Configurar o Fusion Router no SDA

Contents

Introduction

Este documento descreve como configurar o Fusion Routers em uma solução Cisco Software-Defined Access (SDA).

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

> Observação: a configuração é necessária de acordo com os dispositivos suportados que podem ser encontrados em [Link para notas de versão](#)

Componentes Utilizados

As informações neste documento são baseadas nas seguintes versões de hardware:

- DNAC - Versão 1.2.1
- Borda e Borda - Switch Cat3k Cisco
- Fusion - Roteador Cisco com suporte para vazamento de Inter-VRF

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Na solução Cisco SD-Access, os dispositivos são gerenciados e configurados pelo Cisco DNA Center. Em geral, todas as partes da malha do SD-Access podem ser, e normalmente são, configuradas e gerenciadas pelo Cisco DNA Center. O dispositivo Fusion está fora da estrutura, portanto, é configurado manualmente. A automação de fronteiras, discutida a seguir, é um recurso do Cisco DNA Center que pode automatizar a configuração de fronteiras para a transferência de VRFs para os dispositivos Fusion.

Ocasionalmente, por razões geralmente relacionadas à compatibilidade com a configuração atual, a automação de fronteiras não é adequada e, portanto, a transferência da borda para o dispositivo Fusion também pode ser configurada manualmente. Uma compreensão da configuração usada ajuda a ilustrar detalhes importantes sobre a configuração e a operação ideais do sistema geral.

Funcionalidade de um dispositivo de fusão em uma solução de acesso SD do DNA

Um dispositivo Fusion permite o vazamento de VRF (Virtual Routing and Forwarding, roteamento e encaminhamento virtual) em domínios de malha de acesso SD e permite a conectividade de host para serviços compartilhados, como DHCP, DNS, NTP, ISE, Cisco DNA Center, Wireless LAN Controllers (WLC) e similares. Embora essa função possa ser desempenhada por outros dispositivos que não os roteadores, este documento se concentra em roteadores como dispositivos Fusion.

Como mencionado anteriormente, os serviços compartilhados devem ser disponibilizados para todas as redes virtuais (VNs) no campus. Isso é obtido com a criação de peers Border Gateway Protocol (BGP) dos Border Routers para os Fusion Routers. No Fusion Router, as sub-redes do VRF de estrutura que precisam de acesso a esses serviços compartilhados vazam para a GRT, ou para um VRF de serviços compartilhados, e vice-versa. Os mapas de rotas podem ser usados para ajudar a conter tabelas de roteamento para sub-redes específicas da malha de acesso SD.

> Observação: os nós de borda de acesso SD não suportam rotas de sumarização que se sobrepõem aos pools de IP de acesso SD. As rotas de sumarização que se sobrepõem a Pools IP devem ser filtradas nos anúncios de roteamento dos dispositivos Fusion para os nós de borda.

Configurar

Os detalhes de configuração fornecidos aqui dizem respeito à topologia de rede mostrada a seguir. Esta topologia de rede não é uma topologia recomendada para implantações. Ele é usado aqui apenas para facilitar a apresentação das amostras de configuração fornecidas. Para obter os projetos de implantação recomendados, consulte a [Design Zone for Cisco Digital Network Architecture](#).

Diagrama de Rede

A topologia usada para este artigo consiste em dois roteadores de borda configurados como fronteiras externas e dois roteadores de fusão com uma conexão para cada roteador de borda respectivo.
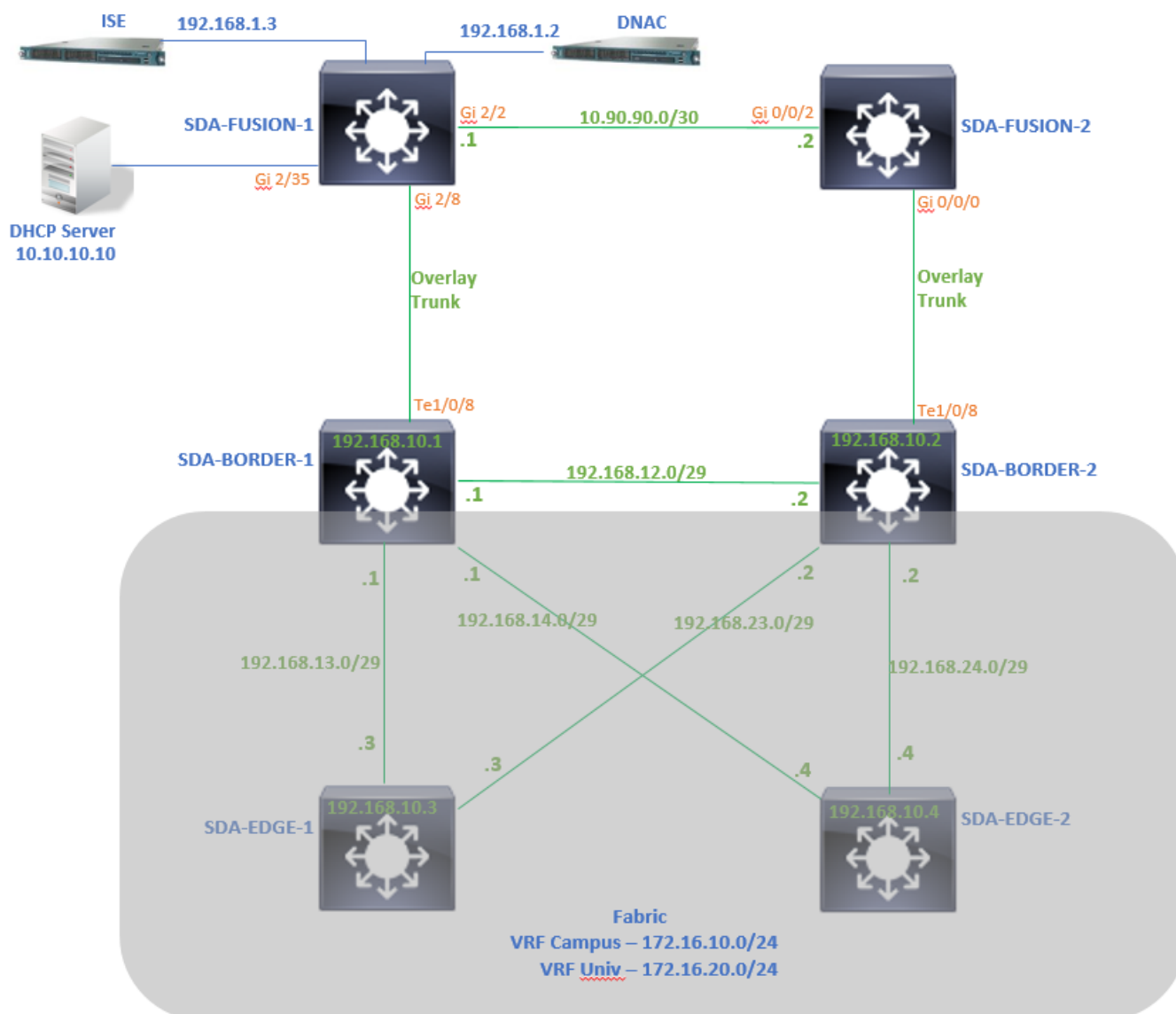
Configurações

