Création et configuration des VPNs en mode transparent

Table of Contents

Mise en oeuvre des VPNs sur l'infrastructure BULL.

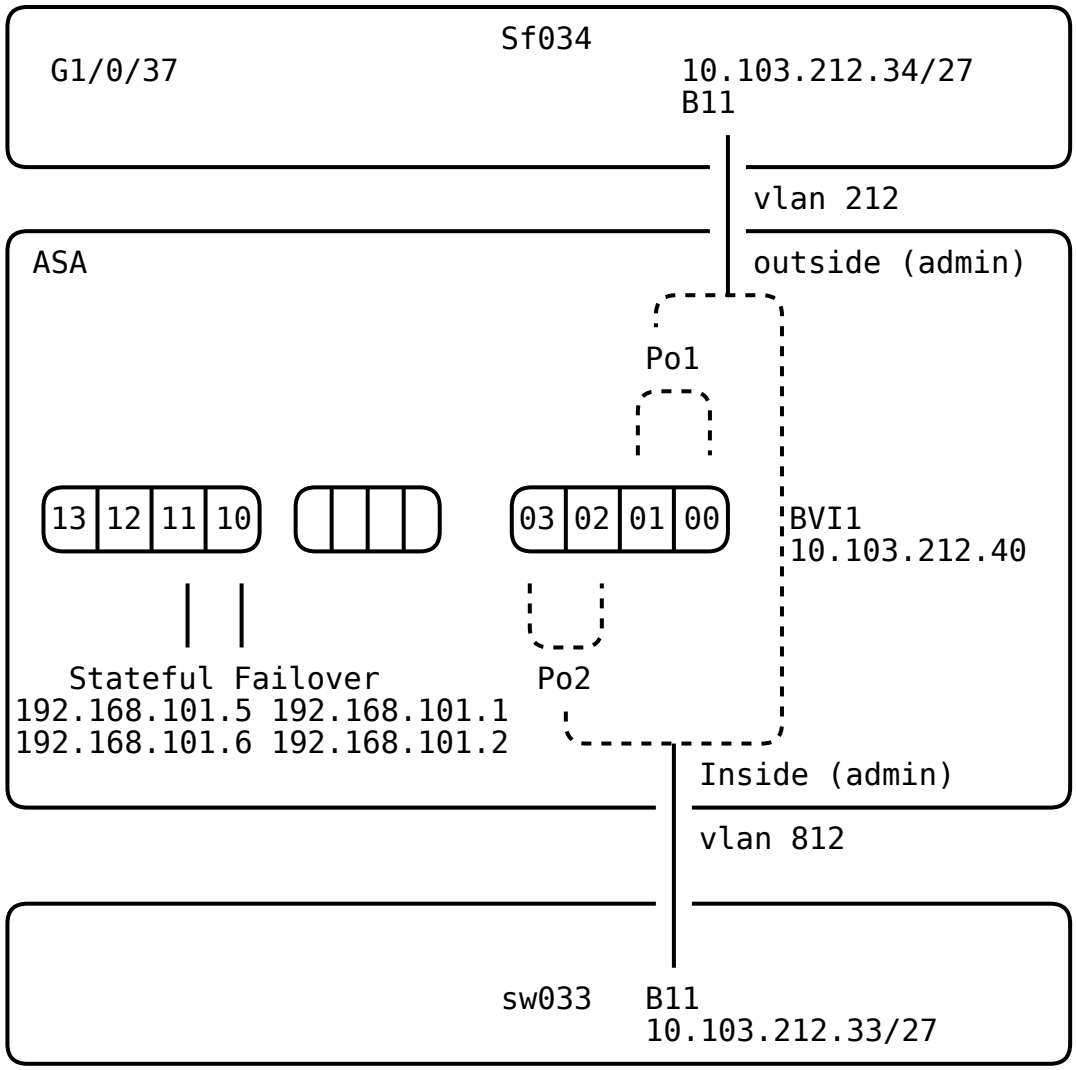
Synthèse

Passerelles à déclarer dans IP ROUTE sur le fédérateur

- D113 10.103.212.137
- E113 10.103.212.147
- G113 10.103.212.157

Configuration des VPNs D113 E113 et G113

Configuration des ASAs (10.103.214.53)



On va utiliser un second contexte en mode trasparent afin d'avoir des interfaces de pont dédiés (inside + outside).

