TP CCSN

# Rapport de Routage – BGP & OSPF Multi-Area

**Projet E5 · Architecture Réseau Sécurisée**

Par **Lilo BENNARDO** & **Ilyan TAYBI**

Panorama ISP → Paris → Lyon → Marseille avec routage dynamique, redistribution et VPN.

#BGP    #OSPF Multi-Area    #VPN OpenConnect    #Radius & FTP
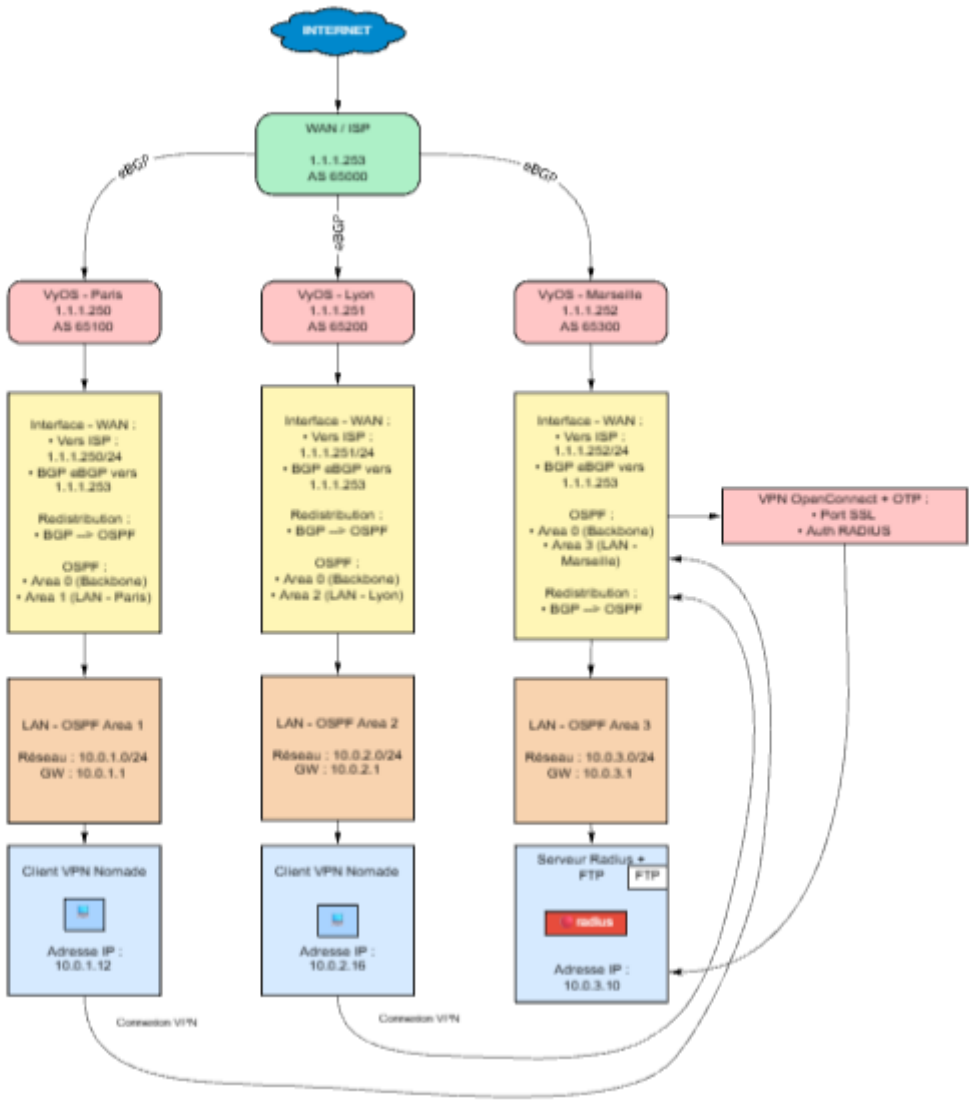
## Sommaire

## Introduction

**Objectif :** documentation complète de l'architecture multi-sites conçue par **Lilo BENNARDO** & **Ilyan TAYBI**, couvrant adressage, protocoles dynamiques, redistribution et sécurisation VPN/Radius/FTP pour l'épreuve E5.

## 1. Schéma du réseau

**Vue d'ensemble :** l'ISP transporte le WAN /29 commun, chaque site maintient son LAN /24 et échange les préfixes via BGP, tandis qu'OSPF multi-area assure la convergence interne.

