Natage des partitions secoures et réseau local

Table of Contents

Le test de basculement réseau du 9 aout 2022 des partitions ATLAS (VIPA 10.37.219.10) et LATLAS (VIPA 10.37.218.110) a échoué.

Les partitions sont joignables de l'extérieur mais les flux internes (à l'exception du ping) échouent.

Natage des adresses de destination

Seules les adresses de destination sont natées par les ASA en adresses connues par le site de secours (10.103.218.110 et 10.103.219.10).

Ainsi un client qui veut de se connecter à LATLAS (10.37.218.110) arrive en entrée du fédérateur du SNS avec cette adresse de destination, les ASAs Modifient cette adresse en 10.103.218.110 et c'est la VM LATLAS hébergée au SNS qui répond et le client recevra le flux en retour avec l'adresse source 10.37.218.110.

Les règles de natages déclarées dans les ASA ne considère que les flux outside,inside (les flux provenant de l'intérieur ne sont pas considérés):

```
nat (outside,inside) source static any any destination static MRS-218
MRS-218
nat (outside,inside) source static any any destination static MRS-219
MRS-219
nat (outside,inside) source static any any destination static TRS-218
MRS-218
nat (outside,inside) source static any any destination static TRS-219
MRS-219
```

Lorsqu'on décompose chaque clause de la commande nat ... sur une ligne distincte:

```
nat (outside,inside)
```

```
source static any any
destination static MRS-21x MRS-21x
```

On peut traduire les actions ainsi :

- Lorsque le trafic outside correspond:
  - une source (client) any
  - une destination (serveur) 10.103.210.0/24
- Envoyer à inside et translater
- la source (client) en any (ne rien faire)
- la destination (serveur) en utilisant une traduction statique en 10.103.21x.0/24

Si la destination du flux est 10.103.21x.xxx (adresses du Z de Marseille) on ne fait rien

```
nat (outside,inside)
source static any any
destination static TRS-21x MRS-21x
```

On peut traduire les actions ainsi :

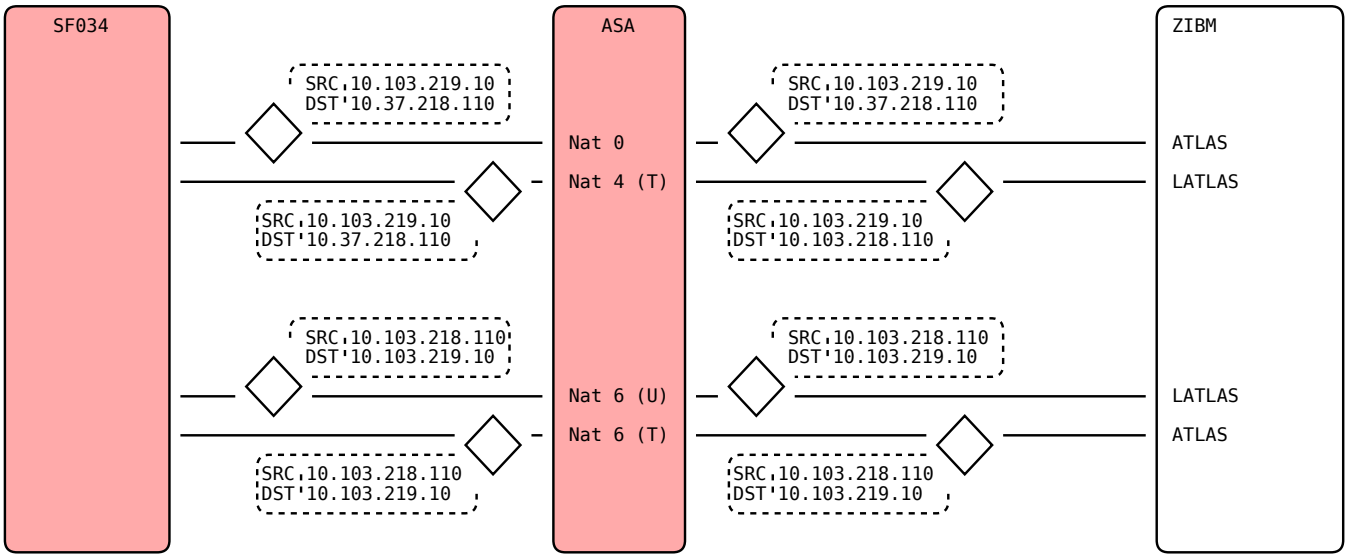
- Lorsque le trafic outside correspond:
  - une source (client) any
  - une destination (serveur) 10.37.21x.0/24
- Envoyer à inside et translater
  - la source (client) en any (ne rien faire)
  - la destination (serveur) en utilisant une traduction statique en 10.103.21x.0/24

