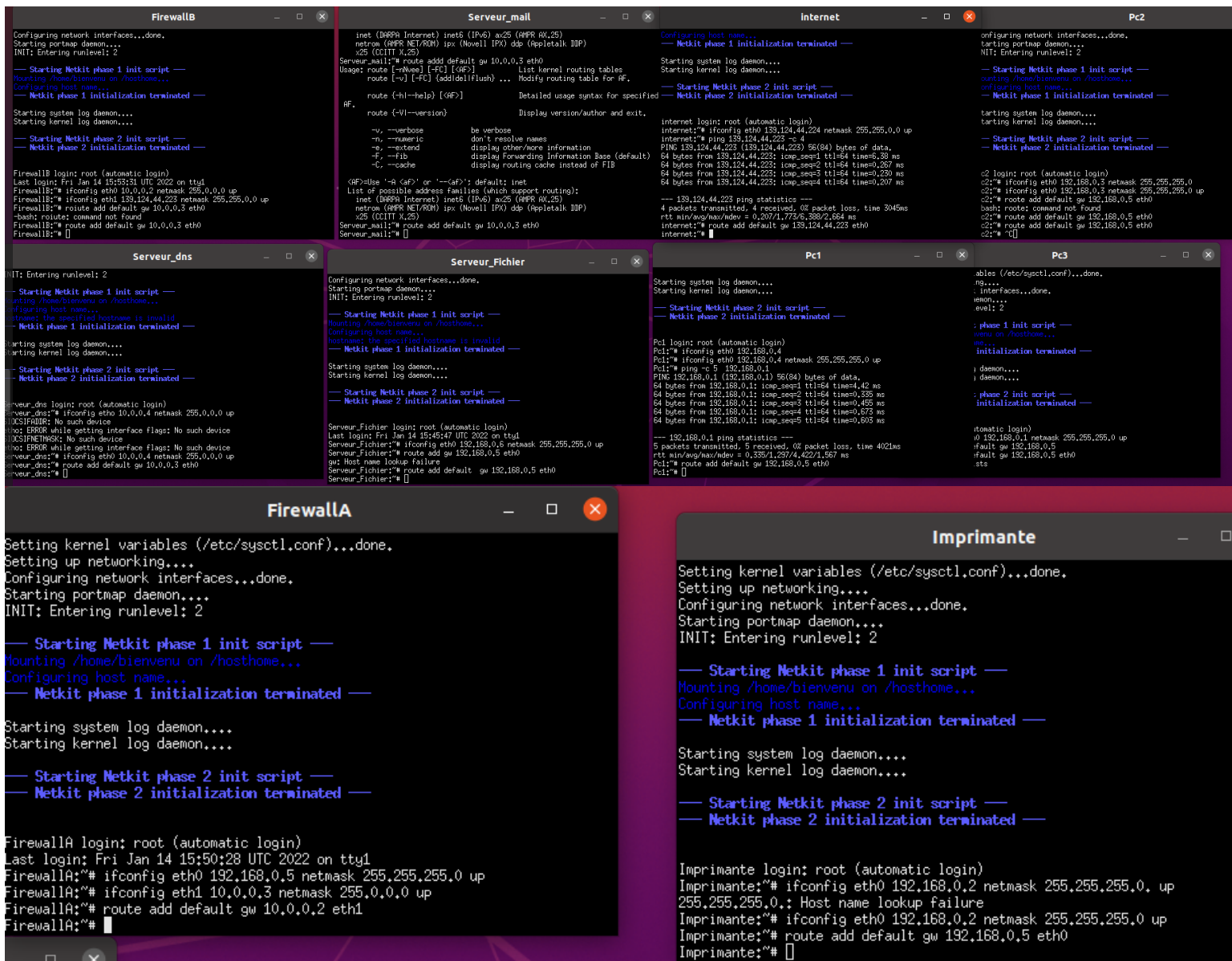
--- 192.168.0.4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3031ms
rtt min/avg/max/mdev = 1.119/3.542/10.585/4.066 ms
internet2:~# telnet 10.0.0.1 80
Trying 10.0.0.1...
Connected to 10.0.0.1.
Escape character is '^]'.
^Cte^C^C^C^CConnection closed by foreign host.
internet2:~# ping 139.124.44.224 -c4
PING 139.124.44.224 (139.124.44.224) 56(84) bytes of data:
64 bytes from 139.124.44.224: icmp_seq=1 ttl=64 time=5.77 ms
64 bytes from 139.124.44.224: icmp_seq=2 ttl=64 time=0.325 ms
64 bytes from 139.124.44.224: icmp_seq=3 ttl=64 time=0.270 ms
64 bytes from 139.124.44.224: icmp_seq=4 ttl=64 time=0.339 ms