*(Insérer ici le schéma réseau annoté : AS, IP WAN, LAN, areas OSPF, liens BGP).*

## 1.1 Table de routage – ISP (AS 65000)

| Destination | Préfixe | Protocole | Next-hop | Interface | Commentaire |
|---|---|---|---|---|---|
| 0.0.0.0/0 | par défaut | Static | 192.168.80.2 | eth0 | Sortie vers Internet / réseau externe |
| 1.1.1.248/29 | WAN | Connected | — | eth1 | Réseau WAN vers Paris / Lyon / Marseille |
| 10.0.1.0/24 | LAN Paris | BGP | 1.1.1.250 | eth1 | Reçu de Paris (AS 65100) |
| 10.0.2.0/24 | LAN Lyon | BGP | 1.1.1.251 | eth1 | Reçu de Lyon (AS 65200) |
| 10.0.3.0/24 | LAN Marseille | BGP | 1.1.1.252 | eth1 | Reçu de Marseille (AS 65300) |
| 192.168.80.0/24 | Management | Connected | — | eth0 | Réseau de gestion de l'ISP |

## 1.2 Table de routage – Paris (AS 65100)

| Destination | Préfixe | Protocole | Next-hop | Interface | Commentaire |
|---|---|---|---|---|---|
| 0.0.0.0/0 | par défaut | Static | 1.1.1.253 | eth2 | Sortie vers l'ISP |
| 1.1.1.248/29 | WAN | Connected | — | eth2 | Réseau WAN via ISP |
| 10.0.1.0/24 | LAN Paris | Connected | — | eth3 | Réseau local du site Paris |
| 10.0.2.0/24 | LAN Lyon | BGP | 1.1.1.251 | eth2 | Appris en eBGP via ISP |
| 10.0.3.0/24 | LAN Mars. | BGP | 1.1.1.252 | eth2 | Appris en eBGP via ISP |

## 1.3 Table de routage – Lyon (AS 65200)

| Destination | Préfixe | Protocole | Next-hop | Interface | Commentaire |
|---|---|---|---|---|---|
| 0.0.0.0/0 | par défaut | Static | 1.1.1.253 | eth2 | Sortie vers l'ISP |
| 1.1.1.248/29 | WAN | Connected | — | eth2 | Réseau WAN via ISP |
| 10.0.2.0/24 | LAN Lyon | Connected | — | eth3 | Réseau local du site Lyon |
| 10.0.1.0/24 | LAN Paris | BGP | 1.1.1.250 | eth2 | Appris en eBGP via ISP |
| 10.0.3.0/24 | LAN Mars. | BGP | 1.1.1.252 | eth2 | Appris en eBGP via ISP |

## 1.4 Table de routage – Marseille (AS 65300)

| Destination | Préfixe | Protocole | Next-hop | Interface | Commentaire |
|---|---|---|---|---|---|
| 0.0.0.0/0 | par défaut | Static | 1.1.1.253 | eth2 | Sortie vers l'ISP |
| 1.1.1.248/29 | WAN | Connected | — | eth2 | Réseau WAN via ISP |
| 10.0.3.0/24 | LAN Mars. | Connected | — | eth3 | Réseau local du site Marseille |
| 10.0.1.0/24 | LAN Paris | BGP | 1.1.1.250 | eth2 | Appris en eBGP via ISP |
| 10.0.2.0/24 | LAN Lyon | BGP | 1.1.1.251 | eth2 | Appris en eBGP via ISP |

## 1.5 Résumé : pourquoi utiliser un /29 au lieu d'un /24 ?

**/29 ciblé, /24 surdimensionné**

- Un **/29** offre exactement quatre IP clientes + l'ISP : dimensionnement réaliste des liaisons WAN.
- Surface d'exposition réduite, cohérente avec les pratiques eBGP inter-AS.
- Tables de routage lisibles et segmentation WAN/LAN plus claire.

**/29 = efficace, sécurisé, optimisé. / /24 = trop vaste pour un WAN partagé.**

# 2. Configuration IP sur chaque routeur

> **Principe :** chaque site possède un WAN en /29 sur `eth2` (ou `eth1` côté ISP) et un LAN /24 sur `eth3`, garantissant une séparation claire.

