Création et configuration des VPNs

Table of Contents

- Création et configuration des VPNs
  - Synthèse
  - Configuration des VPNs D113 E113 et G113
    - Configuration des ASAs (10.103.214.53)
    - Configuration sw033 (10.103.212.33)
    - Configuration sf034 (10.103.212.34)
  - Configuration du VPN SHARED
    - Création du VLAN SHARED
    - Configuration pour le rendre accessible

Mise en oeuvre des VPNs sur l'infrastructure BULL.

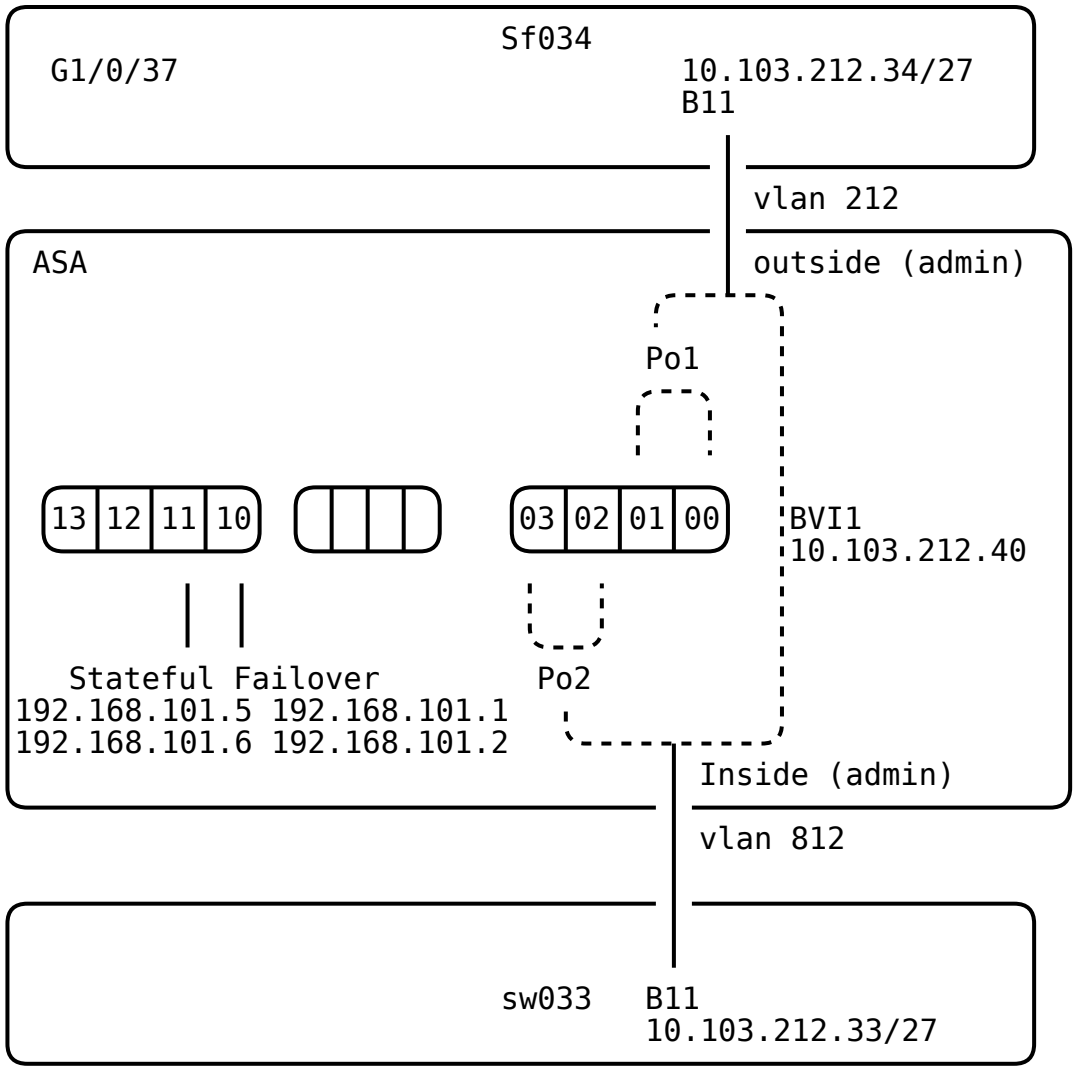
Synthèse

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)



En mode routed, dans un contexte donné, la route par défaut est unique. On va donc définir un seul interface outside mais plusieurs interfaces inside. On va utiliser un second contexte dans ce mode afin d'avoir des interfaces dédiés aux VPNs.

