

SÉCURITÉ RÉSEAU – 06/12/2024**TP n°2 : Sécurisation d'un réseau et Mails chiffrés avec PGP**

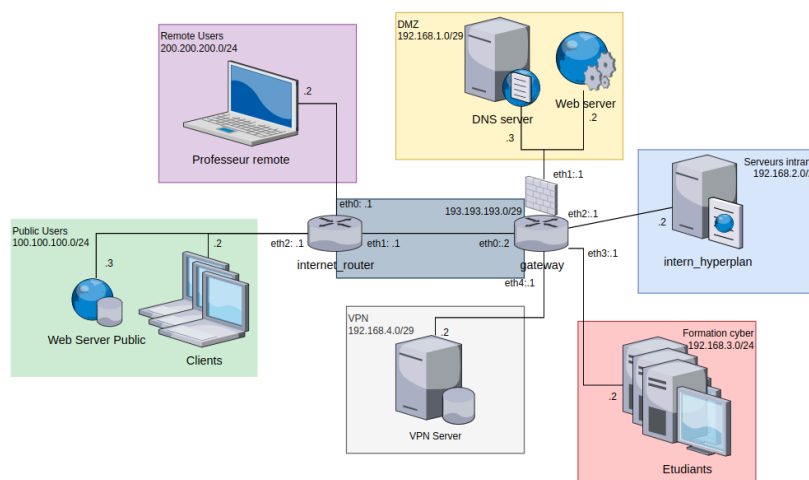
Préambule : Le TP est réalisé sur le PC personnel des étudiants de manière individuelle. Chaque étudiant a à sa disposition les transparents des cours, les manuels des outils à utiliser ainsi que le droit de faire des recherches sur Internet. L'étudiant peut faire appel au responsable du TP afin de ne pas rester bloqué. La preuve des manipulations AINSI que l'explication des commandes utilisées sont prises en compte pour l'évaluation.

Pour faciliter le TP, il est conseillé de faire une copie de l'état du dossier du TP à chaque manipulation pour éviter d'avoir à refaire l'ensemble des manipulations. Le dossier final sera à remettre au responsable du TP.

Prérequis techniques : Les étudiants sont informés en amont du besoin d'installer le logiciel kathara directement à l'adresse <https://www.kathara.org/download.html>.

Situation du TP : L'administrateur système de l'école H vient de terminer sa réunion avec le directeur et ils se sont mis d'accord sur les droits d'accès aux ressources depuis l'intranet et l'extranet. L'administrateur système a démarré le déploiement mais il se perd avec la paramétrisation de son firewall. Vous êtes donc en charge de terminer avec lui la configuration réseau, de déployer des règles sur le firewall et de transmettre les résultats de la procédure par mails chiffrés au directeur.

Ci-dessous, le plan du réseau :



Les spécifications principales associées sont :

- Les « clients » doivent pouvoir accéder à un serveur Web hébergé à l'école
- Les « professeurs en remote » et les « étudiants » doivent pouvoir accéder au serveur interne sans exposer celui-ci sur Internet.
- Les « étudiants » doivent pouvoir accéder à Internet sans ouvrir de brèches sur le système

Afin de réaliser ce travail, vous avez à votre disposition des annexes en plus de votre cours, vos connaissances et Internet. **L'exercice 1 doit impérativement être réalisé en premier pour accéder aux autres parties.** Les autres questions sont indépendantes mais ordonnées dans l'ordre de difficulté croissant.

Pour démarrer, téléchargez le « lab kathara » de la situation initiale.

SÉCURITÉ RÉSEAU – 06/12/2024

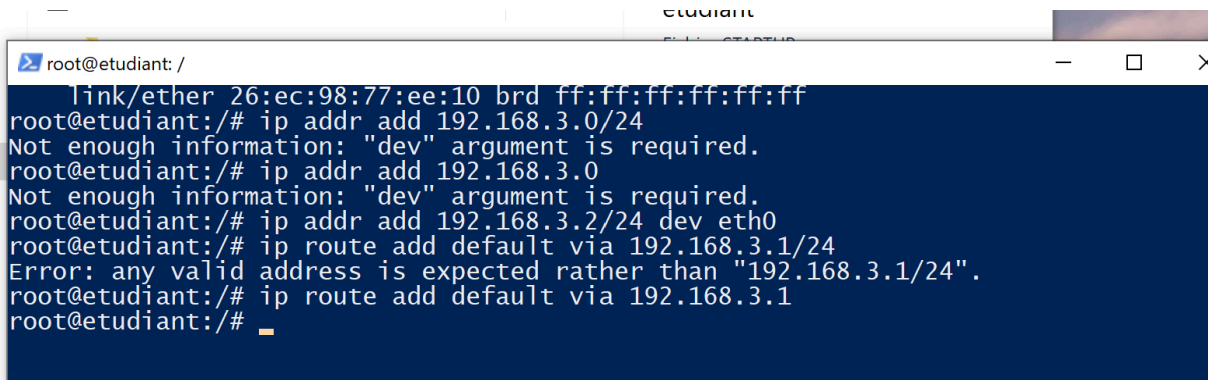
TP n°2 : Sécurisation d'un réseau et Mails chiffrés avec PGP

Exercice 1 : Résolution des problèmes de configuration réseau de l'étudiant (..... /10 points)**Q°1 – (..... / 4)**

- Etudier les paramètres réseaux de « l'étudiant », en vous plaçant sur sa machine ? Que constatez-vous ? Pourquoi ne peut-il pas discuter avec le routeur ? Justifier.

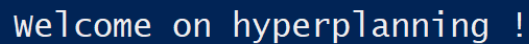
L'interface eth0 est bien active mais elle ne peut pas communiquer avec le routeur. Parceque son adresse IP n'a pas du tout été configurée.