Si la destination est 10.37.21x.xxx celle ci est modifiée en 10.103.21x.xxx

Dans le cas étudié le flux est initié par la partition hébergée l'adresse source est l'adresse de la partition au SNS (10.103.21x.xxx) et l'adresse de destination est l'adresse de la partition à TOURS (10.37.21y.yyy)

L'adresse de destination étant inconnue du réseau local le flux est envoyé au fédérateur qui le redirige vers le coeur de réseau du Backup. En traversant les ASA l'adresse de destination est transformée en 10.103.21y.yyy est c'est la partition à Marseille qui reçoit la demande.

```
3 nat (outside,inside) source static any any destination static MRS-218 MRS-218
4 nat (outside,inside) source static any any destination static TRS-218 MRS-218
5 nat (outside,inside) source static any any destination static MRS-219 MRS-219
6 nat (outside,inside) source static any any destination static TRS-219 MRS-219
```



Les règles de NAT permettent de traduire les adresses de destination.

```
nat: untranslation - outside:10.37.219.10/33443 to
inside:10.103.219.10/33443 (xp:0x25923f80, policy:0x2a0bb910)
nat: untranslation - outside:10.37.219.10/33443 to
inside:10.103.219.10/33443 (xp:0x25923f80, policy:0x2a0bb910)
nat: untranslation - outside:10.37.219.10/33443 to
inside:10.103.219.10/33443 (xp:0x25923f80, policy:0x2a0bb910)
nat: translation - outside:10.103.222.110/50448 to
inside:10.103.222.110/50448 (xp:0x25923e40, policy:0x2a0b8958)
nat: translation - outside:10.103.222.110/50448 to
inside:10.103.222.110/50448 (xp:0x25923e40, policy:0x2a0b8958)
nat: untranslation - outside:10.37.219.10/33443 to
inside:10.103.219.10/33443 (xp:0x25923f80, policy:0x2a0bb910)
nat: untranslation - outside:10.37.219.10/33444 to
inside:10.103.219.10/33444 (xp:0x25923f80, policy:0x2a0bb910)
nat: untranslation - outside:10.37.219.10/33444 to
inside:10.103.219.10/33444 (xp:0x25923f80, policy:0x2a0bb910)
nat: untranslation - outside:10.37.219.10/33444 to
inside:10.103.219.10/33444 (xp:0x25923f80, policy:0x2a0bb910)
nat: translation - outside:10.103.222.110/44306 to
inside:10.103.222.110/44306 (xp:0x25923e40, policy:0x2a0b8958)
nat: translation - outside:10.103.222.110/44306 to
inside:10.103.222.110/44306 (xp:0x25923e40, policy:0x2a0b8958)
```

Cependant les flux d'une partition secourue à destination d'une autre partition secourue échouent (à l'exception du ping):

SSH depuis 10.37.219.10 (ATLAS) vers 10.37.218.110 (LATLAS) KO

```
FOTS2204 ssh: connect to host 10.37.218.110 port 22: EDC8127I Connection
timed out. (errno2=0x76630291)
AT90:TSOSNS1:/u/tsosns1: >
```

Traceroute depuis 10.37.219.10 (ATLAS) vers 10.37.218.110 (LATLAS) KO

```
AT90:TSOSNS1:/u/tsosns1: >traceroute 10.37.218.110
CS V2R3: Traceroute to 10.37.218.110 (10.37.218.110)
Enter ESC character plus C or c to interrupt
1 10.103.222.7 (10.103.222.7)  2 ms  14 ms  1 ms
2 10.103.212.33 (10.103.212.33)  2 ms  0 ms  0 ms
3 LATLAS (10.37.218.110)  2 ms  0 ms  0 ms
4 * * *
```

SSH depuis 10.37.218.110 (LATLAS) vers 10.37.219.10 (ATLAS) KO

```
[root@latlas-foncier ~]# ssh tsosns1@10.37.219.10
ssh: connect to host 10.37.219.10 port 22: Connection timed out
```