Depuis le contexte system créer un contexte vpn:

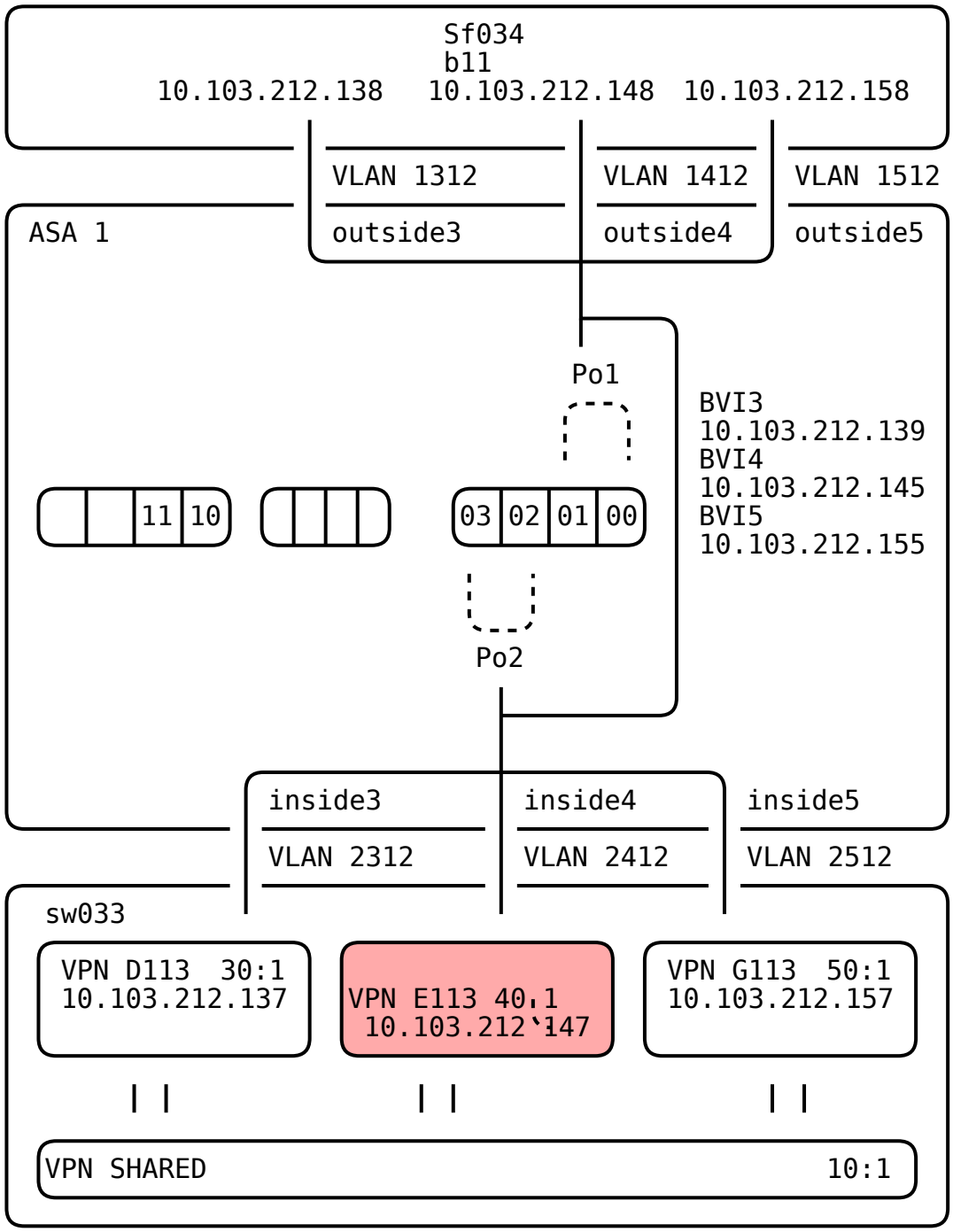
```
context vpn
description vpn
config-url disk0:/vpn.cfg
```