- Résoudre le problème. Intégrer le correctif au fichier « etudiant.startup » afin de pouvoir redémarrer le TP sans risque de perdre votre avancée.



```
root@etudiant: /
link/ether 26:ec:98:77:ee:10 brd ff:ff:ff:ff:ff:ff
root@etudiant: /# ip addr add 192.168.3.0/24
Not enough information: "dev" argument is required.
root@etudiant: /# ip addr add 192.168.3.0
Not enough information: "dev" argument is required.
root@etudiant: /# ip addr add 192.168.3.2/24 dev eth0
root@etudiant: /# ip route add default via 192.168.3.1/24
Error: any valid address is expected rather than "192.168.3.1/24".
root@etudiant: /# ip route add default via 192.168.3.1
root@etudiant: /#
```

- Valider que l'étudiant peut ensuite discuter avec hyperplanning. Pour ce faire, vous utiliserez la commande « links ». Prendre une capture d'écran.



```
welcome on hyperplanning !
```

Q°2 – (..... / 4)

- A présent, tentez de pinguer le « Prof_remote ». Que constatez-vous ? Quel est le problème ?

SÉCURITÉ RÉSEAU – 06/12/2024

TP n°2 : Sécurisation d'un réseau et Mails chiffrés avec PGP

```

+ [2J+ [0;0H--- Startup Commands Log
++ ip addr add 192.168.3.2/24 dev eth0
++ ip route add default via 192.168.3.1
--- End Startup Commands Log
root@etudiant:/# ping 200.200.200.2
PING 200.200.200.2 (200.200.200.2) 56(84) bytes of data.
From 192.168.3.1 icmp_seq=1 Destination Net Unreachable
From 192.168.3.1 icmp_seq=2 Destination Net Unreachable
From 192.168.3.1 icmp_seq=3 Destination Net Unreachable
From 192.168.3.1 icmp_seq=4 Destination Net Unreachable
From 192.168.3.1 icmp_seq=5 Destination Net Unreachable
From 192.168.3.1 icmp_seq=6 Destination Net Unreachable
From 192.168.3.1 icmp_seq=7 Destination Net Unreachable
From 192.168.3.1 icmp_seq=8 Destination Net Unreachable
From 192.168.3.1 icmp_seq=9 Destination Net Unreachable
From 192.168.3.1 icmp_seq=10 Destination Net Unreachable
^C
--- 200.200.200.2 ping statistics ---
10 packets transmitted, 0 received, +10 errors, 100% packet loss, time 9301ms

```

Il y a une erreur "Destination Net unreachable". Elle signifie que le réseau de destination n'est pas accessible. Le problème est lié au routage. Le routeur ne sait pas comment atteindre le réseau auquel est connecté le Prof_remote.

- Régler ce problème sur le « gateway » et/ou l'« etudiant ». Intégrer le correctif au(x) fichier(x) « .startup » associé(s).

```

root@gateway: /
Waiting startup commands execution. Press [ENTER] to override...+ [2J+
++ /etc/init.d/networking restart
Running /etc/init.d/networking restart is deprecated because it may r
Reconfiguring network interfaces...done.
++ ip route add default via 193.193.193.1
--- End Startup Commands Log
root@gateway:/# ping 200.200.200.2
PING 200.200.200.2 (200.200.200.2) 56(84) bytes of data.
64 bytes from 200.200.200.2: icmp_seq=1 ttl=63 time=1.55 ms
64 bytes from 200.200.200.2: icmp_seq=2 ttl=63 time=2.87 ms
64 bytes from 200.200.200.2: icmp_seq=3 ttl=63 time=0.617 ms
64 bytes from 200.200.200.2: icmp_seq=4 ttl=63 time=2.71 ms
64 bytes from 200.200.200.2: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from 200.200.200.2: icmp_seq=6 ttl=63 time=1.68 ms
64 bytes from 200.200.200.2: icmp_seq=7 ttl=63 time=0.972 ms
64 bytes from 200.200.200.2: icmp_seq=8 ttl=63 time=0.580 ms
64 bytes from 200.200.200.2: icmp_seq=9 ttl=63 time=1.06 ms
64 bytes from 200.200.200.2: icmp_seq=10 ttl=63 time=10.7 ms
64 bytes from 200.200.200.2: icmp_seq=11 ttl=63 time=1.99 ms
64 bytes from 200.200.200.2: icmp_seq=12 ttl=63 time=1.78 ms
^C
--- 200.200.200.2 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11059ms
rtt min/avg/max/mdev = 0.580/2.318/10.667/2.611 ms
root@gateway:/#

```

SÉCURITÉ RÉSEAU – 06/12/2024

TP n°2 : Sécurisation d'un réseau et Mails chiffrés avec PGP

Q°3 – (..... / 2)

- Configurer le fichier « /etc/hosts » local de l'« étudiant » pour lui permettre d'accéder au serveur hyperplanning sans taper l'adresse IP. Le nom de domaine du serveur retenu est hyperplanning.intranet. Vérifiez que vous êtes en mesure d'utiliser cette configuration via le navigateur links. Intégrer l'ajout dans le dossier de l'étudiant pour garder en mémoire la configuration

<mettre une capture ou le code de la configuration proposée>

Exercice 2 : Configuration simple du firewall iptables (..... / 10 points)

Remarque : Lors d'opérations sur un firewall, il est conseillé d'observer les flux réseaux (par exemple avec tcpdump, similaire à wireshark) ainsi que de profiter des propriétés du ping.

Q°1 – (..... / 3)

- Déployer une politique de sécurité stricte au niveau de la « gateway » afin de bloquer l'ensemble des échanges entre les différents réseaux et sous-réseaux. Vous pouvez valider votre opération en essayant de pinguer depuis les différentes zones, les autres zones.

```
gateway > opt > $ iptables.sh
1  iptables -F
2  iptables -t nat -F
3  iptables -t mangle -F
4  iptables -P INPUT DROP
5  iptables -P FORWARD DROP
6  iptables -P OUTPUT DROP
```

- Etes-vous tout de même en mesure de pinguer le serveur DNS depuis le serveur Web dans la DMZ pourquoi ?

Oui, parcequ'elles sont sur le même sous-réseau, parce que les paquets n'ont pas besoin de passer par le gateway.

- Pour vous faciliter la vie, il est recommandé de créer un script « iptables.sh » sous le /opt de la gateway directement via les dossiers kathara dans lequel vous en profiterez pour ajouter les commandes suivantes, qui permettent de nettoyer la table :
 - o Iptables -F
 - o Iptables -t nat -F
 - o Iptables -t mangle -F

N'hésitez pas à solliciter l'aide du responsable du TP sur cette manipulation.