## 2.1 ISP

```
set interfaces ethernet eth0 address 192.168.80.10/24
set interfaces ethernet eth1 address 1.1.1.253/29
commit
save
```

## 2.2 Paris

```
set interfaces ethernet eth2 address 1.1.1.250/29
set interfaces ethernet eth3 address 10.0.1.250/24
commit
save
```

## 2.3 Lyon

```
set interfaces ethernet eth2 address 1.1.1.251/29
set interfaces ethernet eth3 address 10.0.2.250/24
commit
save
```

## 2.4 Marseille

```
set interfaces ethernet eth2 address 1.1.1.252/29
set interfaces ethernet eth3 address 10.0.3.250/24
commit
save
```

# 3. Configuration BGP

> **But :** publier les LAN locaux via eBGP et maintenir la visibilité des /24 chez l'ISP.

## 3.1 ISP (AS 65000)

```
set protocols bgp system-as 65000
set protocols bgp parameters router-id 1.1.1.253
set protocols bgp neighbor 1.1.1.250 remote-as 65100
set protocols bgp neighbor 1.1.1.250 address-family ipv4-unicast
```

```
set protocols bgp neighbor 1.1.1.251 remote-as 65200
set protocols bgp neighbor 1.1.1.251 address-family ipv4-unicast
set protocols bgp neighbor 1.1.1.252 remote-as 65300
set protocols bgp neighbor 1.1.1.252 address-family ipv4-unicast
commit
save
```

**Vérification –** `show bgp summary`

```
vyos@ISP# run show bgp summary

IPv4 Unicast Summary (VRF default):
BGP router identifier 1.1.1.253, local AS number 65000 vrf-id 0
BGP table version 3
RIB entries 5, using 480 bytes of memory
Peers 3, using 60 KiB of memory

Neighbor        V        AS MsgRcvd MsgSent   TblVer InQ OutQ Up/Down State/PfxRcd  PfxSnt Desc
1.1.1.250       4     65100     103     103        3   0    0 01:37:04           1       3 N/A
1.1.1.251       4     65200      97      97        3   0    0 01:31:19           1       3 N/A
1.1.1.252       4     65300      96      96        3   0    0 01:30:39           1       3 N/A

Total number of neighbors 3
[edit]
vyos@ISP#
```

**Vérification –** `show ip route`

```
vyos@ISP# run show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

S>* 0.0.0.0/0 [1/0] via 192.168.80.2, eth0, weight 1, 02:22:17
O   1.1.1.248/29 [110/1] is directly connected, eth1, weight 1, 00:37:42
C>* 1.1.1.248/29 is directly connected, eth1, 01:21:27
O   10.0.1.0/24 [110/2] via 1.1.1.250, eth1, weight 1, 00:21:23
B>* 10.0.1.0/24 [20/0] via 1.1.1.250, eth1, weight 1, 01:21:27
O   10.0.2.0/24 [110/2] via 1.1.1.251, eth1, weight 1, 00:19:13
B>* 10.0.2.0/24 [20/0] via 1.1.1.251, eth1, weight 1, 01:21:27
O   10.0.3.0/24 [110/2] via 1.1.1.252, eth1, weight 1, 00:18:03
B>* 10.0.3.0/24 [20/0] via 1.1.1.252, eth1, weight 1, 01:21:27
C>* 192.168.80.0/24 is directly connected, eth0, 02:22:20
[edit]
vyos@ISP#
```

## 3.2 Paris (AS 65100)

```
set protocols bgp system-as 65100
set protocols bgp parameters router-id 1.1.1.250
set protocols bgp neighbor 1.1.1.253 remote-as 65000
set protocols bgp neighbor 1.1.1.253 address-family ipv4-unicast
set protocols bgp address-family ipv4-unicast network 10.0.1.0/24
commit
save
```

**Vérification – `show bgp summary`**

```
vyos@PARIS:~$ show bgp summary

IPv4 Unicast Summary (VRF default):
BGP router identifier 1.1.1.250, local AS number 65100 vrf-id 0
BGP table version 3
RIB entries 5, using 480 bytes of memory
Peers 1, using 20 KiB of memory

Neighbor        V         AS   MsgRcvd   MsgSent   TblVer  InQ OutQ  Up/Down Sta
te/PfxRcd    PfxSnt Desc
1.1.1.253       4      65000       120       120        3    0    0 01:54:31
         2        3 N/A

Total number of neighbors 1
vyos@PARIS:~$
```