--- 139.124.44.224 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3051ms
rtt min/avg/max/mdev = 0.270/1.676/5.772/2.365 ms
internet2:~#
```

e-Configuration du routage statique

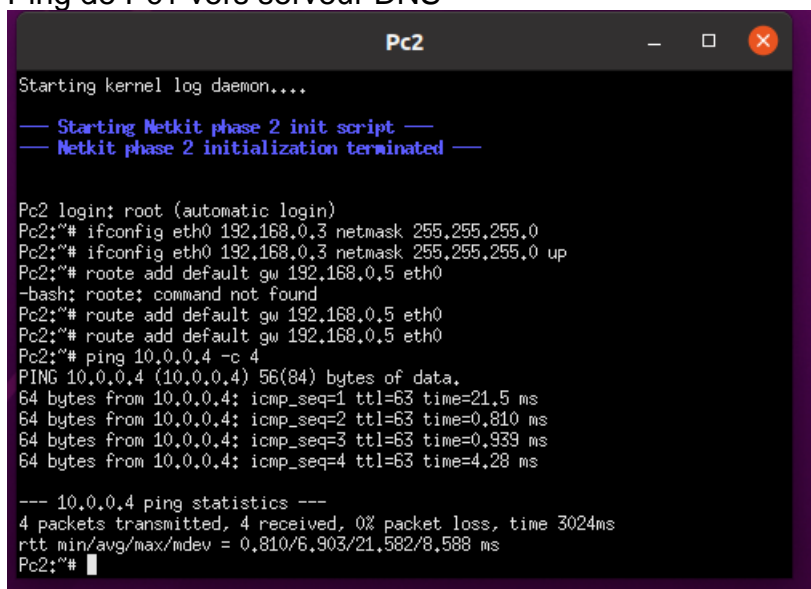
Pour cela nous allons ajouter le Gateway à toutes les machines avec la commande
-route add default gw 192.168.0.4 dev eth0 (pc1 par exemple)

Faisons de même pour les autres machines et puis pour les deux firewalls.



Vérification de la communication entre les deux réseaux (réseau local et DMZ) .

- Ping de Pc1 vers serveur DNS



Ce qui montre que les machines du réseau Local et de la DMZ communiquent

f- Assurons que les machines du réseau Local, de la DMZ et celles situées sur internet communiquent à partir d'un trafic entrant et sortant.

➤ Ping internet et réseau local

```
internet
internet login: root (automatic login)
internet:~# ifconfig eth0 139.124.44.224 netmask 255.255.0.0 up
internet:~# ping 139.124.44.223 -c 4
PING 139.124.44.223 (139.124.44.223) 56(84) bytes of data.
64 bytes from 139.124.44.223: icmp_seq=1 ttl=64 time=6.38 ms
64 bytes from 139.124.44.223: icmp_seq=2 ttl=64 time=0.267 ms
64 bytes from 139.124.44.223: icmp_seq=3 ttl=64 time=0.230 ms
64 bytes from 139.124.44.223: icmp_seq=4 ttl=64 time=0.207 ms

--- 139.124.44.223 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3045ms
rtt min/avg/max/mdev = 0.207/1.773/6.388/2.664 ms
internet:~# route add default gw 139.124.44.223 eth0
internet:~# ping 192.168.0.4 -c 4
PING 192.168.0.4 (192.168.0.4) 56(84) bytes of data.
64 bytes from 192.168.0.4: icmp_seq=1 ttl=62 time=6.54 ms
64 bytes from 192.168.0.4: icmp_seq=2 ttl=62 time=0.990 ms
64 bytes from 192.168.0.4: icmp_seq=3 ttl=62 time=0.933 ms
64 bytes from 192.168.0.4: icmp_seq=4 ttl=62 time=0.830 ms

--- 192.168.0.4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3043ms
rtt min/avg/max/mdev = 0.830/2.325/6.548/2.438 ms
internet:~#
```

➤ Ping internet et DMZ