Q°2 – (..... / 3)

SÉCURITÉ RÉSEAU – 06/12/2024

TP n°2 : Sécurisation d'un réseau et Mails chiffrés avec PGP

- Ajouter une première règle permettant aux étudiants d'accéder aux interfaces du routeur, tout en garantissant que la DMZ n'y a pas accès.

```
gateway > opt > $ iptables.sh
1 iptables -F
2 iptables -t nat -F
3 iptables -t mangle -F
4 iptables -P INPUT DROP
5 iptables -P FORWARD DROP
6 iptables -P OUTPUT DROP
```

```
root@etudiant: /
-[2]-[0;0H--- Startup Commands Log
++ ip addr add 192.168.3.2/24 dev eth0
++ ip route add default via 192.168.3.1
--- End Startup Commands Log
root@etudiant: /# ping 192.168.3.1
PING 192.168.3.1 (192.168.3.1) 56(84) bytes of data.
64 bytes from 192.168.3.1: icmp_seq=1 ttl=64 time=10.8 ms
64 bytes from 192.168.3.1: icmp_seq=2 ttl=64 time=0.369 ms
64 bytes from 192.168.3.1: icmp_seq=3 ttl=64 time=0.312 ms
64 bytes from 192.168.3.1: icmp_seq=4 ttl=64 time=0.402 ms
^C
--- 192.168.3.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3106ms
rtt min/avg/max/mdev = 0.312/2.981/10.842/4.538 ms
```

```
root@dmz_web: /
-[2]-[0;0H--- Startup Commands Log
++ /etc/init.d/networking restart
Running /etc/init.d/networking restart is deprecated because it may not re-enable some interfaces ... (warning).
Reconfiguring network interfaces...done.
++ /etc/init.d/apache2 start
Starting Apache httpd web server: apache2AH00557: apache2: apr_sockaddr_info_get() failed for dmz_web
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.0.1. Set the 'ServerName' directive globally to suppress this message
--- End Startup Commands Log
root@dmz_web: /# ping 192.168.3.2
PING 192.168.3.2 (192.168.3.2) 56(84) bytes of data.
^C
--- 192.168.3.2 ping statistics ---
8 packets transmitted, 0 received, 100% packet loss, time 7320ms
```

```
root@dmz_dns: /
-[2]-[0;0H--- Startup Commands Log
++ /etc/init.d/networking restart
Running /etc/init.d/networking restart is deprecated because it may not re-enable some interfaces ... (warning).
Reconfiguring network interfaces...done.
++ /etc/init.d/bind start
Starting domain name service...: named.
--- End Startup Commands Log
root@dmz_dns: /# ping 192.168.3.2
PING 192.168.3.2 (192.168.3.2) 56(84) bytes of data.
^C
--- 192.168.3.2 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1082ms
```

Q°3 – (..... / 4)

- Ajouter une règle afin de permettre aux étudiants d'accéder au serveur hyperplanning, tout en maintenant le ping bloqué

```
11
12 iptables -A FORWARD -s 192.168.3.0/24 -d 192.168.2.2 -j ACCEPT
13 iptables -A FORWARD -s 192.168.2.2 -d 192.168.3.0/24 -j ACCEPT
14 iptables -I FORWARD -s 192.168.3.0/24 -d 192.168.2.2 -p icmp --icmp-type 8 -j DRO
15
```

SÉCURITÉ RÉSEAU – 06/12/2024

TP n°2 : Sécurisation d'un réseau et Mails chiffrés avec PGP

```

←[2J←[O;0H--- Startup Commands Log
++ ip addr add 192.168.3.2/24 dev eth0
++ ip route add default via 192.168.3.1
--- End Startup Commands Log
root@etudiant:/# ping 192.168.2.2
PING 192.168.2.2 (192.168.2.2) 56(84) bytes of data.
^C
--- 192.168.2.2 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4141ms

root@etudiant:/# links 192.168.2.2
root@etudiant:/# curl 192.168.2.2
<html><body><h1>Welcome on hyperplanning !</h1></body></html>
root@etudiant:/#

```

Exercice 3 : Configuration des accès Internet et de la DMZ (..... / 10 points)**Q°1 – (..... / 5)**

- Autoriser les étudiants à accéder au site web public, tout en étant routé grâce à une adresse publique en sortie de la « gateway ». Quel mécanisme devons-nous mettre en place ?

Le mécanisme à mettre en place est le NAT

- Mettre en place ce mécanisme en appliquant une politique sur le firewall

```

iptables -t nat -A POSTROUTING -s 192.168.3.0/24 -d 100.100.100.3 -o eth0 -j MASQUERADE
iptables -A FORWARD -s 192.168.3.0/24 -d 100.100.100.3 -j ACCEPT
iptables -A FORWARD -s 100.100.100.3 -d 192.168.3.0/24 -j ACCEPT

```

```

root@etudiant:/# curl 100.100.100.3
<html><body><h1>Hello ! (Serveur Web Public)</h1></body></html>
root@etudiant:/# █