**Vérification – `show configuration protocols bgp`**

```
vyos@PARIS:~$ configure
[edit]
vyos@PARIS# show protocols bgp
 address-family {
     ipv4-unicast {
         network 10.0.1.0/24 {
         }
     }
 }
 neighbor 1.1.1.253 {
     address-family {
         ipv4-unicast {
         }
     }
     remote-as 65000
 }
 parameters {
     router-id 1.1.1.250
 }
 system-as 65100
[edit]
vyos@PARIS# _
```

**Vérification – `show ip route`**

```
vyos@PARIS:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

O   1.1.1.248/29 [110/1] is directly connected, eth2, weight 1, 00:55:29
C>* 1.1.1.248/29 is directly connected, eth2, 01:37:23
O   10.0.1.0/24 [110/1] is directly connected, eth3, weight 1, 00:42:55
C>* 10.0.1.0/24 is directly connected, eth3, 02:33:33
O   10.0.2.0/24 [110/2] via 1.1.1.251, eth2, weight 1, 00:40:39
B>* 10.0.2.0/24 [20/0] via 1.1.1.251, eth2, weight 1, 01:37:23
O   10.0.3.0/24 [110/2] via 1.1.1.252, eth2, weight 1, 00:39:29
B>* 10.0.3.0/24 [20/0] via 1.1.1.252, eth2, weight 1, 01:37:23
vyos@PARIS:~$
```

## 3.3 Lyon (AS 65200)

```
set protocols bgp system-as 65200
set protocols bgp parameters router-id 1.1.1.251
set protocols bgp neighbor 1.1.1.253 remote-as 65000
set protocols bgp neighbor 1.1.1.253 address-family ipv4-unicast
set protocols bgp address-family ipv4-unicast network 10.0.2.0/24
commit
save
```

**Vérification – `show bgp summary`**

```
vyos@LYON:~$ show bgp summary

IPv4 Unicast Summary (VRF default):
BGP router identifier 1.1.1.251, local AS number 65200 vrf-id 0
BGP table version 3
RIB entries 5, using 480 bytes of memory
Peers 1, using 20 KiB of memory

Neighbor        V        AS    MsgRcvd   MsgSent   TblVer   InQ OutQ  Up/Down Sta
te/PfxRcd   PfxSnt Desc
1.1.1.253       4      65000       126       126        3     0    0 02:00:09
       2        3 N/A

Total number of neighbors 1
vyos@LYON:~$ _
```

**Vérification – `show configuration protocols bgp`**

```
        vyos@LYON:~$ configure
        [edit]
        vyos@LYON# show protocols bgp
         address-family {
             ipv4-unicast {
                 network 10.0.2.0/24 {
                 }
             }
         }
         neighbor 1.1.1.253 {
             address-family {
                 ipv4-unicast {
                 }
             }
             remote-as 65000
         }
         parameters {
             router-id 1.1.1.251
         }
         system-as 65200
        [edit]
        vyos@LYON#
```

**Vérification – `show ip route`**

```
vyos@LYON:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

S>* 0.0.0.0/0 [1/0] via 1.1.1.250, eth2, weight 1, 01:31:42
O   1.1.1.248/29 [110/1] is directly connected, eth2, weight 1, 01:00:42
C>* 1.1.1.248/29 is directly connected, eth2, 01:31:42
O   10.0.1.0/24 [110/2] via 1.1.1.250, eth2, weight 1, 00:49:02
B>* 10.0.1.0/24 [20/0] via 1.1.1.250, eth2, weight 1, 01:31:42
O   10.0.2.0/24 [110/1] is directly connected, eth3, weight 1, 00:46:59
C>* 10.0.2.0/24 is directly connected, eth3, 02:04:53
O   10.0.3.0/24 [110/2] via 1.1.1.252, eth2, weight 1, 00:45:42
B>* 10.0.3.0/24 [20/0] via 1.1.1.252, eth2, weight 1, 01:31:42
vyos@LYON:~$
```

## 3.4 Marseille (AS 65300)

```
set protocols bgp system-as 65300
set protocols bgp parameters router-id 1.1.1.252
set protocols bgp neighbor 1.1.1.253 remote-as 65000
set protocols bgp neighbor 1.1.1.253 address-family ipv4-unicast
set protocols bgp address-family ipv4-unicast network 10.0.3.0/24
commit
save
```