Etapa 1. Configurar o link de transferência a partir do DNAC

Na etapa de atribuir aos dispositivos uma função de roteador de borda enquanto ele é adicionado

à estrutura, um link de entrega pode ser criado. Na camada 2, é um link de tronco conectado ao Fusion Router. As próximas etapas são necessárias:

1. Configure o número AS local para BGP. Esse número de sistema autônomo (AS) é usado para configurar o processo BGP nos roteadores de borda.

2. Adicione a interface em Trânsito. Esta interface é a conexão direta entre o Border e o Fusion Router. (O 1/0/8 em Borda neste exemplo).

SDA-Border1

Border to
- ○ Rest of Company (Internal)
- ◉ Outside World (External)
- ○ Anywhere (Internal & External)

Local Autonomous Number
65005

ⓘ
Select Ip Pool
✖ BGP (10.50.50.0/24)   ⌄

ⓘ
☑ Connected to the Internet

Transit

⌄   Add

⌄   ABC   🗑

External Interface ⓘ   ⊕ Add Interface

Interface	Number of VN
TenGigabitEthernet1/0/8	2

3. Configure o Número de AS Remoto. Esse número AS é usado em Border Routers para instruções de vizinhos em direção ao Fusion Router para configurar peers de BGP Externo (eBGP).

4. Selecione todas as Virtual Networks (VRFs) para as quais o vazamento de VRF é necessário no Fusion Router.

5. Implante a configuração de DNAC para Dispositivos.

External Interface

✖ TenGigabitEthernet1/0/8   ⌄

Remote AS Number

65004

ℹ️
This number is automatically derived from the selected Transit.
The selected autonomous system number will be used to automate IP routing between Border Node and remote peer.

⌄ ◼️ Virtual Network

☐ DEFAULT_VN

☐ INFRA_VN

☑ Univ

☑ Campus

Use as mesmas etapas para o dispositivo SDA-Border-2.

Etapa 2. Verificar configurações enviadas por DNAC em roteadores de borda

Esta seção abrange a verificação da configuração em roteadores de borda relacionados ao protocolo BGP.

SDA-Borda-1

```
SDA-Border1#show run interface loopback 0
!
interface Loopback0
ip address 192.168.10.1 255.255.255.255
ip router isis
end


SDA-Border1#show run interface tenGigabitEthernet 1/0/8
!
interface TenGigabitEthernet1/0/8
switchport mode trunk
end


SDA-Border1#show run interface loopback 1021

interface Loopback1021
description Loopback Border
vrf forwarding Campus
ip address 172.16.10.1 255.255.255.255
end


SDA-Border1#show run interface loopback 1022
```

```
interface Loopback1022
description Loopback Border
vrf forwarding Univ
ip address 172.16.20.1 255.255.255.255
end


SDA-Border1#show run | section vrf definition Campus
vrf definition Campus
rd 1:4099
!
address-family ipv4
route-target export 1:4099
route-target import 1:4099
exit-address-family


SDA-Border1#show run | section vrf definition Univ
vrf definition Univ
rd 1:4100
!
address-family ipv4
route-target export 1:4100
route-target import 1:4100
exit-address-family
SDA-Border1#


SDA-Border1#show run interface vlan 3007
!
interface Vlan3007 <<< SVI created for BGP Peering under VRF Campus
description vrf interface to External router
vrf forwarding Campus
ip address 10.50.50.25 255.255.255.252
no ip redirects
ip route-cache same-interface
end

SDA-Border1#show run interface vlan 3006
!
interface Vlan3006 <<< SVI created for BGP Peering under VRF Univ
description vrf interface to External router
vrf forwarding Univ
ip address 10.50.50.21 255.255.255.252
no ip redirects
ip route-cache same-interface
end


SDA-Border1#show run | section bgp
router bgp 65005 <<< Local AS Number from DNAC
bgp router-id interface Loopback0
bgp log-neighbor-changes
bgp graceful-restart
!
address-family ipv4
network 192.168.10.1 mask 255.255.255.255
redistribute lisp metric 10
exit-address-family
!
address-family ipv4 vrf Campus
bgp aggregate-timer 0
network 172.16.10.1 mask 255.255.255.255 <<< Anycast IP for Pool in VRF Campus
aggregate-address 172.16.10.0 255.255.255.0 summary-only <<< Only Summary is Advertised
```

```
redistribute lisp metric 10
neighbor 10.50.50.26 remote-as 65004 <<< Peer IP to be used on Fusion for VRF Campus and Remote
AS Number from DNAC
neighbor 10.50.50.26 update-source Vlan3007
neighbor 10.50.50.26 activate
neighbor 10.50.50.26 weight 65535 <<< Weight needed for Fusion peering to make sure locally
originated path from LISP is never preferred
exit-address-family
!
address-family ipv4 vrf Univ
bgp aggregate-timer 0
network 172.16.20.1 mask 255.255.255.255 <<< Anycast IP for Pool in VRF Univ
aggregate-address 172.16.20.0 255.255.255.0 summary-only
redistribute lisp metric 10
neighbor 10.50.50.22 remote-as 65004
neighbor 10.50.50.22 update-source Vlan3006
neighbor 10.50.50.22 activate
neighbor 10.50.50.22 weight 65535
exit-address-family
```