```

SÉCURITÉ RÉSEAU – 06/12/2024

TP n°2 : Sécurisation d'un réseau et Mails chiffrés avec PGP

```

root@public_web: /
-[2J-[0;0H--- Startup Commands Log
++ /etc/init.d/networking restart
Running /etc/init.d/networking restart is deprecated because it may not re-enable some interfaces ... (warning).
Reconfiguring network interfaces...done.
++ /etc/init.d/apache2 start
Starting Apache httpd web server: apache2AH00557: apache2: apr_sockaddr_info_get() failed for public_web
AH00558: apache2: could not reliably determine the server's fully qualified domain name, using 127.0.0.1. Set the 'ServerName' directive globally to suppress this message
.
--- End Startup Commands Log
root@public_web:/# tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
23:33:56.160231 ARP, Request who-has 100.100.100.3 tell 100.100.100.1, length 46
23:33:56.160242 ARP, Reply 100.100.100.3 is-at a6:73:5d:c3:81:bd (oui unknown), length 28
23:33:56.160706 IP 193.193.193.2.46850 > 100.100.100.3.http: Flags [S], seq 1809639111, win 64240, options [mss 1460,sackOK,TS val 605857250 ecr 0,nop,wscale 7], length 0
23:33:56.160748 IP 100.100.100.3.http > 193.193.193.2.46850: Flags [S.], seq 2503149912, ack 1809639112, win 65160, options [mss 1460,sackOK,TS val 1100292364 ecr 605857250,nop,wscale 7], length 0
23:33:56.161604 IP 193.193.193.2.46850 > 100.100.100.3.http: Flags [.] , ack 1, win 502, options [nop,nop,TS val 605857252 ecr 1100292364], length 0
23:33:56.161849 IP 193.193.193.2.46850 > 100.100.100.3.http: Flags [P.], seq 1:78, ack 1, win 502, options [nop,nop,TS val 605857252 ecr 1100292364], length 77: HTTP: GET / HTTP/1.1
23:33:56.161878 IP 100.100.100.3.http > 193.193.193.2.46850: Flags [.] , ack 78, win 509, options [nop,nop,TS val 1100292365 ecr 605857252], length 0
23:33:56.162640 IP 100.100.100.3.http > 193.193.193.2.46850: Flags [P.], seq 1:292, ack 78, win 509, options [nop,nop,TS val 1100292366 ecr 605857252], length 291: HTTP: HTTP/1.1 200 OK
23:33:56.164100 IP 193.193.193.2.46850 > 100.100.100.3.http: Flags [.] , ack 292, win 501, options [nop,nop,TS val 605857254 ecr 1100292366], length 0
23:33:56.164335 IP 193.193.193.2.46850 > 100.100.100.3.http: Flags [F.], seq 78, ack 292, win 501, options [nop,nop,TS val 605857255 ecr 1100292366], length 0
23:33:56.164554 IP 100.100.100.3.http > 193.193.193.2.46850: Flags [F.], seq 292, ack 79, win 509, options [nop,nop,TS val 1100292368 ecr 605857255], length 0
23:33:56.165650 IP 193.193.193.2.46850 > 100.100.100.3.http: Flags [.] , ack 293, win 501, options [nop,nop,TS val 605857256 ecr 1100292368], length 0
23:34:01.153740 ARP, Request who-has 100.100.100.1 tell 100.100.100.3, length 28
23:34:01.154061 ARP, Reply 100.100.100.1 is-at 9e:70:74:f6:f5:06 (oui unknown), length 46
AC
14 packets captured
14 packets received by filter
0 packets dropped by kernel
root@public_web:/#

```

Q°2 – (..... /5)

- Exposer le site Web de la DMZ avec une adresse IP publique afin d'en offrir l'accès aux « clients » sur Internet.

```

iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to-destination 192.168.1.2:80
iptables -A FORWARD -p tcp -s 100.100.100.2 --dport 80 -j ACCEPT
iptables -A FORWARD -p tcp -d 192.168.1.2 --dport 80 -j ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

```

```

root@client: /
-[2J-[0;0H--- Startup Commands Log
++ /etc/init.d/networking restart
Running /etc/init.d/networking restart is deprecated because it may not re-enable some interfaces ... (warning).
Reconfiguring network interfaces...done.
--- End Startup Commands Log
root@client:/# curl http://192.168.1.2
<html><body><h1>Hello ! (Serveur DMZ)</h1></body></html>

```


Nom :

Prénom :

SÉCURITÉ RÉSEAU – 06/12/2024

TP n°2 : Sécurisation d'un réseau et Mails chiffrés avec PGP

```
root@dmz_web: /
+---[0:0H-- Startup Commands Log
++ /etc/init.d/networking restart
Running /etc/init.d/networking restart is deprecated because it may not re-enable some interfaces ... (warning).
Reconfiguring network interfaces...done.
++ /etc/init.d/apache2 start
Starting Apache httpd web server: apache2AH00557: apache2: apr_sockaddr_info_get() failed for dmz_web
AH00558: apache2: could not reliably determine the server's fully qualified domain name, using 127.0.0.1. Set the 'ServerName' directive globally to suppress this message
'
--- End Startup Commands Log
root@dmz_web: /# tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
13:46:01.930457 ARP, Request who-has 192.168.1.2 tell 192.168.1.1, length 46
13:46:01.930470 ARP, Reply 192.168.1.2 is-at 66:cc:b3:a1:5c:ac (oui unknown), length 28
13:46:01.930758 IP 100.100.100.2.35128 > 192.168.1.2.http: Flags [S], seq 2718504871, win 64240, options [mss 1460,sackOK,TS val 1468900415,ecn 0,nop,wscale 7], length 0
13:46:01.930817 IP 192.168.1.2.http > 100.100.100.2.35128: Flags [S.], seq 1527205510, ack 2718504872, win 65160, options [mss 1460,sackOK,TS val 2781267790,ecn 1468900415,nop,wscale 7], length 0
13:46:01.932086 IP 100.100.100.2.35128 > 192.168.1.2.http: Flags [L.], ack 1, win 502, options [nop,nop,TS val 1468900418,ecn 2781267790], length 0
13:46:01.932229 IP 100.100.100.2.35128 > 192.168.1.2.http: Flags [P.], seq 1:76, ack 1, win 502, options [nop,nop,TS val 1468900418,ecn 2781267790], length 75: HTTP: GET / HTTP/1.1
13:46:01.932257 IP 192.168.1.2.http > 100.100.100.2.35128: Flags [L.], ack 76, win 509, options [nop,nop,TS val 2781267791,ecn 1468900418], length 0
13:46:01.933319 IP 192.168.1.2.http > 100.100.100.2.35128: Flags [P.], seq 1:285, ack 76, win 509, options [nop,nop,TS val 2781267792,ecn 1468900418], length 284: HTTP: HTTP/1.1 200 OK
13:46:01.934487 IP 100.100.100.2.35128 > 192.168.1.2.http: Flags [L.], ack 285, win 501, options [nop,nop,TS val 1468900421,ecn 1468900421], length 0
13:46:01.934911 IP 100.100.100.2.35128 > 192.168.1.2.http: Flags [F.], seq 76, ack 285, win 501, options [nop,nop,TS val 1468900421,ecn 2781267794], length 0
13:46:01.935255 IP 192.168.1.2.http > 100.100.100.2.35128: Flags [F.], seq 285, ack 77, win 509, options [nop,nop,TS val 2781267794,ecn 1468900421], length 0
13:46:01.936331 IP 100.100.100.2.35128 > 192.168.1.2.http: Flags [L.], ack 286, win 501, options [nop,nop,TS val 1468900423,ecn 2781267794], length 0
```


Nom :

Prénom :

SÉCURITÉ RÉSEAU – 06/12/2024

TP n°2 : Sécurisation d'un réseau et Mails chiffrés avec PGP

Exercice 4 : Chiffrement d'emails (..... / 10 points)

Mettre en place le chiffrement PGP sur votre outil de lecture de courriel (il faut impérativement un client lourd car le client webbrowser Hexagone ne marche pas avec PGP) et envoyer votre TP par mail chiffré.