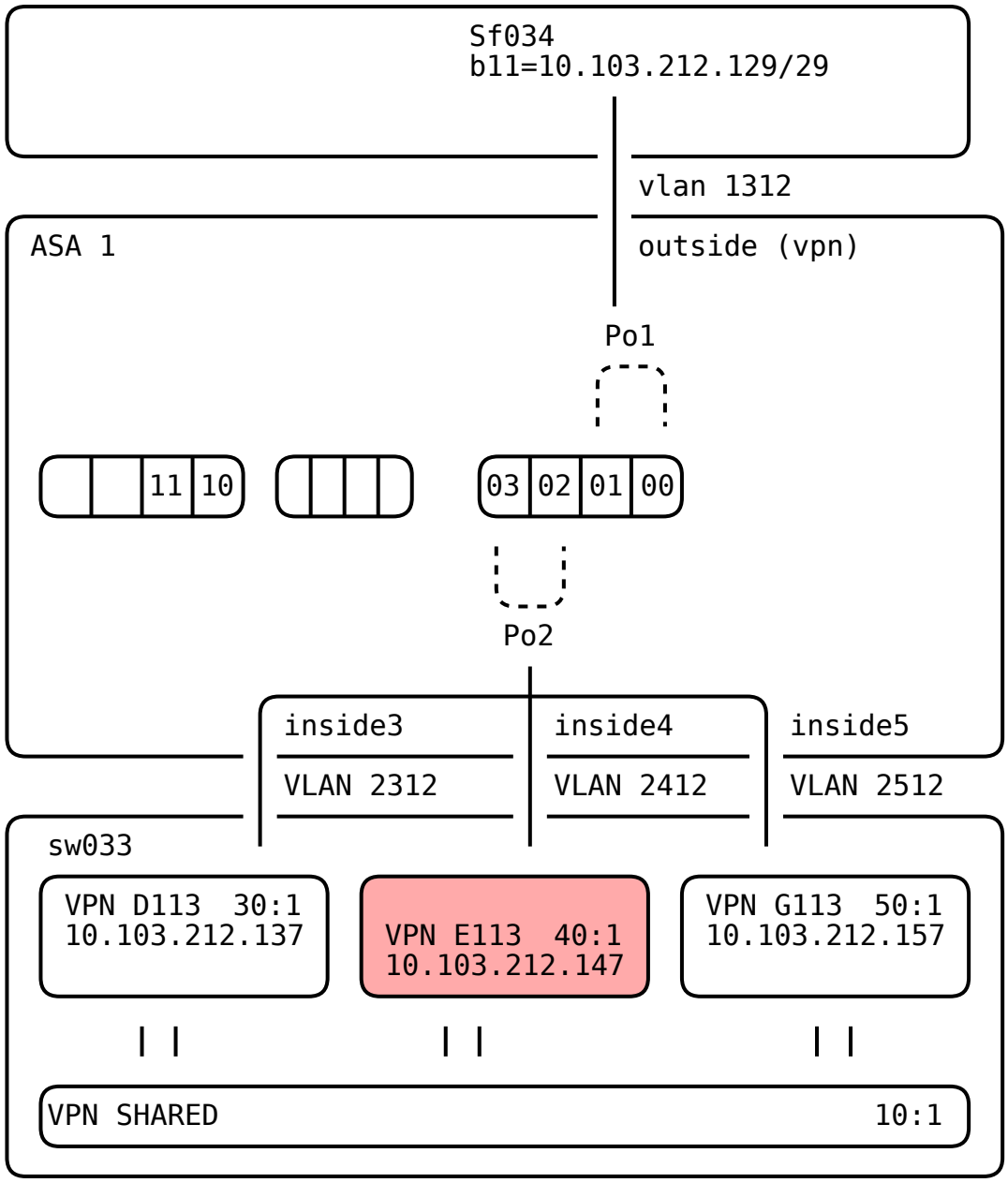
Depuis le contexte system créer un contexte vpn:

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

ID VPN	route-distinguisher	interface	VLAN	@IP sf034	@IP sw033	@IP ASA1	@IP ASA2	Masque
-	-	outside	1312	10.103.212.129	-	10.103.212.130	10.103.212.131	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	10.103.212.138	10.103.212.139	255.255.255.248/29
E113	40:1	inside4	2412	-	10.103.212.147	10.103.212.148	10.103.212.149	255.255.255.248/29
G113	50:1	inside5	2512	-	10.103.212.157	10.103.212.153	10.103.212.154	255.255.255.248/29

On va définir:

1. 1 interface outside sur le Port Channel Po1 pour l'interco 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-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-channel2.2312
allocate-interface Port-channel2.2412
allocate-interface Port-channel2.2512
```

Vérifier:

```
show context
```

Dans le contexte vpn configurer les interfaces Port-channel

```
changeto context vpn
interface Port-channel1.1312
nameif outside
security-level 0
ip address 10.103.212.130 255.255.255.248 standby 10.103.212.131
interface Port-channel2.2312
nameif inside3
security-level 0
ip address 10.103.212.138 255.255.255.248 standby 10.103.212.139
interface Port-channel2.2412
nameif inside4
security-level 0
ip address 10.103.212.148 255.255.255.248 standby 10.103.212.149
interface Port-channel2.2512
nameif inside5
security-level 0
ip address 10.103.212.158 255.255.255.248 standby 10.103.212.153
```

Configurer les ACLs pour permettre le traffic entrant et sortant:

```
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
access-list WAN-IN extended permit ip any any
access-list WAN-IN extended permit tcp any any
access-list WAN-IN extended permit icmp any any
access-group WAN-IN in interface outside
access-group WAN-IN out interface outside
access-group WAN-IN in interface inside3
access-group WAN-IN out interface inside3
access-group WAN-IN in interface inside4
access-group WAN-IN out interface inside4
access-group WAN-IN in interface inside5
access-group WAN-IN out interface inside5
```

Configurer les routes statiques:

```
```

```
route outside 0.0.0.0 0.0.0.0 10.103.212.129
route inside3 10.103.214.0 255.255.255.0 10.103.212.137
route inside4 10.103.212.0 255.255.255.0 10.103.212.147
route inside5 10.103.213.0 255.255.255.0 10.103.212.157
```

Il est nécessaire que les **ASAs** aient connaissance des routes des interfaces **inside**, afin de pouvoir orienter le flux entrant, mais leur configuration sans BVI introduit une coupure dans le flux entre l'interface **outside** et les interfaces **inside**.

Il faut donc utiliser un protocole de routage dynamique afin que les **VPNs** diffusent aux **ASAs** les routes vers les sous-réseaux qui leurs sont attachés.

* Dans les **ASAs** on instancie un serveur **OSPF**:

```
router ospf 130
router-id 10.103.212.130
network 10.0.0.0 255.0.0.0 area 130
```

* Dans chaque **VPN** du **sw033** on instancie un serveur **OSPF**:

```
ospf 130 router-id 10.103.212.137 vpn-instance D113
area 0.0.0.130
network 10.0.0.0 0.255.255.255
#
ospf 140 router-id 10.103.212.147 vpn-instance E113
area 0.0.0.130
network 10.0.0.0 0.255.255.255
#
ospf 150 router-id 10.103.212.157 vpn-instance G113
area 0.0.0.130
network 10.0.0.0 0.255.255.255
```

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 VPN D113 TEST interco

interface vlan 1312
ip address 10.103.212.129 255.255.255.248
```

Ajouter les routes statiques

```
ip route-static 10.103.212.136 255.255.255.248 10.103.212.130 description
interco D113 dans contexte VPN ASA
ip route-static 10.103.212.144 255.255.255.248 10.103.212.130 description
interco E113 dans contexte VPN ASA
ip route-static 10.103.212.152 255.255.255.248 10.103.212.130 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 du vlan 1312 dans l'aggrégation B11:

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

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
```

From:
http://www.ouarte.garden/ - **dwndoc**

Permanent link:
http://www.ouarte.garden/doku.php?id=journal:2024:day-2024-02-15

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