**Vérification – `show bgp summary`**

```
vyos@vyos: $ show bgp summary

IPv4 Unicast Summary (VRF default):
BGP router identifier 1.1.1.252, local AS number 65300 vrf-id 0
BGP table version 3
RIB entries 5, using 480 bytes of memory
Peers 1, using 20 KiB of memory

Neighbor          V      AS    MsgRcvd   MsgSent   TblVer   InQ OutQ  Up/Down Sta
te/PfxRcd    PfxSnt Desc
1.1.1.253        4     65000      127       127        3     0     0 02:01:40
          2      3 N/A


Total number of neighbors 1
vyos@vyos:~$
```

**Vérification – `show configuration protocols bgp`**

```
vyos@MARSEILLE# show protocols bgp
 address-family {
     ipv4-unicast {
         network 10.0.3.0/24 {
         }
     }
 }
 neighbor 1.1.1.253 {
     address-family {
         ipv4-unicast {
         }
     }
     remote-as 65000
 }
 parameters {
     router-id 1.1.1.252
 }
 system-as 65300
[edit]
vyos@MARSEILLE# _
```

**Vérification – `show ip route`**

```
vyos@vyos:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

S>* 0.0.0.0/0 [1/0] via 1.1.1.253, eth2, weight 1, 01:21:24
O    1.1.1.248/29 [110/1] is directly connected, eth2, weight 1, 01:01:40
C>* 1.1.1.248/29 is directly connected, eth2, 01:23:16
O    10.0.1.0/24 [110/2] via 1.1.1.250, eth2, weight 1, 00:50:50
B>* 10.0.1.0/24 [20/0] via 1.1.1.250, eth2, weight 1, 01:23:16
O    10.0.2.0/24 [110/2] via 1.1.1.251, eth2, weight 1, 00:48:40
B>* 10.0.2.0/24 [20/0] via 1.1.1.251, eth2, weight 1, 01:23:16
O    10.0.3.0/24 [110/1] is directly connected, eth3, weight 1, 00:47:36
C>* 10.0.3.0/24 is directly connected, eth3, 02:06:21
vyos@vyos:~$ _
```

# 4. Configuration OSPF multi-area

> **Stratégie :** Area 0 pour le WAN commun, une zone dédiée par site (1/2/3) et redistribution BGP →
> OSPF sur les PE.

## 4.1 ISP – Backbone Area 0

```
set protocols ospf area 0 network 1.1.1.248/29
commit
save
```

**Vérification –** `show protocols ospf`

```
vyos@ISP# show protocols ospf
 area 0 {
     network 1.1.1.248/29
 }
 parameters {
     router-id 1.1.1.253
 }
[edit]
vyos@ISP#
```

**Vérification –** `show ip route ospf`

```
vyos@ISP:~$ show ip route ospf
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

O   1.1.1.248/29 [110/1] is directly connected, eth1, weight 1, 01:39:27
O   10.0.1.0/24 [110/2] via 1.1.1.250, eth1, weight 1, 01:23:08
O   10.0.2.0/24 [110/2] via 1.1.1.251, eth1, weight 1, 01:20:58
O   10.0.3.0/24 [110/2] via 1.1.1.252, eth1, weight 1, 01:19:48
vyos@ISP:~$
```

## 4.2 Paris – Area 1

```
set protocols ospf area 0 network 1.1.1.248/29
set protocols ospf area 1 network 10.0.1.0/24
set protocols ospf redistribute bgp
commit
save
```

**Vérification –** `show protocols ospf`

```
vyos@PARIS:~$ configure
[edit]
vyos@PARIS# show protocols ospf
 area 0 {
     network 1.1.1.248/29
 }
 area 1 {
     network 10.0.1.0/24
 }
[edit]
vyos@PARIS#
```

**Vérification –** `show ip route ospf`

```
vyos@PARIS# run show ip route ospf
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

O    1.1.1.248/29 [110/1] is directly connected, eth2, weight 1, 01:46:14
O    10.0.1.0/24 [110/1] is directly connected, eth3, weight 1, 01:33:40
O    10.0.2.0/24 [110/2] via 1.1.1.251, eth2, weight 1, 01:31:24
O    10.0.3.0/24 [110/2] via 1.1.1.252, eth2, weight 1, 01:30:14
[edit]
```

## 4.3 Lyon – Area 2

```
set protocols ospf area 0 network 1.1.1.248/29
set protocols ospf area 2 network 10.0.2.0/24
set protocols ospf redistribute bgp
commit
save
```