SDA-Borda-2

```
SDA-Border2#show run interface loopback 0
!
interface Loopback0
 ip address 192.168.10.2 255.255.255.255
 ip router isis
end

SDA-Border2#show run interface tenGigabitEthernet 1/0/8
!
interface TenGigabitEthernet1/0/8
 switchport mode trunk
end



SDA-Border2#show run interface loopback 1021
!
interface Loopback1021
description Loopback Border
vrf forwarding Campus
ip address 172.16.10.1 255.255.255.255
end

SDA-Border2#show run interface loopback 1022
!
interface Loopback1022
description Loopback Border
vrf forwarding Univ
ip address 172.16.20.1 255.255.255.255
end
SDA-Border2#show run | section vrf definition Campus vrf definition Campus rd 1:4099 ! address-
family ipv4 route-target export 1:4099 route-target import 1:4099 exit-address-family SDA-
Border2#show run | section vrf definition Univ vrf definition Univ rd 1:4100 ! address-family
ipv4 route-target export 1:4100 route-target import 1:4100 exit-address-family SDA-Border2#show
run interface vlan 3001 ! interface Vlan3001 description vrf interface to External router vrf
forwarding Campus ip address 10.50.50.1 255.255.255.252 no ip redirects ip route-cache same-
interface end SDA-Border2#show run interface vlan 3003 ! interface Vlan3003 description vrf
interface to External router vrf forwarding Univ ip address 10.50.50.9 255.255.255.252 no ip
redirects ip route-cache same-interface end SDA-Border2#show run | section bgp router bgp 65005
bgp router-id interface Loopback0 bgp log-neighbor-changes bgp graceful-restart ! address-family
```

```
ipv4 network 192.168.10.2 mask 255.255.255.255 redistribute lisp metric 10 exit-address-family !
address-family ipv4 vrf Campus bgp aggregate-timer 0 network 172.16.10.1 mask 255.255.255.255
aggregate-address 172.16.10.0 255.255.255.0 summary-only redistribute lisp metric 10 neighbor
10.50.50.2 remote-as 65004 neighbor 10.50.50.2 update-source Vlan3001 neighbor 10.50.50.2
activate neighbor 10.50.50.2 weight 65535 exit-address-family ! address-family ipv4 vrf Univ bgp
aggregate-timer 0 network 172.16.20.1 mask 255.255.255.255 aggregate-address 172.16.20.0
255.255.255.0 summary-only redistribute lisp metric 10 neighbor 10.50.50.10 remote-as 65004
neighbor 10.50.50.10 update-source Vlan3003 neighbor 10.50.50.10 activate neighbor 10.50.50.10
weight 65535 exit-address-family
```

Etapa 3. Configurar alocação em roteadores de borda

Devido ao vazamento de VRF no roteador Fusion, a família de endereços ipv4 para campus VRF aprende a rota originada pelo VRF Univ (172.16.20.0/24). No entanto, tanto o roteador de origem quanto o de aprendizagem têm o mesmo número AS de BGP (65005). Para superar os mecanismos de prevenção de loop BGP e aceitar/instalar as rotas em Border Routers, **alowas-in** deve ser configurado para os peers com o Fusion Router:

```
SDA-Border1

SDA-Border1(config)#router bgp 65005
SDA-Border1(config-router)#address-family ipv4 vrf Campus
SDA-Border1(config-router-af)#neighbor 10.50.50.26 allowas-in
SDA-Border1(config-router-af)#exit-address-family
SDA-Border1(config-router)#
SDA-Border1(config-router)#address-family ipv4 vrf Univ
SDA-Border1(config-router-af)#neighbor 10.50.50.22 allowas-in
SDA-Border1(config-router-af)#exit-address-family
SDA-Border1(config-router)#
```

```
SDA-Border2

SDA-Border2(config)#router bgp 65005
SDA-Border2(config-router)#address-family ipv4 vrf Campus
SDA-Border2(config-router-af)#neighbor 10.50.50.2 allowas-in
SDA-Border2(config-router-af)#exit-address-family
SDA-Border2(config-router)#
SDA-Border2(config-router)#address-family ipv4 vrf Univ
SDA-Border2(config-router-af)#neighbor 10.50.50.10 allowas-in
SDA-Border2(config-router-af)#exit-address-family
SDA-Border2(config-router)#
```

Observação: o comando **allowas-in** deve ser usado com precaução, pois pode causar loops. Quando você usa apenas um dispositivo Fusion com o qual ambas as Bordas fazem peer, a filtragem é necessária para garantir que as rotas originadas localmente não sejam aceitas de volta para o AS a partir do peer Fusion - dentro do mesmo VN. Se isso acontecer, o caminho eBGP tem preferência sobre o caminho originado localmente devido ao peso máximo para caminhos eBGP.