Traceroute depuis 10.37.218.110 (LATLAS) vers 10.37.219.10 (ATLAS) KO

```
[root@latlas-foncier ~]# traceroute 10.37.219.10
traceroute to 10.37.219.10 (10.37.219.10), 30 hops max, 60 byte packets
 1  gateway (10.103.222.7)  2.373 ms  2.752 ms  3.150 ms
 2  10.103.212.33 (10.103.212.33)  0.930 ms  1.440 ms  1.905 ms
 3  10.103.212.34 (10.103.212.34)  1.049 ms  1.600 ms  2.075 ms
 4  * * *
```

On note une différence:
* Dans le traceroute de ATLAS vers LATLAS le dernier saut pointe vers l'adresse 10.37.218.110
* Dans le traceroute de LATLAS vesr ATLAS le dernier saut pointe vers le fédérateur

On constate que les adresses utilisés ne correspondent plus à l'adresse du flux d'origine, ainsi à l'origine c'est la partition LATLAS à TOURS que l'on veut contacter, après le passage par les ASAs ce sont les adresses de Marseille qui vont répondre (avec l'adresse source 10.103.21x.xxx).

L'absence de MASQUERADE peut expliquer la difficulté rencontrée, une solution consiste à masquer l'adresse source pour faire croire que c'est une adresse en 10.37.21x qui répond.

Masquerade

Le MASQUERADE consiste à masquer les adresses sources, c'est à dire faire coire que c'est une autre adresse qui répond (en général l'adresse publique).

Par exemple les box internet font du MASQUERADE parceque c'est l'adresse publique de la box qui est présentée comme adresse source et non l'adresse du micro connecté à la box (adresse attribuée en dhcp par la box).

On va essayer de faire quelque chose de similaire en masquant les adresses à l'intérieur du réseau.

Masquerade ATLAS

La règle suivante est ajoutée:

```
nat (inside,outside) 1 source static MRS-219 TRS-219 destination static
TRS-218 MRS-218
```

Lorsqu'on décompose chaque clause de la commande nat ... sur une ligne distincte:

```
nat (inside,outside)
source static MRS-219 TRS-219
destination static TRS-218 MRS-218
```

On peut traduire les actions ainsi :

- Lorsque le trafic inside correspond:
  - une source (client) 10.103.219.xxx
  - une destination (serveur) 10.37.218.xxx
- Envoyer à inside et translater
  - la source (client) en 10.37.219.xxx
  - la destination (serveur) en 10.103.218.xxx

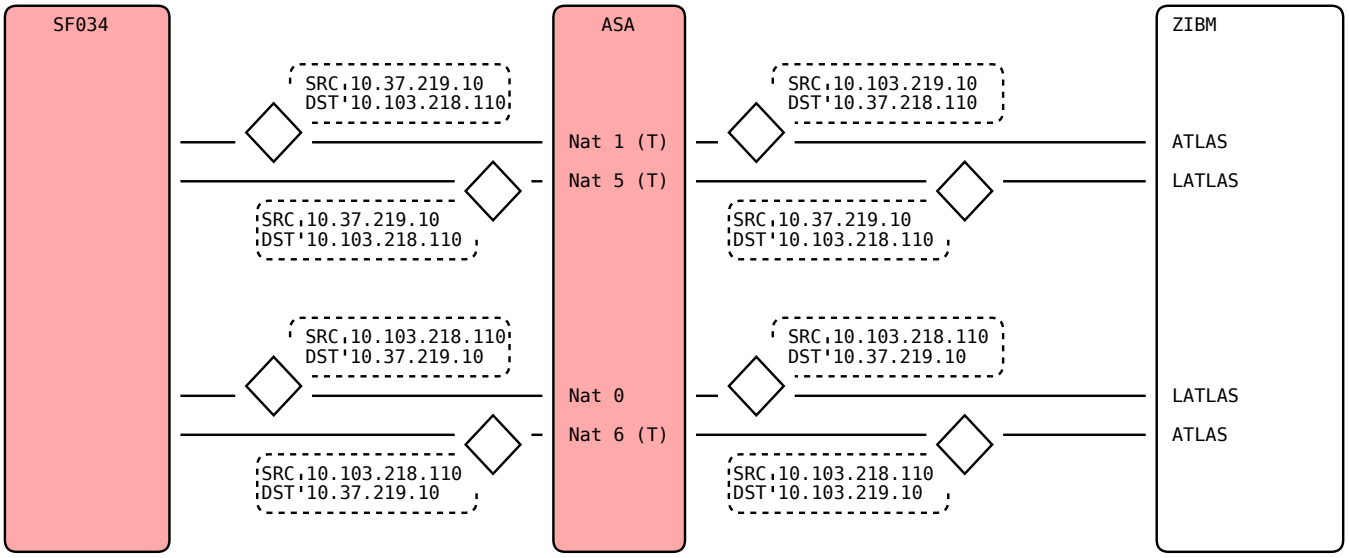
Cela fonctionne correctement pour les flux initiés par ATLAS (10.103.219.10)