ID VPN	route-distinguisher	interface	VLAN	@IP sf034	@IP sw033	@IP ASA1	@IP ASA2	Masque
-	-	outside3	1312	10.103.212.138	-	-	-	255.255.255.248/29
-	-	outside4	1412	10.103.212.148	-	-	-	255.255.255.248/29
-	-	outside5	1512	10.103.212.158	-	-	-	255.255.255.248/29
-	-	BVI3	1312	-	-	10.103.212.139	10.103.212.140	255.255.255.248/29
-	-	BVI4	1412	-	-	10.103.212.145	10.103.212.146	255.255.255.248/29
-	-	BVI5	1512	-	-	10.103.212.155	10.103.212.156	255.255.255.248/29
SHARED	10:1	-	250	-	10.103.250.7	-	-	255.255.255.0/24
D113	30:1	inside3	2312	-	10.103.212.137	-	-	255.255.255.248/29
E113	40:1	inside4	2412	-	10.103.212.147	-	-	255.255.255.248/29
G113	50:1	inside5	2512	-	10.103.212.157	-	-	255.255.255.248/29

On va définir:

1. 3 interfaces outside sur le Port Channel Po1 pour les intercos vers le fédérateur

2. 3 interfaces inside sur le Port Channel Po2 pour les intercos des 3 VPNs.



Dans le contexte system créer les interfaces Port-channel:

```
context system
interface Port-channel1.1312
vlan 1312
interface Port-channel1.1412
vlan 1412
interface Port-channel1.1512
vlan 1512
interface Port-channel2.2312
```

```
vlan 2312
interface Port-channel2.2412
vlan 2412
interface Port-channel2.2512
vlan 2512
```

Dans la vue context vpn du system allouer les Port-channel:

```
context vpn
allocate-interface Port-channel1.1312
allocate-interface Port-channel1.1412
allocate-interface Port-channel1.1512
allocate-interface Port-channel2.2312
allocate-interface Port-channel2.2412
allocate-interface Port-channel2.2512
```

Vérifier:

```
show context
```

Passer le contexte vpn en mode transparent

```
changeto context vpn
firewall mode transparent
```

Toujours dans le contexte vpn configurer les interfaces Port-channel

```
interface Port-channel1.1312
 vlan 1312
interface Port-channel1.1412
 vlan 1412
interface Port-channel1.1512
 vlan 1512
interface Port-channel1.1312
 nameif outside3
 bridge-group 3
 security-level 3
interface Port-channel1.1412
 nameif outside4
 bridge-group 4
 security-level 4
interface Port-channel1.1512
 nameif outside5
 bridge-group 5
 security-level 5
interface Port-channel2.2312
 nameif inside3
```

```
 bridge-group 3
 security-level 3
interface Port-channel2.2412
 nameif inside4
 bridge-group 4
 security-level 4
interface Port-channel2.2512
 nameif inside5
 bridge-group 5
 security-level 5
```

Configurer les ACLs pour permettre le traffic entrant et sortant:

```
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
```

Configurer les interfaces BVI:

```
interface BVI3
ip address 10.103.212.139 255.255.255.248 standby 10.103.212.140
interface BVI4
ip address 10.103.212.145 255.255.255.248 standby 10.103.212.146
interface BVI5
ip address 10.103.212.155 255.255.255.248 standby 10.103.212.156
```

Configuration sw033 (10.103.212.33)

Créer les VLANs:

```
ip vpn-instance D113
route-distinguisher 30:1
vpn-target 30:1
description VPN D113 interco
ip vpn-instance E113
route-distinguisher 40:1
vpn-target 40:1
description VPN E113 interco
ip vpn-instance G113
route-distinguisher 50:1
vpn-target 50:1
description VPN G113 interco
```

Configurer les VLAN et les lier aux VPNs respectifs:

```
VLAN 2312
description VPN D113 interco
```

```
interface vlan 2312
ip binding vpn-instance D113
ip address 10.103.212.137 255.255.255.248

VLAN 2412
description VPN E113 interco

interface vlan 2412
ip binding vpn-instance E113
ip address 10.103.212.147 255.255.255.248

VLAN 2512
description VPN G113 interco

interface vlan 2512
ip binding vpn-instance G113
ip address 10.103.212.157 255.255.255.248
```