```
Serveur_dns
Serveur_dns login: root (automatic login)
Serveur_dns:~# ifconfig eth0 10.0.0.4 netmask 255.0.0.0 up
SIOCSIFADDR: No such device
eth0: ERROR while getting interface flags: No such device
SIOCSIFNETMASK: No such device
eth0: ERROR while getting interface flags: No such device
Serveur_dns:~# ifconfig eth0 10.0.0.4 netmask 255.0.0.0 up
Serveur_dns:~# route add default gw 10.0.0.3 eth0
Serveur_dns:~# ping 139.124.44.224 -c 4
PING 139.124.44.224 (139.124.44.224) 56(84) bytes of data.
64 bytes from 139.124.44.224: icmp_seq=1 ttl=63 time=28.4 ms
From 10.0.0.3: icmp_seq=2 Redirect Host(New nexthop: 10.0.0.2)
64 bytes from 139.124.44.224: icmp_seq=2 ttl=63 time=0.524 ms
From 10.0.0.3: icmp_seq=3 Redirect Host(New nexthop: 10.0.0.2)
64 bytes from 139.124.44.224: icmp_seq=3 ttl=63 time=0.856 ms
From 10.0.0.3: icmp_seq=4 Redirect Host(New nexthop: 10.0.0.2)
64 bytes from 139.124.44.224: icmp_seq=4 ttl=63 time=0.814 ms

--- 139.124.44.224 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3043ms
rtt min/avg/max/mdev = 0.524/7.651/28.413/11.987 ms
Serveur_dns:~#
```

Les trois réseaux se communiquent entre eux

4. Automatisations de toutes les configurations en créant un fichier « lab.conf » pour enregistrer toutes vos configuration afin d'éviter de les perdre à chaque redémarrage de votre système et votre simulateur NetKit.

➤ Voici le contenu du fichier PC1.startup

Pour ne pas être répétitif nous allons présenter seulement pour le pc1 et le lab.conf

- Voici le contenu du fichier lab.conf

```
Pc1[0]="A"
Pc2[0]="A"
Pc3[0]="A"
Imprimante[0]="A"
Serveur_Fichier[0]="A"
FirewallA[0]="A"
FirewallA[1]="B"
FirewallB[0]="B"
FirewallB[1]="C"
Serveur_dns[0]="B"
Serveur_mail[0]="B"
internet[0]="C"
internet2[0]="C"
```

5. Mise en place des différents services au niveau des serveurs qui sont présentent dans l'architecture des systèmes d'information.

- Service dns-ftp-ssh Avec les commandes suivantes
- /etc/init.d/bind start (dns)
 - /etc/init.d/ssh start (ssh)
 - /etc/init.d/proftpd start (ftp)

```

Serveur_dns
Lab directory (host): /home/bienvenu/netkit/netkit/Laboratoires
Version: <none>
Author: <none>
Email: <none>
Web: <none>
Description:
<none>

*****

— Netkit phase 2 initialization terminated —

Serveur_dns login: root (automatic login)
Serveur_dns:~# /etc/init.d/bind start
Starting domain name service...: bind9.
Serveur_dns:~# /etc/init.d/ssh start
Starting OpenBSD Secure Shell server: sshd.
Serveur_dns:~# /etc/init.d/proftpd start
-bash: /etc/init.d/proftpd: No such file or directory
Serveur_dns:~# /etc/init.d/proftpd start
Starting ftp server: proftpd.
Serveur_dns:~# █

```

- Service web et smtp Avec la commande suivante
/etc/init.d/apache2 start (web)
/etc/init.d/exim4 start (smtp)

```

Serveur_mail

— Netkit phase 2 initialization terminated —

Serveur_mail login: root (automatic login)
Serveur_mail:~# ping 192.168.0.1 -c4
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data:
64 bytes from 192.168.0.1: icmp_seq=1 ttl=63 time=21.6 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=63 time=2.57 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=63 time=6.06 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=63 time=2.76 ms

--- 192.168.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 2.572/8.253/21.614/7.837 ms
Serveur_mail:~# /etc/init.d/apache2 start
Starting web server: apache2apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.0.1 for ServerName
*
Serveur_mail:~# /etc/init.d/apache2 start
Starting web server: apache2apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.0.1 for ServerName
httpd (pid 526) already running
*
Serveur_mail:~# █

```

Partie2 :Les règles iptables pour la redirection des trafics.

Dans cette partie

Pour cela ajouter ceci dans le fichier de firewallB.startup