Traceroute depuis 10.37.218.110 (LATLAS) vers 10.37.219.10 (ATLAS) OK

```
AT90:TSOSNS1:/u/tsosns1: >traceroute 10.37.218.110
CS V2R3: Traceroute to 10.37.218.110 (10.37.218.110)
Enter ESC character plus C or c to interrupt
1 10.103.222.7 (10.103.222.7)  1 ms  1 ms  1 ms
2 LATLAS (10.37.218.110)  1 ms  1 ms  0 ms
3 LATLAS (10.37.218.110)  66 ms  2 ms  3 ms
4 LATLAS (10.37.218.110)  1 ms  1 ms  1 ms
5 LATLAS (10.37.218.110)  0 ms !10  0 ms !10  0 ms !10
```

La source est effectivement masquée (c'est l'adresse de TOURS) qui répond.

```
1 nat (inside,outside) source static MRS-219 TRS-219 destination static TRS-218 MRS-218
3 nat (outside,inside) source static any any destination static MRS-218 MRS-218
4 nat (outside,inside) source static any any destination static TRS-218 MRS-218
5 nat (outside,inside) source static any any destination static MRS-219 MRS-219
6 nat (outside,inside) source static any any destination static TRS-219 MRS-219
```



SSH 10.37.218.110 (LATLAS) depuis 10.37.219.10 (ATLAS) est également OK

```
AT90:TSOSNS1:/u/tsosns1: >ssh root@10.37.218.110
The authenticity of host '10.37.218.110 (10.37.218.110)' can't be
established.
ECDSA key MD5 fingerprint is
34:88:f9:89:17:8e:fb:7c:9f:ec:49:69:a9:ca:95:30.
Are you sure you want to continue connecting (yes/no)? yes
FOTS2274 Warning: Permanently added '10.37.218.110' (ECDSA) to the list of
known hosts.
root@10.37.218.110's password:
FOTS1346 Permission denied, please try again.
root@10.37.218.110's password:
Last failed login: Tue Aug 23 09:18:55 CEST 2022 from 10.37.219.10 on
ssh:notty
There was 1 failed login attempt since the last successful login.
Last login: Tue Aug 23 08:28:57 2022 from 10.13.251.85
[root@latlas-foncier ~]#
```

SSH vers 10.37.219.10 (ATLAS) depuis 10.37.218.110 (LATLAS) KO.

```
[root@latlas-foncier ~]# ssh tsosns1@10.37.219.10
ssh: connect to host 10.37.219.10 port 22: Connection timed out
[root@latlas-foncier ~]#
```

Traceroute vers 10.37.219.10 (ATLAS) depuis 10.37.218.110 (LATLAS) KO.

```
traceroute to 10.37.219.10 (10.37.219.10), 30 hops max, 60 byte packets
 1  gateway (10.103.222.7)  2.483 ms  2.881 ms  3.271 ms
```

```
 2  10.103.212.34 (10.103.212.34)  1.026 ms  1.544 ms  2.068 ms
 3  * * *
 4  * * *
```

Masquerade LATLAS

Dans la logique de ce qui a été fait précédemment on ajoute la règle suivante:

```
nat (inside,outside) 1 source static MRS-218 TRS-218 destination static
TRS-219 MRS-219,
```

Lorsqu'on décompose chaque clause de la commande nat ... sur une ligne distincte:

```
nat (inside,outside)
source static MRS-218 TRS-218
destination static TRS-219 MRS-219
```

On peut traduire les actions ainsi :

- Lorsque le trafic inside correspond:
  - une source (client) 10.103.218.xxx
  - une destination (serveur) 10.37.219.xxx
- Envoyer à inside et translater
  - la source (client) en 10.37.218.xxx
  - la destination (serveur) en 10.103.219.xxx