Nom :

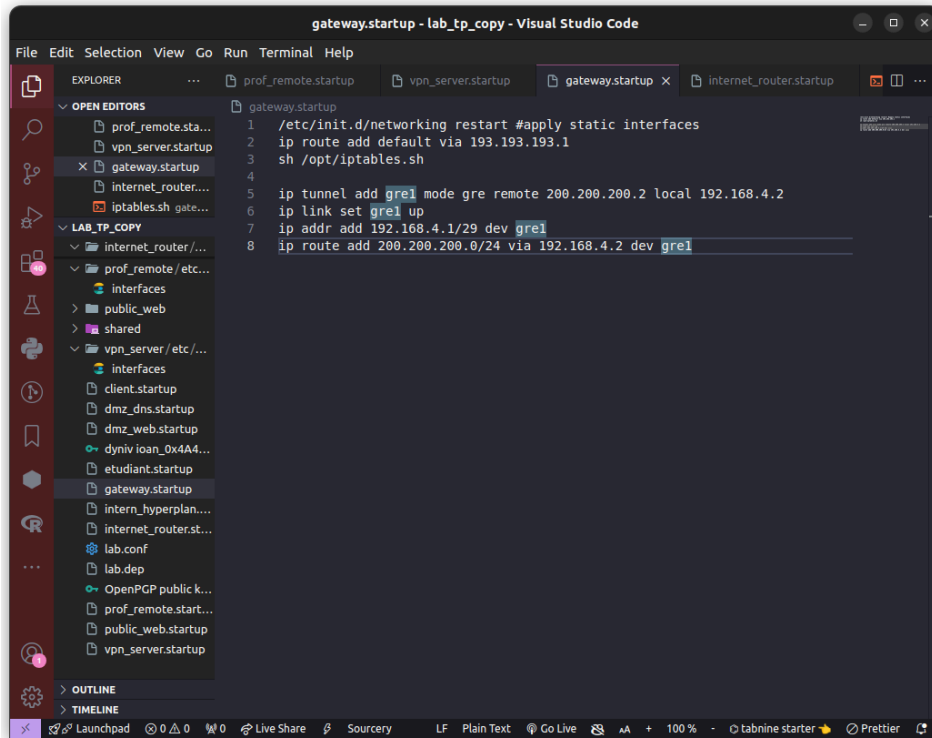
Prénom :

SÉCURITÉ RÉSEAU – 06/12/2024

TP n°2 : Sécurisation d'un réseau et Mails chiffrés avec PGP

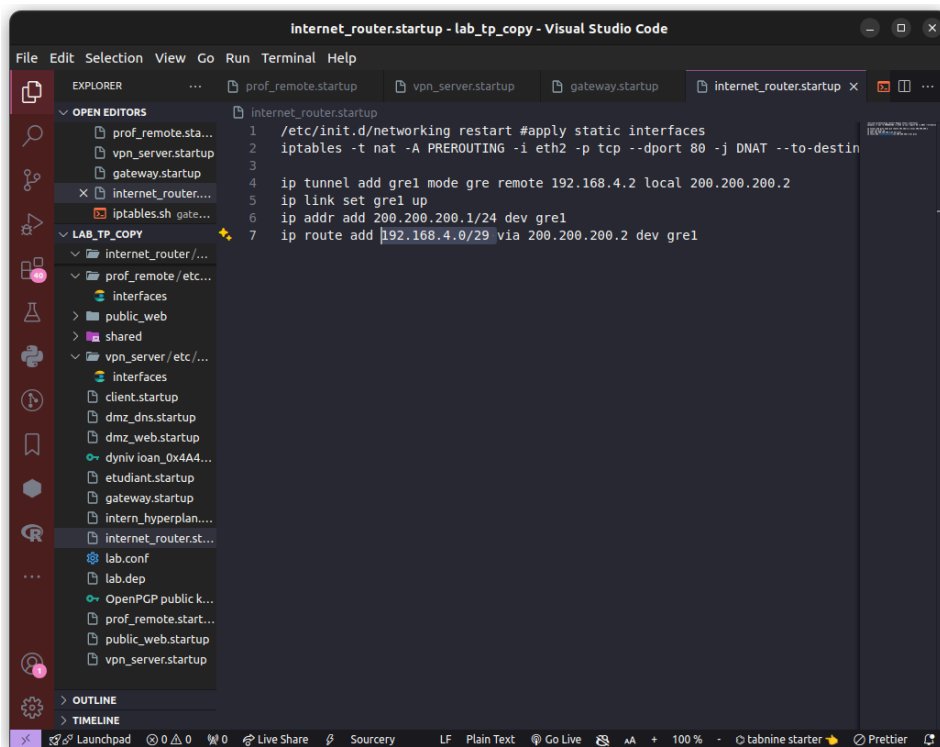
Exercice Bonus : Tunnel IP (..... / 10 points)