```

iptables -t nat -A POSTROUTING -o -j MASQUERADE
iptables -A FORWARD -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -p tcp --dport 53 -j ACCEPT
iptables -A FORWARD -p tcp --dport 21 -j ACCEPT
iptables -A FORWARD -p tcp --dport 22 -j ACCEPT
iptables -A FORWARD -p tcp --dport 25 -j ACCEPT
iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j DNAT --to-destination 10.0.0.1:80
iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 53 -j DNAT --to-destination 10.0.0.4:53
iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 21 -j DNAT --to-destination 10.0.0.4:21
iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 22 -j DNAT --to-destination 10.0.0.4:22
iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 25 -j DNAT --to-destination 10.0.0.1:25

```

```

Cleaning up ifupdown....
Mounting kernel modules directory (/home/bienvenu/netkit/netkit/kernel/modules/1
ib/modules) on /lib/modules/ ...
Loading kernel modules...done.
Setting kernel variables (/etc/sysctl.conf)...done.
Setting up networking....
Configuring network interfaces...done.
Starting portmap daemon....
INIT: Entering runlevel: 2

--- Starting Netkit phase 1 init script ---
Mounting /home/bienvenu on /hosthome...
Mounting /home/bienvenu/netkit/netkit/Laboratoires on /hostlab ...
Configuring host name...
--- Netkit phase 1 initialization terminated ---

Starting system log daemon....
Starting kernel log daemon....

--- Starting Netkit phase 2 init script ---

>>> Running FirewallA specific startup script...
>>> End of FirewallA specific startup script.

*****

Lab directory (host): /home/bienvenu/netkit/netkit/Laboratoires
Version: <none>
Author: <none>
Email: <none>
Web: <none>
Description:
<none>

*****

--- Netkit phase 2 initialization terminated ---

FirewallA login: root (automatic login)
Last login: Mon Jan 24 15:18:47 UTC 2022 on tty1
FirewallA:~# iptables -F
FirewallA:~# iptables -X
FirewallA:~# iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
Chain FORWARD (policy ACCEPT)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
FirewallA:~# iptables -P FORWARD DROP
FirewallA:~# iptables -P INPUT DROP
FirewallA:~# iptables -P OUTPUT DROP
FirewallA:~# iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
FirewallA:~# iptables -A FORWARD -m state --state NEW -P tcp --dport 80 -j ACCEPT
iptables v1.4.1.1: Can't use -P with -A
Try 'iptables -h' or 'iptables --help' for more information.
FirewallA:~# iptables -A FORWARD -m state --state NEW -p tcp --dport 80 -j ACCEPT
FirewallA:~#

```

Les six(6) premières règles vont nous permettre de contrôler les trafics qui vont traverser le firewallB(Par les ports 80 53 21 22 25). Ceux qui suivent vont nous permettre de contrôler les trafics qui vont venir vers le firewallB

Pour le firewallA mettons :

```

iptables -t nat -A POSTROUTING -o -j MASQUERADE
iptables -A FORWARD -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -p tcp --dport 53 -j ACCEPT
iptables -A FORWARD -p tcp --dport 21 -j ACCEPT
iptables -A FORWARD -p tcp --dport 22 -j ACCEPT
iptables -A FORWARD -p tcp --dport 25 -j ACCEPT

```

Vérification avec Pctest qui est internet et avec Pc1

Avec la commande telnet on a :

- Internet vers serveur web par le port 80.

```
internet2
Description:
<none>

*****

--- Netkit phase 2 initialization terminated ---

internet2 login: root (automatic login)
internet2:~# ping 192.168.0.4 -c4
PING 192.168.0.4 (192.168.0.4) 56(84) bytes of data:
64 bytes from 192.168.0.4: icmp_seq=1 ttl=62 time=10.5 ms
64 bytes from 192.168.0.4: icmp_seq=2 ttl=62 time=1.11 ms
64 bytes from 192.168.0.4: icmp_seq=3 ttl=62 time=1.16 ms
64 bytes from 192.168.0.4: icmp_seq=4 ttl=62 time=1.29 ms

--- 192.168.0.4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3031ms
rtt min/avg/max/mdev = 1.119/3.542/10.585/4.066 ms
internet2:~# telnet 10.0.0.1 80
Trying 10.0.0.1...
Connected to 10.0.0.1.
Escape character is '^['.
```

On constate que la machine d'internet a pu se connecter au serveur web.

- Pc1 vers le serveur web