Configurer le permit vlan dans l'aggrégation B11:

```
int b11
port trunk permit vlan 2312 2412 2512
```

Configurer la route par défaut dans chaque VPN:

```
ip route-static vpn-instance D113 0.0.0.0 0.0.0.0 10.103.212.138
ip route-static vpn-instance E113 0.0.0.0 0.0.0.0 10.103.212.148
ip route-static vpn-instance G113 0.0.0.0 0.0.0.0 10.103.212.158
```

Configuration sf034 (10.103.212.34)

Configurer les VLANs:

```
VLAN 1312
description interco VPN D113
VLAN 1412
description interco VPN E113
VLAN 1512
description interco VPN G113
interface Vlan-interface1312
 ip address 10.103.212.138 255.255.255.248
interface Vlan-interface1412
 ip address 10.103.212.148 255.255.255.248
interface Vlan-interface1512
 ip address 10.103.212.158 255.255.255.248
```

Ajouter les routes statiques

```
ip route-static 10.103.212.136 255.255.255.248 10.103.212.137 description
interco D113 dans contexte VPN ASA
ip route-static 10.103.212.144 255.255.255.248 10.103.212.147 description
interco E113 dans contexte VPN ASA
ip route-static 10.103.212.152 255.255.255.248 10.103.212.157 description
interco G113 dans contexte VPN ASA
```

Lors du basculement des VLANs dans les VPNs il faut modifier les routes statiques des sous-réseaux backupés (10.103.214.0/24, 10.103.213.0/24, 10.103.212/24).

Configurer le permit des vlan 1312, 1412 et 1512 dans l'aggrégation B11:

```
int b11
port trunk permit vlan 1312 1412 1512
```

Configuration du VPN SHARED

Dans la configuration mise en œuvre ci-dessus tous les flux de et à destination des VPN doivent passer par le fédérateur. C'est également le cas des flux entre les VPN, même s'ils sont hébergés sur le même switch.

Si un VPN A veut envoyer un flux au VPN B qui se trouve sur le même switch, celui-ci prendra la route par défaut (sortie) pour revenir par l'interface dédié.

Ainsi tous les flux entre les GCOS et le Virtuo mutualisé connecté au switch sw033 prendrait ce chemin:

```
D113  ── sw033 ─interco VPN D113── sf034 ──interco sw033 ── sw033 ──Virtuo
virtuo── sw033 ─interco sw033──── sf034 ──interco VPN D213── sw033 ──D113
```

Ce n'est pas satisfaisant car cela engendre un traffic inutile entre le sw033 et le sf034.

Afin d'optimiser la configuration on va créer un VPN SHARED directement accessible depuis les autres VLAN.

Création du VLAN SHARED

```
ip vpn-instance SHARED
description VPN virtuo BULL
route-distinguisher 10:1
vpn-target 10:1
description VPN Virtuo
```

Pour le test on va créer un interface **Loopback0** afin de porter une addresse simulant un équipement à l'intérieur du VPN:

```
interface LoopBack0
ip binding vpn-instance SHARED
ip address 172.16.3.1 255.255.255.255
```

Configuration pour le rendre accessible

Pour le rendre accessible aux autres VLAN il faut ajouter:

- dans `ip vpn-instance SHARED` les route-distinguisher des autres VPN `vpn-target 30:1 40:1 50:1`
- dans `ip vpn-instance D113` la cible 10:1 (VPN SHARED) `vpn-target 10:1`
- dans `ip vpn-instance E113` la cible 10:1 (VPN SHARED) `vpn-target 10:1`
- dans `ip vpn-instance G113` la cible 10:1 (VPN SHARED) `vpn-target 10:1`

Ensuite les VPNs doivent être configurés pour échanger leurs routes, par exemple en BGP:

```
bgp 65000
 ip vpn-instance D113
  address-family ipv4 unicast
   network 10.103.214.0 255.255.255.0
 ip vpn-instance E113
  address-family ipv4 unicast
   network 10.103.213.0 255.255.255.0
 ip vpn-instance G113
  address-family ipv4 unicast
   network 10.103.212.0 255.255.255.0
 ip vpn-instance SHARED
  address-family ipv4 unicast
   network 10.103.250.0 255.255.255.0
```