Test VPN D113

Table of Contents

Atelier de mise en oeuvre des VPNs sur une infrastructure de test.

Configuration du VPN D113

Création d'un contexte en mode routed

L'interface de pont ne peut gérer qu'un couple d'interface (inside + outside) et, dans un contexte donné, la route par défaut est unique. Pour définir plusieurs interfaces il faut utiliser le mode routed, donc on va utiliser un second contexte dans ce mode afin d'avoir des interfaces dédiés aux VPNs.

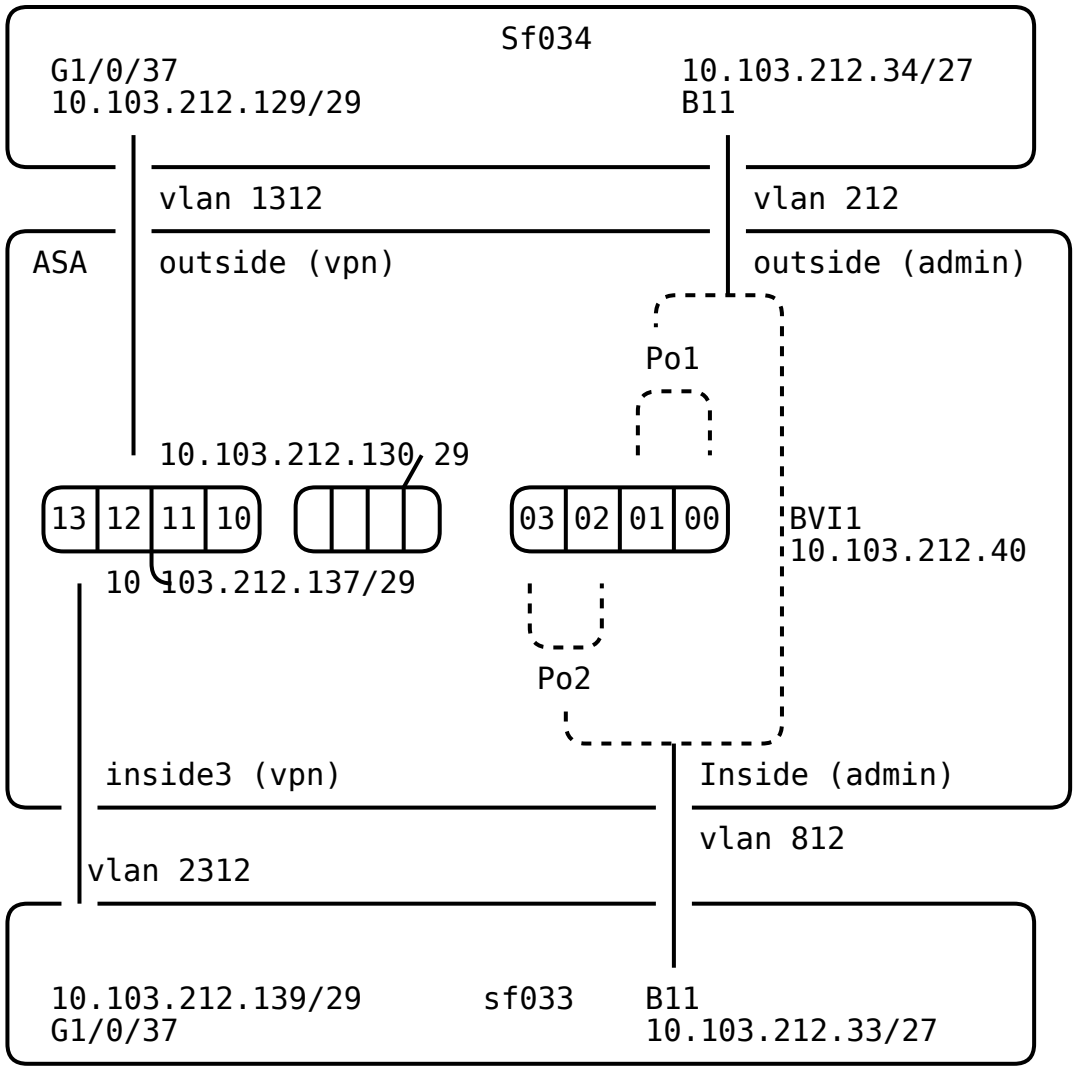
Depuis le contexte system créer un contexte vpn:

```
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	10.103.21×2.153	10.103.212.154	255.255.255.248/29

Configuration des ASA (10.103.214.53) avec des interfaces dédiés

Infrastructure de test comprenant deux interfaces du fédérateur (G1/0/37 et G2/0/37), les deux interfaces restants sur les ASA (1/2 et 1/3) et deux interfaces sur le switch 33 (G1/0/37 et G2/0/37) un VPN avec deux VLAN un vlan d'interco + 1 vlan de test ave une @ip de passerelle



L'inconvénient de cette infrastructure est que l'on dispose de peut d'nterfaces sur les appliances et que les interfaces de la carte d'extension ne peuvent pas être agrégées dans un PortChannel.

Dans la vue contexte vpn du system attribuer les ports 1/2 et 1/3:

```
context vpn
allocate-interface GigabitEthernet1/2
allocate-interface GigabitEthernet1/3
```

Dans le contexte system activer les interfaces:

```
interface GigabitEthernet1/2
no shutdown
interface GigabitEthernet1/3
no shutdown
```

Vérifier:

```
show context
```

Dans le contexte vpn configurer les interfaces GigabitEthernet1/2 et GigabitEthernet1/3:

```
changeto context vpn
interface GigabitEthernet1/2
nameif outside3
security-level 0
ip address 10.103.212.130 255.255.255.248 standby 10.103.212.131
interface GigabitEthernet1/3
nameif inside3
security-level 0
ip address 10.103.212.137 255.255.255.248 standby 10.103.212.138
```

Configurer les ACLs pour permettre le traffic entrant et sortant:

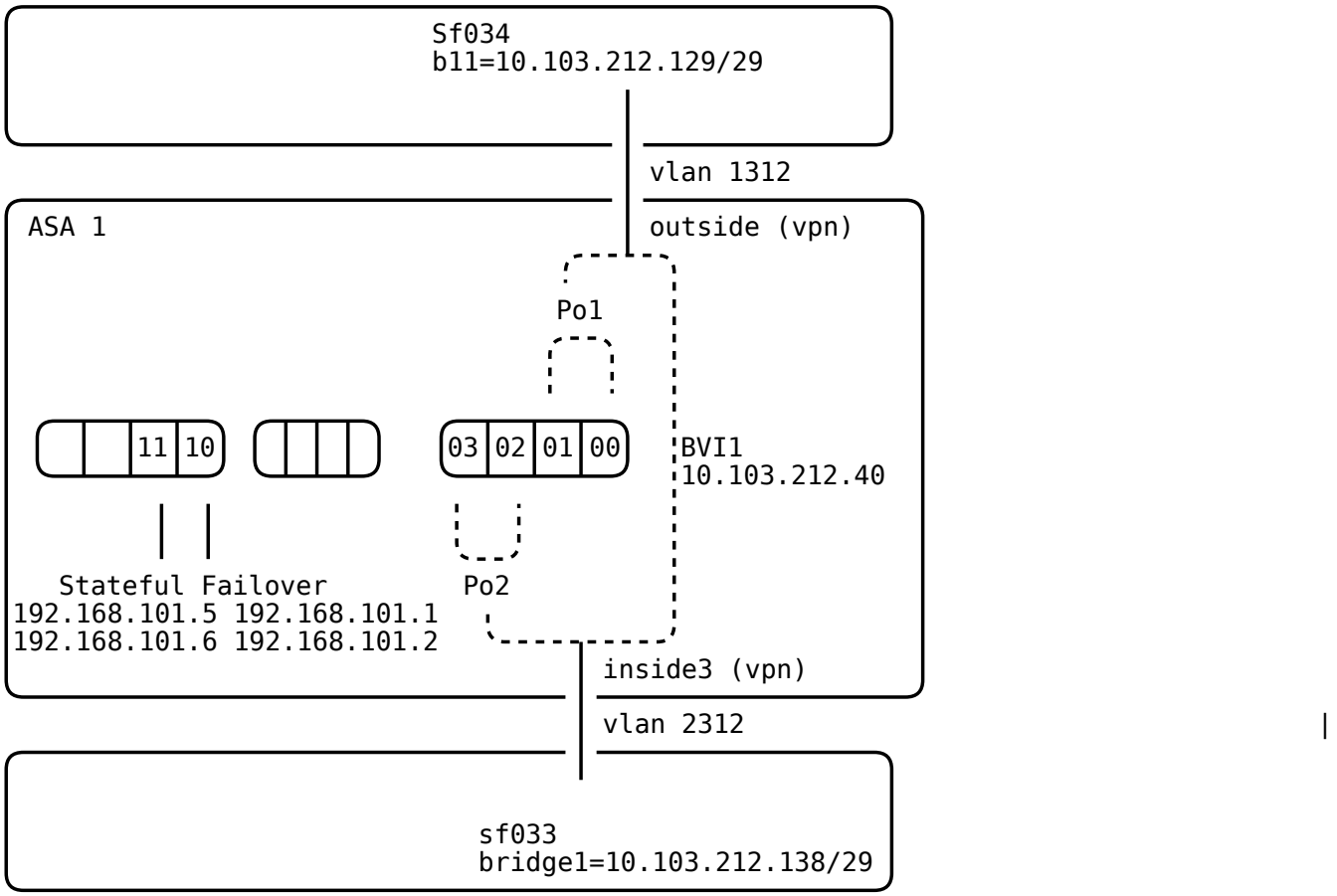
```
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
access-list WAN-IN extended permit ip any any
access-list WAN-IN extended permit tcp any any
access-list WAN-IN extended permit icmp any any
access-group WAN-IN in interface outside
access-group WAN-IN out interface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