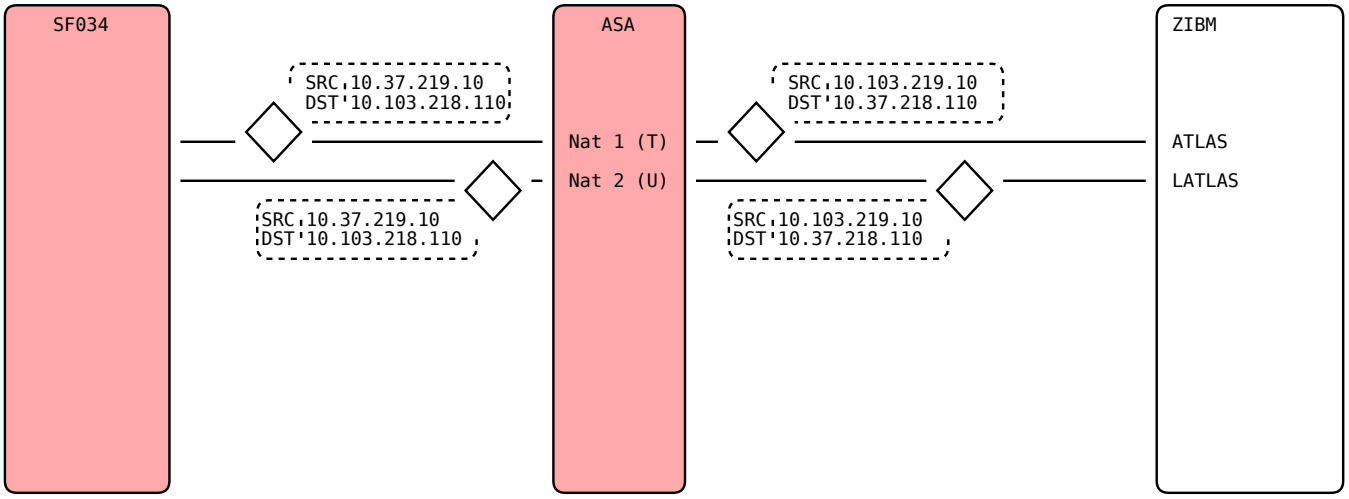
Le traceroute vers 10.37.218.110 (LATLAS) depuis ATLAS (10.37.219.10) KO.

```
AT90:TSOSNS1:/u/tsosns1: >traceroute 10.37.218.110
CS V2R3: Traceroute to 10.37.218.110 (10.37.218.110)
Enter ESC character plus C or c to interrupt
1 10.103.222.7 (10.103.222.7)  4 ms  1 ms  1 ms
2 LATLAS (10.37.218.110)  1 ms  0 ms  0 ms
3 * * *
```

La règle de nat ajoutée inverse la translation effectué en sortie lorsque le flux reviens.

```
nat: untranslation - inside:10.37.219.10/0 to outside:10.103.219.10/0
nat: untranslation - inside:10.37.219.10/0 to outside:10.103.219.10/0
nat: untranslation - inside:10.37.219.10/0 to outside:10.103.219.10/0
```

```
1 nat (inside,outside) source static MRS-219 TRS-219 destination static TRS-218 MRS-218
2 nat (inside,outside) source static MRS-218 TRS-218 destination static TRS-219 MRS-219
3 nat (outside,inside) source static any any destination static MRS-218 MRS-218
4 nat (outside,inside) source static any any destination static TRS-218 MRS-218
5 nat (outside,inside) source static any any destination static MRS-219 MRS-219
6 nat (outside,inside) source static any any destination static TRS-219 MRS-219
```



SSH depuis 10.37.218.110 (LATLAS) vers 10.37.219.10 (ATLAS) OK (le commutateur d'extrémité connait l'adresse MAC):

```
AT90:TSOSNS1:/u/tsosns1: >ssh root@10.37.218.110
root@10.37.218.110's password:
Last login: Tue Aug 23 09:19:02 2022 from 10.37.219.10
[root@latlas-foncier ~]#
```

SSH depuis 10.37.218.110 (LATLAS) vers 10.37.219.10 (ATLAS) KO

```
[root@latlas-foncier ~]# ssh tsosns1@10.37.219.10
ssh: connect to host 10.37.219.10 port 22: Connection timed out
```

Traceroute depuis 10.37.218.110 (LATLAS) vers 10.37.219.10 (ATLAS) KO

```
[root@latlas-foncier ~]# traceroute 10.37.219.10
traceroute to 10.37.219.10 (10.37.219.10), 30 hops max, 60 byte packets
 1  gateway (10.103.222.7)  2.373 ms  2.752 ms  3.150 ms
 2  10.103.212.33 (10.103.212.33)  0.930 ms  1.440 ms  1.905 ms
 3  10.103.212.34 (10.103.212.34)  1.049 ms  1.600 ms  2.075 ms
 4  * * *
```

Le problème semble provenir plutôt du fait d'un problème de natage assymétrique (un paquet emprunte un chemin différent selon le sens du trafic).