Etapa 4. Configurar Roteadores Fusion

Esta seção ilustra a configuração manual dos roteadores Fusion.

SDA-Fusion-1

Configure o link em direção ao roteador de borda como um tronco para corresponder à configuração de vlan em Border-1:

```
interface GigabitEthernet2/8
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 3006, 3007
 switchport mode trunk
end
```

Configure os VRFs necessários:

```
vrf definition Campus
 rd 1:4099
 !
 address-family ipv4
  route-target export 1:4099
  route-target import 1:4099
 exit-address-family
!

vrf definition Univ
 rd 1:4100
 !
 address-family ipv4
  route-target export 1:4100
  route-target import 1:4100
 exit-address-family
```

Configurar interfaces SVI:

```
interface Vlan3007
 vrf forwarding Campus
 ip address 10.50.50.26 255.255.255.252
end

interface Vlan3006
 vrf forwarding Univ
 ip address 10.50.50.22 255.255.255.252
end
```

Configure o peering de BGP externo (eBGP) com SDA-Border-1:

```
router bgp 65004                             <<< Remote AS from DNAC
 bgp log-neighbor-changes
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv4 vrf Campus
  neighbor 10.50.50.25 remote-as 65005
  neighbor 10.50.50.25 update-source Vlan3007
  neighbor 10.50.50.25 activate
 exit-address-family
 !
```

```
address-family ipv4 vrf Univ
 neighbor 10.50.50.21 remote-as 65005
 neighbor 10.50.50.21 update-source Vlan3006
 neighbor 10.50.50.21 activate
exit-address-family
```

Configure o peering de BGP interno (iBGP) com SDA-Fusion-2:

```
interface GigabitEthernet2/2
 description SDA-Fusion1--->SDA-Fusion2
 ip address 10.90.90.1 255.255.255.252
end

router bgp 65004
 neighbor 10.90.90.2 remote-as 65004
 !
 address-family ipv4
  neighbor 10.90.90.2 activate
 exit-address-family
 !
```

Anuncie a sub-rede do servidor DHCP na família de endereços global onde o IP do servidor DHCP é 10.10.10.10:

```
interface GigabitEthernet2/35
 description connection to DHCP server
 ip address 10.10.10.9 255.255.255.252
end


router bgp 65004
 !
 address-family ipv4
  network 10.10.10.8 mask 255.255.255.252
 exit-address-family
 !
```

SDA-Fusion-2

Configure o link em direção ao roteador de borda. Se uma interface no Fusion for L3 em vez de trunk - configure as subinterfaces:

```
interface GigabitEthernet0/0/0.3001
 encapsulation dot1Q 3001
 vrf forwarding Campus
 ip address 10.50.50.2 255.255.255.252
end

interface GigabitEthernet0/0/0.3003
 encapsulation dot1Q 3003
 vrf forwarding Univ
 ip address 10.50.50.10 255.255.255.252
end
```

Configure os VRFs correspondentes:

```
vrf definition Campus
 rd 1:4099
 !
 address-family ipv4
  route-target export 1:4099
  route-target import 1:4099
 exit-address-family
!
!
vrf definition Univ
 rd 1:4100
 !
 address-family ipv4
  route-target export 1:4100
  route-target import 1:4100
 exit-address-family
!
```

Configure o Peering de eBGP com SDA-Border-2:

```
router bgp 65004
 bgp log-neighbor-changes
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv4 vrf Campus
  neighbor 10.50.50.1 remote-as 65005
  neighbor 10.50.50.1 update-source GigabitEthernet0/0/0.3001
  neighbor 10.50.50.1 activate
 exit-address-family
 !
 address-family ipv4 vrf Univ
  neighbor 10.50.50.9 remote-as 65005
  neighbor 10.50.50.9 update-source GigabitEthernet0/0/0.3003
  neighbor 10.50.50.9 activate
 exit-address-family
```

Configure o Peering de iBGP com SDA-Fusion-1:

```
interface GigabitEthernet0/0/2
ip address 10.90.90.2 255.255.255.252
negotiation auto
end

router bgp 65004 neighbor 10.90.90.1 remote-as 65004 ! address-family ipv4 neighbor 10.90.90.1
activate exit-address-family
```

Etapa 5. Configurar Vazamento de VRF no Fusion Router

A configuração para vazamento de VRF é idêntica para os roteadores de fusão SDA-Fusion-1 e SDA-Fusion-2.

Primeiro, configure o vazamento de VRF entre os dois VRFs (Campus e Univ), use **importação de destino de rota**:

```
vrf definition Campus
 !
 address-family ipv4
route-target export 1:4099 route-target import 1:4099
route-target import 1:4100 <<< Import VRF Univ prefixes in VRF Campus
exit-address-family
!
vrf definition Univ
!
address-family ipv4
route-target export 1:4100 route-target import 1:4100
route-target import 1:4099 <<< Import VRF Campus prefixes in VRF Univ
exit-address-family
!
```