```
Pc1
Author: <none>
Email: <none>
Web: <none>
Description:
<none>

*****

--- Netkit phase 2 initialization terminated ---

Pc1 login: root (automatic login)
Last login: Tue Jan 25 16:39:32 UTC 2022 on tty1
Pc1:~# telnet 10.0.0.1:80
telnet: could not resolve 10.0.0.1:80/telnet: Temporary failure in name resolution
Pc1:~# telnet 10.0.0.180
Trying 10.0.0.180...
telnet: Unable to connect to remote host: No route to host
Pc1:~# telnet 10.0.0.1 80
Trying 10.0.0.1...
Connected to 10.0.0.1.
Escape character is '^['.
```

On constate que le Pc1 du réseau local a pu se connecter au serveur web au port 80 à l'adresse 10.0.0.1.

- internet vers le serveur Dns au port 53.

```
Pc1
>>> End of Pc1 specific startup script.

*****

Lab directory (host): /home/bienvenu/netkit/netkit/Laboratoires
Version: <none>
Author: <none>
Email: <none>
Web: <none>
Description:
<none>

*****

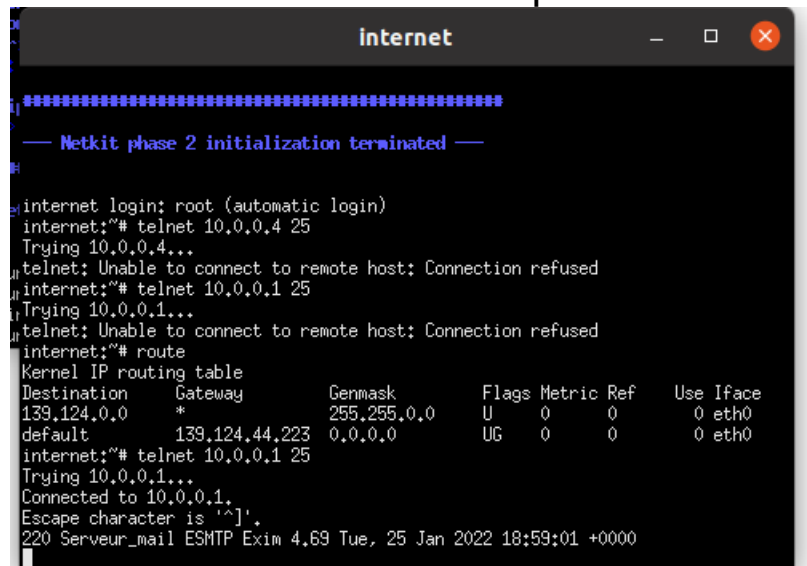
--- Netkit phase 2 initialization terminated ---

Pc1 login: root (automatic login)
Pc1:~# telnet 10.0.0.4 21
Trying 10.0.0.4...
Connected to 10.0.0.4.
Escape character is '^['.
```

On constate que le Pc1 du réseau local a pu se connecter au serveur ftp.

- Internet vers le serveur Dns au port 53.

Nous allons vérifier si une machine d'internet peut se connecter au serveur ssh. Tapons alors la commande telnet



```
#####
— Netkit phase 2 initialization terminated —

internet login: root (automatic login)
internet:~# telnet 10.0.0.4 25
Trying 10.0.0.4...
telnet: Unable to connect to remote host: Connection refused
internet:~# telnet 10.0.0.1 25
Trying 10.0.0.1...
telnet: Unable to connect to remote host: Connection refused
internet:~# route
Kernel IP routing table
Destination    Gateway         Genmask         Flags Metric Ref    Use Iface
139.124.0.0    *               255.255.0.0     U        0      0        0 eth0
default        139.124.44.223  0.0.0.0         UG        0      0        0 eth0
internet:~# telnet 10.0.0.1 25
Trying 10.0.0.1...
Connected to 10.0.0.1.
Escape character is '^]'.
220 Serveur_mail ESMTP Exim 4.69 Tue, 25 Jan 2022 18:59:01 +0000
```

Après les Telnet on constate que la machine arrive à se connecter à ce serveur

A présent le trafic adressé à l'interface du firewallB (139.124.44.223) est redirigé en fonction du port vers le service approprié.