**Vérification –** `show protocols ospf`

```
vyos@LYON# show protocols ospf
 area 0 {
     network 1.1.1.248/29
 }
 area 2 {
     network 10.0.2.0/24
 }
[edit]
vyos@LYON#
```

**Vérification –** `show ip route ospf`

```
vyos@LYON# run show ip route ospf
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

O   1.1.1.248/29 [110/1] is directly connected, eth2, weight 1, 01:47:00
O   10.0.1.0/24 [110/2] via 1.1.1.250, eth2, weight 1, 01:35:20
O   10.0.2.0/24 [110/1] is directly connected, eth3, weight 1, 01:33:17
O   10.0.3.0/24 [110/2] via 1.1.1.252, eth2, weight 1, 01:32:00
[edit]
vyos@LYON#
```

## 4.4 Marseille – Area 3

```
set protocols ospf area 0 network 1.1.1.248/29
set protocols ospf area 3 network 10.0.3.0/24
set protocols ospf redistribute bgp
commit
save
```

**Vérification –** `show protocols ospf`

```
[edit]
vyos@MARSEILLE# show protocols ospf
 area 0 {
     network 1.1.1.248/29
 }
 area 3 {
     network 10.0.3.0/24
 }
[edit]
vyos@MARSEILLE#
```

**Vérification –** `show ip route ospf`

```
[edit]
vyos@MARSEILLE# run show ip route ospf
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

O   1.1.1.248/29 [110/1] is directly connected, eth2, weight 1, 01:48:16
O   10.0.1.0/24 [110/2] via 1.1.1.250, eth2, weight 1, 01:37:26
O   10.0.2.0/24 [110/2] via 1.1.1.251, eth2, weight 1, 01:35:16
O   10.0.3.0/24 [110/1] is directly connected, eth3, weight 1, 01:34:12
[edit]
vyos@MARSEILLE#
```

# 5. Redistribution BGP <-> OSPF

> **Alignement :** double redistribution pour fournir une table cohérente à tous les protocoles.

```
set protocols ospf redistribute bgp
set protocols bgp address-family ipv4-unicast redistribute ospf
commit
save
```

# 6. Tests de connectivité

> **Preuves :** ping inter-sites et traceroute confirment la diffusion via l'ISP.

## 6.1 Ping inter-sites (LAN -> LAN)

**Paris -> Lyon**

```
ping 10.0.2.250
```

```
vyos@PARIS# ping 10.0.2.250
PING 10.0.2.250 (10.0.2.250) 56(84) bytes of data.
64 bytes from 10.0.2.250: icmp_seq=1 ttl=64 time=0.719 ms
64 bytes from 10.0.2.250: icmp_seq=2 ttl=64 time=8.16 ms
64 bytes from 10.0.2.250: icmp_seq=3 ttl=64 time=1.34 ms
^C
--- 10.0.2.250 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.719/3.406/8.163/3.372 ms
[edit]
vyos@PARIS#
```

**Paris -> Marseille**

```
ping 10.0.3.250
```

```
vyos@PARIS# ping 10.0.3.250
PING 10.0.3.250 (10.0.3.250) 56(84) bytes of data.
64 bytes from 10.0.3.250: icmp_seq=1 ttl=64 time=0.636 ms
64 bytes from 10.0.3.250: icmp_seq=2 ttl=64 time=0.900 ms
64 bytes from 10.0.3.250: icmp_seq=3 ttl=64 time=1.71 ms
^C
--- 10.0.3.250 ping statistics ---
```

**Lyon -> Paris**

```
ping 10.0.1.250
```

```
vyos@LYON# ping 10.0.1.250
PING 10.0.1.250 (10.0.2.250 56(84) bytes of data.
64 bytes from 10.0.1.250: icmp_seq=1 0.825 ms
64 bytes from 10.0.1.250: icmp_sed=2 1.06 ms
64 bytes from 10.0.3.250: icmp_seq=1 1.20 ms
```

6.2 Traceroute (preuve que le trafic passe par l'ISP)

**Exemple Paris -> Lyon**

```
vyos@PARIS: $ traceroute 10.0.2.250
traceroute to 10.0.2.250 (10.0.2.250), 30 hops max, 60 byte packets
 1  10.0.2.250 (10.0.2.250)  0.877 ms  0.590 ms  0.594 ms
vyos@PARIS:~$
```