Em seguida, configure o vazamento de rota entre a Tabela de Roteamento Global (GRT) para os VRFs e dos VRFs para a GRT, use **import ... map** e **export ... map**:

```
ip prefix-list Campus_Prefix seq 5 permit 172.16.10.0/24    <<< Include Prefixes belonging to
VRF Campus
ip prefix-list Global_Prefix seq 5 permit 10.10.10.8/30     <<< Include Prefixes belonging to
Global (eq DHCP Server Subnet)
ip prefix-list Univ_Prefix seq 5 permit 172.16.20.0/24      <<< Include Prefixes belonging to
VRF Univ

route-map Univ_Map permit 10
 match ip address prefix-list Univ_Prefix
route-map Global_Map permit 10
 match ip address prefix-list Global_Prefix
route-map Campus_Map permit 10
 match ip address prefix-list Campus_Prefix


vrf definition Campus
 !
 address-family ipv4
  import ipv4 unicast map Global_Map     <<< Injecting Global into VRF Campus matching route-map
Global_Map
export ipv4 unicast map Campus_Map <<< Injecting VRF Campus into Global matching route-map
Campus_Map
exit-address-family
!
vrf definition Univ
!
address-family ipv4
import ipv4 unicast map Global_Map <<< Injecting Global into VRF Univ matching route-map
Global_Map
export ipv4 unicast map Univ_Map <<< Injecting VRF Univ into Global matching route-map Univ_Map
exit-address-family
!
```

Verificar

Esta seção contém etapas de verificação para garantir que a configuração anterior tenha entrado em vigor corretamente.

Etapa 1. Verificar o Peering eBGP entre os Roteadores Fusion e Border

SDA-Border-1 ------Peering--------SDA-Fusion-1

```
SDA-Border1#show ip bgp vpnv4 vrf Campus summary

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.50.50.26     4        65004   1294    1295       32    0    0 19:32:22         2




SDA-Border1#show ip bgp vpnv4 vrf Univ summary

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.50.50.22     4        65004   1294    1292       32    0    0 19:32:57         2



----------------------------------------------------


SDA-Fusion1#show ip bgp vpnv4 vrf Campus summary

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.50.50.25     4        65005   1305    1305       31    0    0 19:41:58         1


SDA-Fusion1#show ip bgp vpnv4 vrf Univ summary

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.50.50.21     4        65005   1303    1305       31    0    0 19:42:14         1
```

SDA-Border-2 ------Peering--------SDA-Fusion-2

```
SDA-Border2#show ip bgp vpnv4 vrf Campus summary

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.50.50.2      4        65004      6       6       61    0    0 00:01:37         2


SDA-Border2#show ip bgp vpnv4 vrf Univ summary

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.50.50.10     4        65004      6       6       61    0    0 00:01:39         2

------------------------------------------------------------------------------

SDA-Fusion2#show ip bgp vpnv4 vrf Campus summary

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.50.50.1      4        65005     17      17        9    0    0 00:11:16         1


SDA-Fusion2#show ip bgp vpnv4 vrf Univ summary

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.50.50.9      4        65005     17      17        9    0    0 00:11:33         1
```

Etapa 2. Verificar o Peering iBGP entre ambos os Roteadores Fusion

SDA-Fusion-1 ------Peering--------SDA-Fusion-2

```
SDA-Fusion1#show ip bgp summary
```

```
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.90.90.2      4        65004     10      12       12    0    0 00:04:57         2


-------------------------------------------------------------

SDA-Fusion2#show ip bgp summary

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.90.90.1      4        65004     19      17        4    0    0 00:11:35         3
```

Etapa 3. Verificar prefixos na tabela BGP e na tabela de roteamento

SDA-Borda-1

```
SDA-Border1#show ip bgp vpnv4 vrf Campus

     Network          Next Hop          Metric LocPrf Weight Path
Route Distinguisher: 1:4099 (default for vrf Campus)
 *>   10.10.10.8/30    10.50.50.26                       65535 65004 i        <<< Prefix
leaked from Global Routing Table on Fusion
 *>   172.16.10.0/24   0.0.0.0                           32768 i              <<< VRF Campus
originated prefix
 *>   172.16.20.0/24   10.50.50.26                       65535 65004 65005 i  <<< Prefix
originated in VRF Univ, leaked on Fusion to VRF Campus


SDA-Border1#show ip route vrf Campus bgp Routing Table: Campus B 10.10.10.8/30 [20/0] via
10.50.50.26, 20:30:30 <<< RIB entry for DHCP Server pool prefix B 172.16.10.0/24 [200/0],
20:32:45, Null0 <<< Null entry created by "aggregate-address" BGP configuration B 172.16.20.0/24
[20/0] via 10.50.50.26, 20:32:45 <<< RIB entry for VRF Univ prefix ----------------------------
-------------------------------------------- SDA-Border1#show ip bgp vpnv4 vrf Univ Network
Next Hop Metric LocPrf Weight Path Route Distinguisher: 1:4100 (default for vrf Univ) *>
10.10.10.8/30 10.50.50.22 65535 65004 i <<< Prefix leaked from Global Routing Table on Fusion *>
172.16.10.0/24 10.50.50.22 65535 65004 65005 i <<< Prefix originated in VRF Campus, leaked on
Fusion to VRF Univ *> 172.16.20.0/24 0.0.0.0 32768 i <<< VRF Univ originated prefix SDA-
Border1#show ip route vrf Univ bgp Routing Table: Univ B 10.10.10.8/30 [20/0] via 10.50.50.22,
20:31:06 <<< RIB entry for DHCP Server pool prefix B 172.16.10.0/24 [20/0] via 10.50.50.22,
20:33:21 <<< RIB entry for VRF Campus prefix B 172.16.20.0/24 [200/0], 20:33:21, Null0 <<< Null
entry created by "aggregate-address" BGP configuration
```