Configurer les routes statiques:

```
route inside3 192.168.254.0 255.255.255.0 10.103.212.139
route outside 0.0.0.0 0.0.0.0 10.103.212.129
```

Configuration des ASA (10.103.214.53) avec le lien d'interco existant

Il est possible de définir plus d'un VLAN sur les ports de l'aggégation BVI existante.



Dans le contexte system configurer les Port-channel1.1312 et Port-channel2.2312

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

Dans la vue contexte vpn du system attribuer les Port-channel1.1312 et Port-channel2.2312:

```
context vpn
allocate-interface Port-channel1.1312
allocate-interface Port-channel2.2312
```

Vérifier:

```
show context
```

Dans le contexte vpn configurer les interfaces Port-channel1.1312 et Port-channel2.2312:

```
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
```

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
```

Configurer les routes statiques:

```
route inside3 192.168.254.0 255.255.255.0 10.103.212.137
route outside 0.0.0.0 0.0.0.0 10.103.212.129
```

Configuration sw033 (10.103.212.33)

Configurer le VLAN 312 et le lier au VPN D113

```
ip vpn-instance D113
route-distinguisher 30:1
vpn-target 30:1
description VPN D113 TEST interco


VLAN 2312
description VPN D113 TEST interco

interface vlan 2312
ip binding vpn-instance D113
ip address 10.103.212.139 255.255.255.248

VLAN 354
description VLAN 254 TEST

interface vlan 354
ip binding vpn-instance D113
ip 192.168.254.7 255.255.255.255.0
```

Configurer le permit vlan dans l'aggrégation B11:

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

On va également créer un interface **Loopback3** pour avoir un interface monté dans le VPN

```
interface Loopback 3
ip binding vpn-instance D113
ip 192.168.254.33 255.255.255.255.0
```

Configurer la route par défaut du VPN D213

```
ip vpn instance D113 route-static 0.0.0.0 0.0.0.0 10.103.212.137
```

Configuration sf034 (10.103.212.34)

Configurer le VLAN 1312

```
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 192.168.254.0 24 10.103.212.130
ip route-static 10.103.212.136 255.255.255.248 10.103.212.130
```

Configurer le permit vlan dans l'aggrégation B11:

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

Configuration du VPN SHARED

Dans la configuration mise en oeuvre 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'inetrface 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 VPN 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` la cible 30:1 (VPN D113) `route-target 30:1`
- dans `ip vpn-instance D113` la cible 10:1 (VPN SHARED) `route-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 10.103.212.137 255.255.255.255
 ip vpn-instance SHARED
  address-family ipv4 unicast
   network 172.16.3.1 255.255.255.255
```