

Masquerade STF

Table of Contents

- [Masquerade STF](#)
 - [Test du 17-10-2022](#)
 - [Périmètre](#)
 - [Configuration du NAT sourcing](#)
 - [Configuration du basculement](#)
 - [Test de basculement 17-11-2022](#)
 - [Périmètre](#)
 - [Configuration du NAT sourcing](#)
 - [Configuration du basculement](#)

Lors de l'échange de fichiers les partitions hébergées au SNS répondent avec l'adresse IP physique de secours or:

1. les parefeu du SPS n'autorisent que les adresses VIPA de Tours,
2. le VIPA des VM utilisent l'adresse physique dans l'entête TCP/IP

Afin de contourner cela le SNS met en place des règles de NAT sourcing pour masquer l'adresse IP de secours par l'adresse IP de production, lorsque la VM STF essaye de contacter son homologue du SPS.

Test du 17-10-2022

Périmètre

@ physique de la VM STF secours	10.103.216.115
@ VIPA de le VM STF à Tours	10.37.237.115 à aspirer
@ de destination (BN de secours)	10.13.83.198

Configuration du NAT sourcing

Définition des objets:

```
object network TRS-STF
  host 10.37.237.115
object network MRS-STF
  host 10.103.216.115
object network MRS-BNS
  host 10.13.83.198
```

Définition de la règle de Nat:

```
nat (inside,outside) 1 source static MRS-STF TRS-STF destination static MRS-BNS MRS-BNS
```

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

```
nat (inside,outside)
source static MRS-STF TRS-STF
destination static MRS-BNS MRS-BNS
```

On peut traduire les actions ainsi :

- Lorsque le trafic inside correspond:
 - une source (client) 10.103.237.115
 - une destination (serveur) 10.13.83.198
- Envoyer à inside et traduire
 - la source (client) en 10.37.237.115
 - la destination (serveur) en 10.13.83.198

Configuration du basculement

```
ip route-static 10.37.237.115 32 10.103.212.36 tag 10
```

Cela fonctionne correctement pour les flux initiés par 10.103.216.115

Test de basculement 17-11-2022

Périmètre

Nom ZVM	@IP VIPA TRS	@IP VIPA MRS	@IP PHYS	@IP STF DISTANT
STF3SAQ1	10.37.218.31	10.103.218.31	10.nnn.235.31	10.157.8.110
STF3SAI1	10.37.218.30	10.103.218.30	10.nnn.235.30	10.156.4.210

Configuration du NAT sourcing

Sur les **ASAs** ajout des règles de **NAT** pour faire du **MASQUERADE** de l'IP source

Définition des objets:

```
object network TRS-STFSAQ1
  host 10.37.218.31
object network MRS-STFSAQ1
  host 10.103.215.31
object network CIP-STFU
```

```
host 10.157.8.110
object network TRS-STFSAI1
  host 10.37.218.30
object network MRS-STFSAI1
  host 10.103.215.30
object network CIP-STFI
  host 10.156.4.210
```

Définition de la règle de Nat:

```
nat (inside,outside) 1 source static MRS-STFSAQ1 TRS-STFSAQ1 destination
static CIP-STFU CIP-STFU
nat (inside,outside) 1 source static MRS-STFSAI1 TRS-STFSAI1 destination
static CIP-STFI CIP-STFI
```

La règle de MASQUERADE implantée converti l'adresse physique (10.103.215.31) en adresse vipa (10.37.218.31).

Cependant l'ensemble des contrats concernant **stf3saq1 10.37.235.31** (adresse physique)



Pour tester le MASQUERADE avec l'adresse physique de **STF3SAQ1**:

- remplacer dans les ASA l'adresse de l'objet **TRS-STFSAQ1** par l'adresse physique:

```
object network TRS-STFSAQ1
```

```
host 10.37.235.31
```

- remplacer la route statique dans le fédérateur

```
undo ip route-static 10.37.218.31 32 10.103.212.36
```

```
ip route-static 10.37.235.31 32 10.103.212.36 tag 10 description
TRS-STFSAQ1
```

Pour prendre en compte l'ensemble des adresses des contrats de service les adresses des clients suivant sont ajoutées:

```
object network RLCPGSE001
  host 10.154.232.3
object network SCPPGSE001
  host 10.154.9.102
object network BDPPGSE001
  host 10.157.5.196
object network LAMEATLASIIA
  host 10.69.237.240
object network LAMEATLASIIA2
  host 10.69.237.78
object network TLRPUSD405
  host 10.154.68.14
object network REFPGSE001
```

```
host 10.154.240.245
object network SAPPGE001
  host 10.154.230.177
object network TSCPGSE001
  host 10.154.229.121
object network LCAMQ702
  host 10.69.237.150
object network TSCPGSE001
  host 10.154.229.121
```

```
nat (inside,outside) 1 source static MRS-STFSAQ1 TRS-STFSAQ1 destination
static RLCPGE001 RLCPGE001
nat (inside,outside) 1 source static MRS-STFSAQ1 TRS-STFSAQ1 destination
static SCPPGE001 SCPPGE001
nat (inside,outside) 1 source static MRS-STFSAQ1 TRS-STFSAQ1 destination
static BDPPGE001 BDPPGE001
nat (inside,outside) 1 source static MRS-STFSAQ1 TRS-STFSAQ1 destination
static LAMEATLASIIA LAMEATLASIIA
nat (inside,outside) 1 source static MRS-STFSAQ1 TRS-STFSAQ1 destination
static LAMEATLASIIA2 LAMEATLASIIA2
nat (inside,outside) 1 source static MRS-STFSAQ1 TRS-STFSAQ1 destination
static TLRPUSD405 TLRPUSD405
nat (inside,outside) 1 source static MRS-STFSAQ1 TRS-STFSAQ1 destination
static REFPGSE001 REFPGSE001
nat (inside,outside) 1 source static MRS-STFSAQ1 TRS-STFSAQ1 destination
static SAPPGE001 SAPPGE001
nat (inside,outside) 1 source static MRS-STFSAQ1 TRS-STFSAQ1 destination
static TSCPGSE001 TSCPGSE001
nat (inside,outside) 1 source static MRS-STFSAQ1 TRS-STFSAQ1 destination
static LCAMQ702 LCAMQ702
nat (inside,outside) 1 source static MRS-STFSAQ1 TRS-STFSAQ1 destination
static TSCPGSE001 TSCPGSE001
```

Configuration du basculement

Sur le fédérateur (sf034-a5500-013sns1) déclaration des routes en BGP pour le basculement réseau.

Basculement réseau

```
ip route-static 10.37.218.31 32 10.103.212.36 tag 10 description TRS-STFSAQ1
ip route-static 10.37.218.30 32 10.103.212.36 tag 10 description TRS-STFSAI1
```

Retour en nominal

```
undo ip route-static 10.37.218.31 32 10.103.212.36
undo ip route-static 10.37.218.30 32 10.103.212.36
```

From:

<http://www.ouarte.garden/> - **dwndoc**

Permanent link:

<http://www.ouarte.garden/doku.php?id=journal:2022:day-2022-10-17>

Last update: **2025/02/19 10:59**