Réaliser un tunnel IP entre le serveur du professeur en remote et le serveur VPN grâce à la commande « ip tunnel ». Ne vous préoccupez pas du problème de chiffrement



```
gateway.startup - lab_tp_copy - Visual Studio Code
File Edit Selection View Go Run Terminal Help
EXPLORER
  OPEN EDITORS
    prof_remote.startup
    vpn_server.startup
    gateway.startup X
    internet_router.startup
    iptables.sh gate...
  LAB_TP_COPY
    internet_router/...
    prof_remote/etc/...
      interfaces
      public_web
      shared
    vpn_server/etc/...
      interfaces
      client.startup
      dmz_dns.startup
      dmz_web.startup
      dyniv ioan_0x4A4...
      etudiant.startup
      gateway.startup
      intern_hyperplan...
      internet_router.st...
      lab.conf
      lab.dep
      OpenPGP public k...
      prof_remote.start...
      public_web.startup
      vpn_server.startup
    OUTLINE
    TIMELINE
  Launchpad 0 0 0 0 Live Share Sourcery LF Plain Text Go Live 100% tabnine starter Prettier
```

```
1 /etc/init.d/networking restart #apply static interfaces
2 ip route add default via 193.193.193.1
3 sh /opt/iptables.sh
4
5 ip tunnel add gre1 mode gre remote 200.200.200.2 local 192.168.4.2
6 ip link set gre1 up
7 ip addr add 192.168.4.1/29 dev gre1
8 ip route add 200.200.200.0/24 via 192.168.4.2 dev gre1
```



```
internet_router.startup - lab_tp_copy - Visual Studio Code
File Edit Selection View Go Run Terminal Help
EXPLORER
  OPEN EDITORS
    prof_remote.startup
    vpn_server.startup
    gateway.startup
    internet_router.startup X
    iptables.sh gate...
  LAB_TP_COPY
    internet_router/...
    prof_remote/etc/...
      interfaces
      public_web
      shared
    vpn_server/etc/...
      interfaces
      client.startup
      dmz_dns.startup
      dmz_web.startup
      dyniv ioan_0x4A4...
      etudiant.startup
      gateway.startup
      intern_hyperplan...
      internet_router.st...
      lab.conf
      lab.dep
      OpenPGP public k...
      prof_remote.start...
      public_web.startup
      vpn_server.startup
    OUTLINE
    TIMELINE
  Launchpad 0 0 0 0 Live Share Sourcery LF Plain Text Go Live 100% tabnine starter Prettier
```

```
1 /etc/init.d/networking restart #apply static interfaces
2 iptables -t nat -A PREROUTING -i eth2 -p tcp --dport 80 -j DNAT --to-destin
3
4 ip tunnel add gre1 mode gre remote 192.168.4.2 local 200.200.200.2
5 ip link set gre1 up
6 ip addr add 200.200.200.1/24 dev gre1
7 ip route add 192.168.4.0/29 via 200.200.200.2 dev gre1
```

SÉCURITÉ RÉSEAU – 06/12/2024

TP n°2 : Sécurisation d'un réseau et Mails chiffrés avec PGP

Annexe 1 : Présentation de kathara

Kathara est un système d'émulation de réseau Open-Source basé sur des conteneurs permettant de présenter des démonstrations/leçons interactives, de tester des réseaux de production dans un environnement « sandbox » ou de développer de nouveaux protocoles de réseau.

Il utilise docker et un système de simplification d'architectures réseaux. Vous retrouverez plus d'informations sur <https://www.kathara.org/>.

- Lancer une configuration (« un lab ») kathara (Attention : il faut être placé dans le dossier du lab)

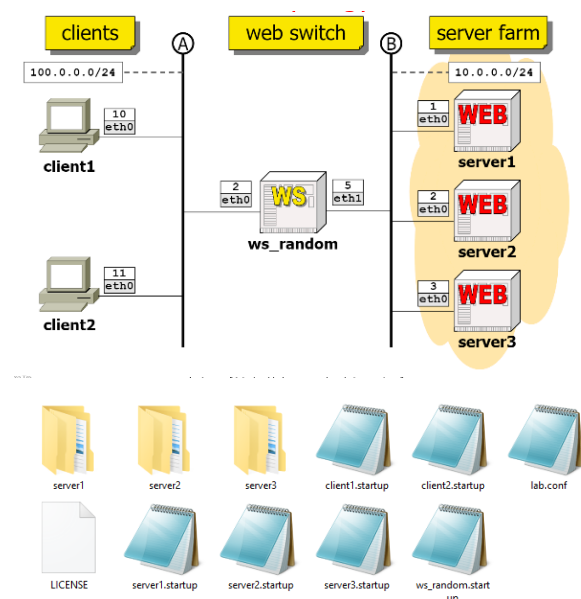
```
kathara Lstart
```

- Stopper une configuration (« un lab ») kathara (Attention : il faut être placé dans le dossier du lab)

```
kathara Lclean
```

- Présentation d'un lab kathara ou une configuration réseau

Ci-dessous, l'architecture du lab considéré et l'arborescence de sa représentation définie dans kathara.



On observe différents fichiers et dossiers. Ils représentent :

- *lab.conf* : L'architecture du réseau (attention, il ne définit pas les adresses IPs)

SÉCURITÉ RÉSEAU – 06/12/2024

TP n°2 : Sécurisation d'un réseau et Mails chiffrés avec PGP

```

client1[0]=A

client2[0]=A

ws_random[0]=A
ws_random[1]=B

server1[0]=B

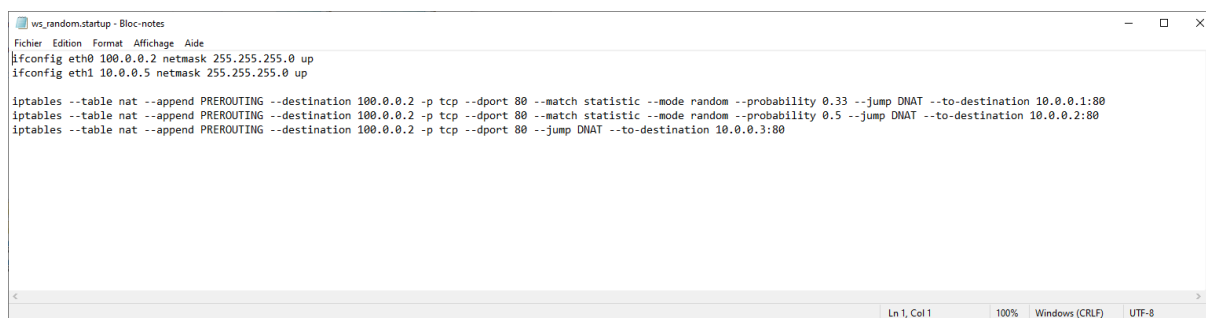
server2[0]=B

server3[0]=B

```

Sur l'exemple, client1 et client2 partagent un même réseau(A), les serveurs également(B) et ws_random fait le lien.