SDA-Borda-2

```
SDA-Border2#show ip bgp vpnv4 vrf Campus

     Network          Next Hop          Metric LocPrf Weight Path
Route Distinguisher: 1:4099 (default for vrf Campus)
 *>   10.10.10.8/30    10.50.50.2                        65535 65004 i        <<< Prefix
leaked from Global Routing Table on Fusion
 *>   172.16.10.0/24   0.0.0.0                           32768 i              <<< VRF Campus
originated prefix
 *>   172.16.20.0/24   10.50.50.2                        65535 65004 65005 i  <<< Prefix
originated in VRF Univ, leaked on Fusion to VRF Campus


SDA-Border2#show ip route vrf Campus bgp

B       10.10.10.8/30 [20/0] via 10.50.50.2, 01:02:19          <<< RIB entry for DHCP Server
pool prefix
B       172.16.10.0/24 [200/0], 1w6d, Null0                    <<< Null entry created by
"aggregate-address" BGP configuration
```

```
B       172.16.20.0/24 [20/0] via 10.50.50.2, 01:02:27          <<< RIB entry for VRF Univ
Prefix


---------------------------------------------------------------------

SDA-Border2#show ip bgp vpnv4 vrf Univ

     Network          Next Hop          Metric LocPrf Weight Path
Route Distinguisher: 1:4100 (default for vrf Univ)
 *>   10.10.10.8/30    10.50.50.10                      65535 65004 i       <<< Prefix
leaked from Global Routing Table on Fusion
 *>   172.16.10.0/24   10.50.50.10                      65535 65004 65005 i   <<< Prefix
originated in VRF Campus, leaked on Fusion to VRF Univ
 *>   172.16.20.0/24   0.0.0.0                          32768 i              <<< VRF Univ
originated prefix



SDA-Border2#show ip route vrf Univ bgp

B       10.10.10.8/30 [20/0] via 10.50.50.10, 01:02:29       <<< RIB entry for DHCP Server
pool prefix
B       172.16.10.0/24 [20/0] via 10.50.50.10, 01:02:34       <<< RIB entry for VRF Campus
prefix
B       172.16.20.0/24 [200/0], 1w6d, Null0                    <<< Null entry created by
"aggregate-address" BGP configuration
```

SDA-Fusion-1

```
SDA-Fusion1#show ip bgp

     Network          Next Hop          Metric LocPrf Weight Path
 *>   10.10.10.8/30    0.0.0.0               0          32768 i          <<< Locally
originated Global prefix
 * i 172.16.10.0/24   10.50.50.1            0    100      0 65005 i      <<< Prefix imported
from VRF Campus
 *>                   10.50.50.25           0            0 65005 i
 * i 172.16.20.0/24   10.50.50.9            0    100      0 65005 i      <<< Prefix imported
from VRF Univ
 *>                   10.50.50.21           0            0 65005 i


SDA-Fusion1#show ip route

C       10.10.10.8/30 is directly connected, GigabitEthernet2/35         <<< Prefix for DHCP
Server
B       172.16.10.0 [20/0] via 10.50.50.25 (Campus), 20:50:21         <<< Prefix imported
from VRF Campus
B       172.16.20.0 [20/0] via 10.50.50.21 (Univ), 20:50:21         <<< Prefix imported from
VRF Univ


---------------------------------------------------------------------------


SDA-Fusion1#show ip bgp vpnv4 vrf Campus

     Network          Next Hop          Metric LocPrf Weight Path
Route Distinguisher: 1:4099 (default for vrf Campus)
Import Map: Global_Map, Address-Family: IPv4 Unicast, Pfx Count/Limit: 1/1000
Export Map: Campus_Map, Address-Family: IPv4 Unicast, Pfx Count/Limit: 1/1000
 *>   10.10.10.8/30    0.0.0.0               0          32768 i          <<< Prefix imported
```

```
from Global Routing
 *>  172.16.10.0/24   10.50.50.25              0            0 65005 i <<< Prefix learnt from
Border1 in VRF Campus
 *>  172.16.20.0/24   10.50.50.21              0            0 65005 i <<< Prefix imported fron
VRF Univ


SDA-Fusion1#show ip bgp vpnv4 vrf Campus 172.16.20.0/24
BGP routing table entry for 1:4099:172.16.20.0/24, version 27
Paths: (1 available, best #1, table Campus)
Advertised to update-groups:
5
Refresh Epoch 1
65005, (aggregated by 65005 192.168.10.1), imported path from 1:4100:172.16.20.0/24 (Univ)
10.50.50.21 (via vrf Univ) (via Univ) from 10.50.50.21 (192.168.10.1)
Origin IGP, metric 0, localpref 100, valid, external, atomic-aggregate, best
Extended Community: RT:1:4100
rx pathid: 0, tx pathid: 0x0


SDA-Fusion1#show ip route vrf Campus bgp B 10.10.10.8/30 is directly connected, 20:46:51,
GigabitEthernet2/35 B 172.16.10.0 [20/0] via 10.50.50.25, 20:50:07 B 172.16.20.0 [20/0] via
10.50.50.21 (Univ), 20:50:07 ----------------------------------------------------------------
--------- SDA-Fusion1#show ip bgp vpnv4 vrf Univ Network Next Hop Metric LocPrf Weight Path
Route Distinguisher: 1:4100 (default for vrf Univ) Import Map: Global_Map, Address-Family: IPv4
Unicast, Pfx Count/Limit: 1/1000 Export Map: Univ_Map, Address-Family: IPv4 Unicast, Pfx
Count/Limit: 1/1000 *> 10.10.10.8/30 0.0.0.0 0 32768 i <<< Prefix imported from Global Routing
*> 172.16.10.0/24 10.50.50.25 0 0 65005 i <<< Prefix imported fron VRF Campus *> 172.16.20.0/24
10.50.50.21 0 0 65005 i <<< Prefix learnt from Border1 in VRF Univ

SDA-Fusion1#show ip bgp vpnv4 vrf Univ 172.16.10.0/24
BGP routing table entry for 1:4100:172.16.10.0/24, version 25
Paths: (1 available, best #1, table Univ)
Advertised to update-groups:
4
Refresh Epoch 1
65005, (aggregated by 65005 192.168.10.1), imported path from 1:4099:172.16.10.0/24 (Campus)
10.50.50.25 (via vrf Campus) (via Campus) from 10.50.50.25 (192.168.10.1)
Origin IGP, metric 0, localpref 100, valid, external, atomic-aggregate, best
Extended Community: RT:1:4099
rx pathid: 0, tx pathid: 0x0


SDA-Fusion1#show ip route vrf Univ bgp B 10.10.10.8/30 is directly connected, 20:47:01,
GigabitEthernet2/35 B 172.16.10.0 [20/0] via 10.50.50.25 (Campus), 20:50:17 B 172.16.20.0 [20/0]
via 10.50.50.21, 20:50:17
```