# 7. Analyse Wireshark (FTP non lisible grâce au VPN)

> **Confidentialité :** capture chiffrée attestant que le FTP passe par le tunnel.

| Wireshark |
|---|
| View  Go  Capture  Analyze  Statistics  Telephony  Wireless  Tools  Help |

| Time | Destination | Protocol | Length | Info |
|---|---|---|---|---|
| 0.0000609 | 10.0.2.1 | VPN | 101 | Encrypted Payload |
| 2 0.0000969 | 10.0.2.0 | VPN | 109 | Encrypted Payload |
| 3 0.0000874 | 10.0.2.1 | VPN | 109 | Encrypted Payload |
| d 0.0004812 | 10.0.2.10 | VPN | 18l | Encrypted Payload |
| 3 0.0000807 | 10.0.2.2 | VPN | 109 | Encrypted Payload |
| 6 0.0000121 | 10.0.2.3 | VPN | 105 | Encrypted Payload |
| 7 0.0000156 | 10.0.2.4 | VPN | 101 | Encrypted Payload |
| 9 0.0000185 | 10.0.2.5 | VPN | 109 | Encrypted Payload |
| 9 0.0000216 | 10.0.2.6 | VPN | 109 | Encrypted Payload |
| 0 0.0000230 | 10.0.2.7 | VPN | 109 | Encrypted Payload |

· 1 4 byte cire (1519 byies) 151 bytes on ware

# 8. Configuration VPN (OpenConnect + OTP + RADIUS)

> **Assemblage :** chaîne Radius + vsftpd + OpenConnect pour authentifier et protéger les accès distants.

Config RADIUS

```
nano /etc/freeradius/3.0/users
```

```
lilo Cleartext-Password := "12345"
```

```
systemctl restart freeradius
systemctl enable freeradius
```

```
apt update
apt install vsftpd -y
systemctl enable vsftpd
systemctl restart vsftpd
```

```
root@debian:~# radtest lilo 12345 127.0.0.1 0 testing123
Sent Access-Request Id 197 from 0.0.0.0:42420 to 127.0.0.1:1812 length 74
        User-Name = "lilo"
        User-Password = "12345"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 0
        Message-Authenticator = 0x00
        Cleartext-Password = "12345"
Sent Access-Request Id 197 from 0.0.0.0:42420 to 127.0.0.1:1812 length 74
        User-Name = "lilo"
        User-Password = "12345"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 0
        Message-Authenticator = 0x00
        Cleartext-Password = "12345"
Sent Access-Request Id 197 from 0.0.0.0:42420 to 127.0.0.1:1812 length 74
        User-Name = "lilo"
        User-Password = "12345"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 0
        Message-Authenticator = 0x00
        Cleartext-Password = "12345"
^C
root@debian:~#
```

## Connexion VPN nomade

```
set vpn openconnect ssl-cert-file /config/auth/server.crt
set vpn openconnect ssl-key-file /config/auth/server.key
set vpn openconnect authentication mode radius
set vpn openconnect authentication radius server 10.0.3.10 secret radiussecret
set vpn openconnect network 10.10.10.0/24
set vpn openconnect port 4443
commit
save
```

```
user@hostname:~$ openconnect vpn.example.com
POST https://vpn.example.com/
Connected to 203.0.113.1
SHA-256 fingerprint419b429f4ac74450e89041a93a2b9ceb7a88cd111f32f69f3
Connected to HTTPS on vpn.example.com
RADIUS username: user
RADIUS token:
Enter OTP 000223
RADIUS: Authentication succeeded.
Got CONNECT response:200
Connected as 10.10.10.11, using SSL, with DTLS in progress
Adding 'split DNS' vpn.example.com
Adding new default route via 10.10.101.1
Press Ctrl+C to dismiss, Ctrl+Z to suspeń, see man page for details.
user@hostname:~$ftp 10.10.10.1
Connected to 10.10.10.100.
220 (vsFTPd 3.0.3)
Name (10.10.10.100:usr): ftpuser
Password:****
user@hostname:~$
```

## 9. Conclusion

**Bilan :** la combinaison BGP/OSPF/vpn répond aux objectifs pédagogiques : connectivité inter-AS assurée, convergence interne rapide, accès distants chiffrés et preuves Wireshark à l'appui. Cette architecture constitue une base solide pour de futures évolutions sécurisées.