- ***.startup** : Les commandes lancées au démarrage de la machine considérée



```

ws_random.startup - Bloc-notes
Fichier Edition Format Affichage Aide
ifconfig eth0 100.0.0.2 netmask 255.255.255.0 up
ifconfig eth1 10.0.0.5 netmask 255.255.255.0 up

iptables --table nat --append PREROUTING --destination 100.0.0.2 -p tcp --dport 80 --match statistic --mode random --probability 0.33 --jump DNAT --to-destination 10.0.0.1:80
iptables --table nat --append PREROUTING --destination 100.0.0.2 -p tcp --dport 80 --match statistic --mode random --probability 0.5 --jump DNAT --to-destination 10.0.0.2:80
iptables --table nat --append PREROUTING --destination 100.0.0.2 -p tcp --dport 80 --jump DNAT --to-destination 10.0.0.3:80

```

Sur l'exemple, le routeur configure différentes interfaces et appliquent des règles iptables.

- **<dossier_machinename>** : Ces dossiers permettent d'intégrer des scripts et/ou logiciels sur la machine considérées en respectant le chemin d'accès du dossier

Par exemple, pour un serveur Web apache2, on aura un fichier dans /var/www/html/index.html

```

public_web/var:
www

public_web/var/www:
apache2-default html rfc2616.txt

public_web/var/www/apache2-default:
index.html

public_web/var/www/html:
index.html

```

Attention le nommage des dossiers et fichiers startup doit impérativement respecter les noms utilisés dans le fichier *lab.conf*.

Nom :

Prénom :

SÉCURITÉ RÉSEAU – 06/12/2024

TP n°2 : Sécurisation d'un réseau et Mails chiffrés avec PGP

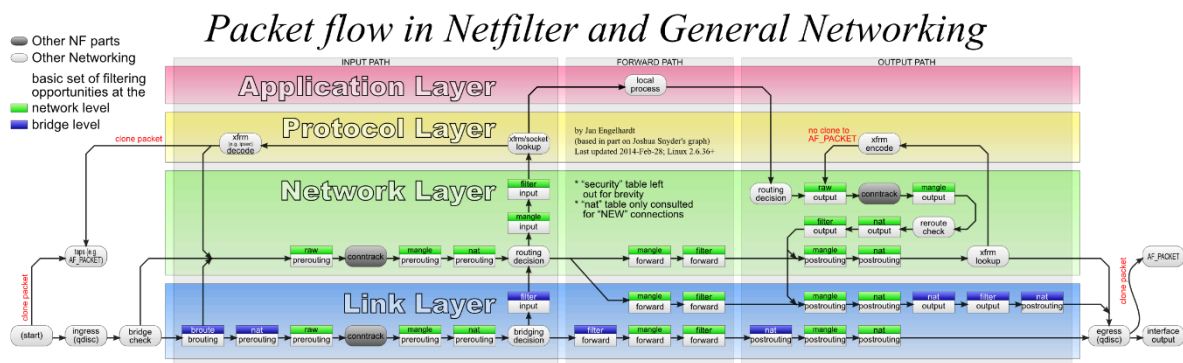
Annexe 2 : Présentation de iptables

iptables est un logiciel libre de l'espace utilisateur Linux grâce auquel l'administrateur système peut configurer les chaînes et règles dans le pare-feu en espace noyau (et qui est composé par des modules Netfilter).

- Fonctionnement

iptables permet à l'administrateur système de créer des tableaux, lesquels contiennent des « chaînes », elles-mêmes composées d'un ensemble de règles de traitement des paquets. Chaque tableau est associé à un type de traitement des paquets (cf. schéma netfilter). Les paquets suivent séquentiellement chaque règle des chaînes. Une règle dans une chaîne peut provoquer un saut à une autre chaîne (goto ou jump), et ce processus peut être renouvelé autant qu'il le faut, quel que soit le niveau d'imbrication atteint.

Chaque paquet réseau, entrant ou sortant, traverse donc au moins une chaîne.



L'origine du paquet détermine la première chaîne qu'il traverse. Il existe cinq chaînes prédéfinies (associées aux cinq hooks de Netfilter), cependant leur utilisation n'est pas obligatoire dans chaque tableau.

Chacune des chaînes prédéfinies ont une politique (par exemple DROP), qui est appliquée au paquet s'il arrive à la fin de la chaîne. L'administrateur système peut créer autant d'autres chaînes qu'il le souhaite. Ces chaînes n'ont pas de politique : si un paquet arrive à la fin de la chaîne, il est renvoyé à la chaîne qui a appelé. Une chaîne peut même être vide (n'avoir aucune règle).

Les cinq types de chaînes prédéfinies sont les suivants :

- **"PREROUTING"** : Les paquets vont entrer dans cette chaîne avant qu'une décision de routage ne soit prise.
- **"INPUT"** : Le paquet va être livré sur place (N.B. : la livraison sur place ne dépend pas d'un processus ayant un socket ouvert ; la livraison est contrôlée par le tableau « local » de routage : `ip route show table local`).
- **"FORWARD"** : Tous les paquets qui ont été acheminés et ne sont pas livrés sur place parcourent la chaîne.
- **"OUTPUT"** : Les paquets envoyés à partir de la machine elle-même se rendront à cette chaîne.
- **"POSTROUTING"** : La décision de routage a été prise. Les paquets entrent dans cette chaîne, juste avant qu'ils ne soient transmis vers le matériel.