SDA-Fusion-2

```
SDA-Fusion2#show ip bgp

     Network          Next Hop         Metric LocPrf Weight Path
 *>i 10.10.10.8/30    10.90.90.1            0    100      0 i
 *>  172.16.10.0/24   10.50.50.1            0             0 65005 i
 * i                  10.50.50.25          0    100      0 65005 i
 *>  172.16.20.0/24   10.50.50.9           0             0 65005 i
 * i                  10.50.50.21          0    100      0 65005 i


SDA-Fusion2#show ip route

B        10.10.10.8/30 [200/0] via 10.90.90.1, 01:25:56
B        172.16.10.0 [20/0] via 10.50.50.1 (Campus), 01:25:56
```

```
B          172.16.20.0 [20/0] via 10.50.50.9 (Univ), 01:25:56


-------------------------------------------------------------------------

SDA-Fusion2#show ip bgp vpnv4 vrf Campus

       Network          Next Hop          Metric LocPrf Weight Path
Route Distinguisher: 1:4099 (default for vrf Campus)
Import Map: Global_Map, Address-Family: IPv4 Unicast, Pfx Count/Limit: 1/1000
Export Map: Campus_Map, Address-Family: IPv4 Unicast, Pfx Count/Limit: 1/1000
 *>i 10.10.10.8/30    10.90.90.1                0    100      0 i
 *>  172.16.10.0/24   10.50.50.1                0             0 65005 i
 *>  172.16.20.0/24   10.50.50.9                0             0 65005 i


SDA-Fusion2#show ip route vrf Campus bgp


B          10.10.10.8/30 [200/0] via 10.90.90.1, 01:26:09
B          172.16.10.0 [20/0] via 10.50.50.1, 01:26:13
B          172.16.20.0 [20/0] via 10.50.50.9 (Univ), 01:26:13


--------------------------------------------------------------------------

SDA-Fusion2#show ip bgp vpnv4 vrf Univ

       Network          Next Hop          Metric LocPrf Weight Path
Route Distinguisher: 1:4100 (default for vrf Univ)
Import Map: Global_Map, Address-Family: IPv4 Unicast, Pfx Count/Limit: 1/1000
Export Map: Univ_Map, Address-Family: IPv4 Unicast, Pfx Count/Limit: 1/1000
 *>i 10.10.10.8/30    10.90.90.1                0    100      0 i
 *>  172.16.10.0/24   10.50.50.1                0             0 65005 i
 *>  172.16.20.0/24   10.50.50.9                0             0 65005 i


SDA-Fusion2#show ip route vrf Univ bgp


B          10.10.10.8/30 [200/0] via 10.90.90.1, 01:26:19
B          172.16.10.0 [20/0] via 10.50.50.1 (Campus), 01:26:23
B          172.16.20.0 [20/0] via 10.50.50.9, 01:26:23
```

Configuração Manual para Redundância de Borda

Para redundância entre os PETRs quando um link externo de borda falha, para fronteiras externas e externas+internas, você precisa criar manualmente sessões de iBGP entre as duas Bordas para cada um dos VNs. Além disso, no caso da fronteira externa+interna onde o BGP é importado para o LISP e o LISP é redistribuído de volta para o BGP, as tags são necessárias para evitar as importações de rotas do iBGP para o LISP e, portanto, evitar loops potenciais.

SDA-Borda-1

```
interface Vlan31
 description vrf interface to SDA-Border-2
 vrf forwarding Campus
 ip address 10.31.1.1 255.255.255.252
!
interface Vlan33
```

```
 description vrf interface to SDA-Border-2
 vrf forwarding Univ
 ip address 10.33.1.1 255.255.255.252
!


router bgp 65005
!
address-family ipv4 vrf Campus
redistribute lisp metric 10 <<< open redistribution pushed by DNAC
neighbor 10.31.1.2 remote-as 65005      <<< iBGP peering with SDA-Border-2
neighbor 10.31.1.2 activate
neighbor 10.31.1.2 send-community     <<< we need to send community/tag to the neighbor
neighbor 10.31.1.2 route-map tag_local_eids out    <<< route-map used to tag prefixes sent out
!
address-family ipv4 vrf Univ
redistribute lisp metric 10
 neighbor 10.33.1.2 remote-as 65005
neighbor 10.33.1.2 activate
neighbor 10.33.1.2 send-community
neighbor 10.33.1.2 route-map tag_local_eids out
!


router lisp
!
instance-id 4099
service ipv4
eid-table vrf Campus
 route-import database bgp 65005 route-map DENY-Campus locator-set rloc_a0602921-91eb-4e27-a294-
f88949a1ca37 <<< pushed by DNAC if Border is (also) Internal
!
 instance-id 4103
 service ipv4
 eid-table vrf Univ
 route-import database bgp 65005 route-map DENY-Univ locator-set rloc_a0602921-91eb-4e27-a294-
f88949a1ca37
!


ip community-list 1 permit 655370 <<< community-list matching tag 655370 - pushed by DNAC
!


route-map DENY-Campus deny 5 <<< route-map pushed by DNAC and used in route-import
match ip address prefix-list Campus
!
route-map DENY-Campus deny 10
match ip address prefix-list l3handoff-prefixes
!
route-map DENY-Campus deny 15
match community 1 <<< match on community-list 1 to deny iBGP prefixes to be imported into LISP
!
route-map DENY-Campus deny 25
match ip address prefix-list deny_0.0.0.0
!
route-map DENY-Campus permit 30
!


route-map DENY-Univ deny 5 <<< similar route-map is pushed for Univ VN
match ip address prefix-list Univ
!
route-map DENY-Univ deny 10
match ip address prefix-list l3handoff-prefixes
!
route-map DENY-Univ deny 15
match community 1
!
```

```
route-map DENY-Univ deny 25
match ip address prefix-list deny_0.0.0.0
!
route-map DENY-Univ permit 30
!

route-map tag_local_eids permit 5 <<< route-map we need to create in order to tag the routes
advertised to the iBGP peer
set community 655370 <<< setting community/tag to 655370
!
```