Afin de ne pas soumettre les flux à du natage assymétrique, une solution est de nater les adresses sources lorqu'ils proviennent de l'intérieur afin de les forcer à emprunter toujours le même chemin.

Nattage des adresses sources

Lors des premiers tests réalisés avec les ASAs ce problème n'a pas été vu car le nattage des adresses sources (des clients) permettait de forcer les flux à emprunter le même chemin quelque soit le sens du trafic.

Les règles de nattages suivantes sont ajoutées:

```
object network MRS-BKUP
 subnet 10.103.0.0 255.255.0.0
object network BKUP-MRS
 subnet 172.20.0.0 255.255.0.0
nat (outside,inside) 1 source static MRS-BKUP BKUP-MRS destination static
TRS-219 MRS-219
nat (outside,inside) 1 source static MRS-BKUP BKUP-MRS destination static
TRS-218 MRS-218
```

Traceroute de LATLAS (10.37.218.110) vers LATLAS (10.37.219.10) OK

```
[root@latlas-foncier ~]# traceroute 10.37.219.10
traceroute to 10.37.219.10 (10.37.219.10), 30 hops max, 60 byte packets
 1  gateway (10.103.222.7)  2.612 ms  3.009 ms  3.399 ms
 2  10.103.212.33 (10.103.212.33)  0.854 ms  1.332 ms  1.763 ms
 3  10.103.212.34 (10.103.212.34)  1.035 ms  1.500 ms  1.991 ms
 4  atlas-foncier.d037.dgfip (10.37.219.10)  1.282 ms  1.716 ms  2.083 ms
 5  atlas-foncier.d037.dgfip (10.37.219.10)  3.540 ms  3.986 ms  4.418 ms
 6  atlas-foncier.d037.dgfip (10.37.219.10)  0.739 ms  0.477 ms  0.467 ms
```

SSH de ATLAS (10.37.218.110) vers LATLAS (10.37.219.10) OK

```
[root@latlas-foncier ~]# ssh tsosns1@10.37.219.10
The authenticity of host '10.37.219.10 (10.37.219.10)' can't be established.
RSA key fingerprint is SHA256:d4fti5kxhaG3aZXu9dkyJTPtV4DORTjYznwZV1HBFzQ.
RSA key fingerprint is MD5:7d:eb:47:11:fe:69:ca:e8:fd:20:a4:23:c1:bd:fc:7d.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.37.219.10' (RSA) to the list of known hosts.
tsosns1@10.37.219.10's password:
AT90:TSOSNS1:/u/tsosns1: >
```

Traceroute de ATLAS (10.37.219.10) vers LATLAS (10.37.218.110) OK

```
AT90:TSOSNS1:/u/tsosns1: >traceroute 10.37.218.110
CS V2R3: Traceroute to 10.37.218.110 (10.37.218.110)
Enter ESC character plus C or c to interrupt
1 10.103.212.7 (10.103.212.7)  1 ms  1 ms  1 ms
2 10.103.212.33 (10.103.212.33)  0 ms  0 ms  0 ms
```

```
3 LATLAS (10.37.218.110)  1 ms  0 ms  0 ms
4 LATLAS (10.37.218.110)  1 ms  0 ms  0 ms
5 LATLAS (10.37.218.110)  1 ms  1 ms  1 ms
6 LATLAS (10.37.218.110)  0 ms !10  0 ms !10  0 ms !10
```

SSH de ATLAS (10.37.219.10) vers LATLAS (10.37.218.110) OK

```
AT90:TSOSNS1:/u/tsosns1: >ssh root@10.37.218.110
root@10.37.218.110's password:
Last login: Wed Aug 24 12:33:02 2022 from 10.13.251.85
[root@latlas-foncier ~]# ifconfig
dummy0: flags=195<UP,BROADCAST,RUNNING,NOARP>  mtu 1500
        inet 10.103.218.110  netmask 255.255.255.255  broadcast 0.0.0.0
        inet6 fe80::58e3:72ff:feaf:f17c  prefixlen 64  scopeid 0x20<link>
        ether 5a:e3:72:af:f1:7c  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3  bytes 210 (210.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Conclusion

Le Natage des adresses sources lorsque le flux a pour origine une partition secourue et pour destination une autre partition secourue permet d'établir la communication entre ces partitions.