SÉCURITÉ RÉSEAU – 06/12/2024

TP n°2 : Sécurisation d'un réseau et Mails chiffrés avec PGP

Une chaîne (qui est une liste de règles) n'existe pas de façon indépendante : toute chaîne appartient nécessairement à une table. Iptables comprend quatre tables nommées : **mangle**, **filter**, **nat**, **raw**. Cet aspect est souvent mal expliqué (ou peu mis en exergue) dans les tutoriaux qui de ce fait laissent penser qu'il existe des chaînes en dehors des tables. Cette confusion vient du fait que la table **filter** est la table par défaut. Ainsi elle est souvent implicite dans les commandes et le discours. Par exemple lorsqu'un tutoriel parle de la chaîne **INPUT** sans autre précision il s'agit donc de la chaîne **INPUT** de la table **filter**. Ci-dessous nous indiquons des commandes pour lister les chaînes définies dans les différentes tables.

```
# liste en mode tableau de la table filter
```

```
iptables -L
```

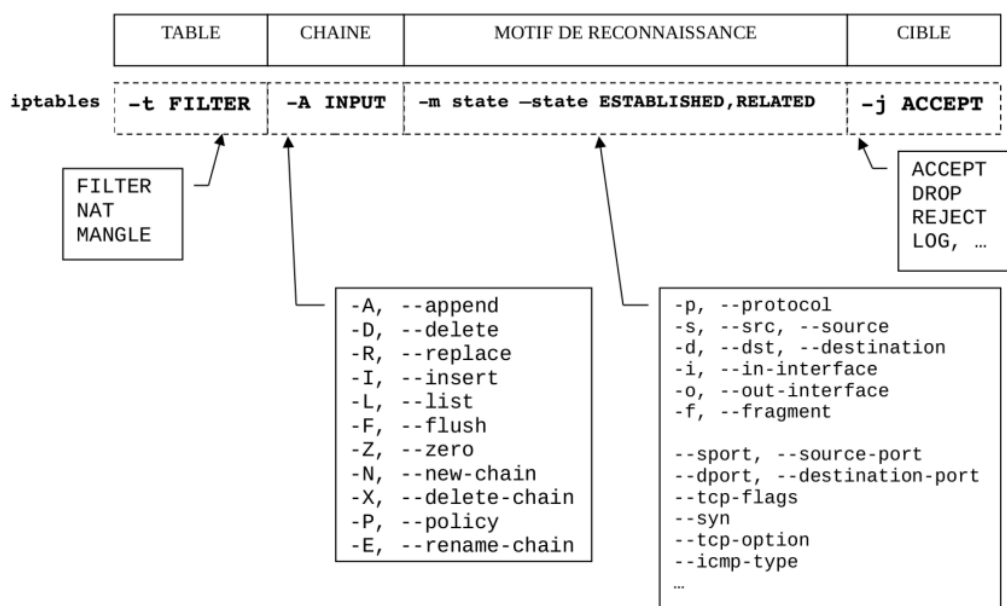
```
# liste en mode rules de la table filter
```

```
iptables -S
```

```
# liste en mode rules/tableau de la chaîne précisée (mangle, nat, raw)
```

```
iptables -t <table_name> -L/-S
```

Chaque règle d'une chaîne contient la spécification (en anglais : **matches**) des paquets qui lui correspondent. Elle peut également contenir une action (en anglais : **target**) (utilisée pour les extensions) ou un jugement (une de plusieurs décisions intégrées). Quand un paquet traverse une chaîne, chaque règle, à son tour, est examinée. Si une règle ne correspond pas au paquet, le paquet est passé à la règle suivante. Si une règle correspond au paquet, elle prend les mesures indiquées par l'action/le jugement, ce qui peut conduire à autoriser le paquet à continuer dans la chaîne ou, à l'inverse, à l'exclure. Les spécifications constituent la grande partie des règles, car elles contiennent les conditions selon lesquelles les paquets sont testés. Ces spécifications peuvent fournir pour toute couche du modèle OSI, comme par exemple les paramètres `--mac-source` et `-p tcp --dport`, et il y a aussi des spécifications indépendantes du protocole, par exemple `-m time`. Ci-dessous une liste non exhaustive d'exemples de commandes et la logique de l'outil :



SÉCURITÉ RÉSEAU – 06/12/2024

TP n°2 : Sécurisation d'un réseau et Mails chiffrés avec PGP

```
# Interdire tout ce qui sort sur l'interface eth0
iptables -A OUTPUT -o eth0 -j DROP

# Interdire tout ce qui rentre du réseau
iptables -A INPUT -s 0/0 -j DROP

# Interdire toutes les requêtes echo (ping)
iptables -A INPUT -p icmp -icmp-type 8 -j DROP

# Interdire toutes les réponses echo (ping)
iptables -A INPUT -p icmp -icmp-type 0 -j DROP

# Interdire l'accès au serveur web du réseau 192.168.1.0
iptables -A INPUT -p TCP -d 192.168.1.0/24 -dport http -j DROP

# Initialiser une politique de sécurité stricte
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP

# Vider ("flusher") toutes les règles existantes
iptables -F
iptables -t nat -F
iptables -t mangle -F

# Ajouter une règle dans la table de translation d'adresses NAT du routeur
qui opère après la décision de routage (postrouting) et qui masque
(masquerade) le trafic provenant du réseau 10.2.0.0 et à destination du
réseau 10.3.0.0. Ce dernier voit le trafic sortant de l'interface eth2
comme provenant uniquement du routeur
iptables -t nat -A POSTROUTING -s 10.2.0.0/16 -d 10.3.0.0/16 -o eth2 -j
MASQUERADE

# Autoriser tous les paquets qui ont une communication déjà établie
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

# Rendre accessible un serveur tcp 80 sur un LAN sous une adresse IP
publique grâce à la translation de port
iptables -t nat -A PREROUTING -i <interface_internet> -p tcp -dport 80 -j
DNAT --to-destination <local_ip :local_port>
```

Nom :

Prénom :

SÉCURITÉ RÉSEAU – 06/12/2024

TP n°2 : Sécurisation d'un réseau et Mails chiffrés avec PGP

Annexe 3 : Création de clés PGP et envoi de mails chiffrés via Outlook ou Thunderbird

- *Manipulation sous Outlook et Windows*

Suivre le tutoriel <https://docs.nitrokey.com/fr/pro/windows/openpgp-outlook.html>

- *Manipulation sous Thunderbird et Linux (attention, il n'est plus nécessaire d'utiliser enigmail dans les dernières versions de thunderbird, c'est embarqué directement.*

Suivre le tutoriel <https://support.mozilla.org/fr/kb/signature-numerique-et-chiffrement-des-messages>

-