SDA-Borda-2

```
interface Vlan31
 description vrf interface to SDA-Border-1
 vrf forwarding Campus
 ip address 10.31.1.2 255.255.255.252
!
interface Vlan33
 description vrf interface to SDA-Border-1
 vrf forwarding Univ
 ip address 10.33.1.2 255.255.255.252
!

router bgp 65005
!
address-family ipv4 vrf Campus
 neighbor 10.31.1.1 remote-as 65005
 neighbor 10.31.1.1 activate
 neighbor 10.31.1.1 send-community
 neighbor 10.31.1.1 route-map tag_local_eids out
!
address-family ipv4 vrf Univ
 neighbor 10.33.1.1 remote-as 65005
 neighbor 10.33.1.1 activate
 neighbor 10.33.1.1 send-community
 neighbor 10.33.1.1 route-map tag_local_eids out
!

router lisp
!
 instance-id 4099
 service ipv4
  eid-table vrf Campus
route-import database bgp 65005 route-map DENY-Campus locator-set rloc_677c0a8a-0802-49f9-99cc-
f9c6ebda80f3      <<< pushed by DNAC
!

 instance-id 4103
  service ipv4
   eid-table vrf Univ
route-import database bgp 65005 route-map DENY-Univ locator-set rloc_677c0a8a-0802-49f9-99cc-
f9c6ebda80f3
!

ip community-list 1 permit 655370
!

route-map DENY-Campus deny 5
match ip address prefix-list Campus
!
route-map DENY-Campus deny 10
match ip address prefix-list l3handoff-prefixes
```

```
!
route-map DENY-Campus deny 15
match community 1
!
route-map DENY-Campus deny 25
match ip address prefix-list deny_0.0.0.0
!
route-map DENY-Campus permit 30
!

route-map DENY-Univ deny 5
match ip address prefix-list Univ
!
route-map DENY-Univ deny 10
match ip address prefix-list l3handoff-prefixes
!
route-map DENY-Univ deny 15
match community 1
!
route-map DENY-Univ deny 25
match ip address prefix-list deny_0.0.0.0
!
route-map DENY-Univ permit 30
!

route-map tag_local_eids permit 5
set community 655370
!
```

Simplifique a configuração do Fusion com o uso de modelos

Esta seção contém exemplos de configuração do Fusion Template de exemplo para ajudar a simplificar a configuração.

A seguir estão as Variáveis que devem ser definidas com base no seu projeto de implantação. Neste exemplo, as configurações e as VPNs são baseadas na topologia anterior que tem duas VLANs, Campus e Univ.

Definição de Variável

```
interface_Fusion1: GigabitEthernet2/8
interface_Fusion2: GigabitEthernet0/0/0

Global_prefixes = 10.10.10.8/30

FUSION_BGP_AS = 65004
BORDER_BGP_AS = 65005
```
    Para VN1:

```
VN1 = Campus
Fusion1_VN1_VLAN = 3007
Fusion2_VN1_VLAN = 3001
VN1_prefixes = 172.16.10.0/24

Fusion1_VN1_IP = 10.50.50.26

Fusion1_VN1_MASK = 255.255.255.252
```

```
Fusion2_VN1_IP = 10.50.50.2

Fusion2_VN1_MASK = 255.255.255.252
VN1_RD = 4099
VN1_ border1_neighbor_IP = 10.50.50.25
VN1_border2_neighbor_IP = 10.50.50.1
```
Para VN2:

```
VN2 = Univ
Fusion1_VN2_VLAN = 3006
Fusion2_VN2_VLAN = 3003
VN2_prefixes = 172.16.20.0/24

Fusion1_VN2_IP = 10.50.50.22

Fusion1_VN2_MASK = 255.255.255.252
Fusino2_VN2_IP2 = 10.50.50.10

Fusion2_VN2_MASK = 255.255.255.252
VN2_RD = 4100
VN2_border1_neighbor_IP = 10.50.50.21
VN2_border2_neighbor_IP = 10.50.50.9
```

Exemplo de modelo

Fusão 1

```
interface $interface_Fusion1
switchport
switchport mode trunk
switchport trunk allowed vlan add $Fusion1_VN1_VLAN, $Fusion1_VN2_VLAN
!
vlan $Fusion1_VN1_VLAN
no shut
!
vlan $Fusion1_VN2_VLAN
no shut
!
vrf definition $VN1
rd 1:$VN1_RD
!
address-family ipv4
route-target export 1:$VN1_RD
route-target import 1:$VN1_RD
route-target import 1:$VN2_RD
exit-address-family
!
vrf definition $VN2
rd 1:$VN2_RD
!
address-family ipv4
route-target export 1:$VN2_RD
route-target import 1:$VN2_RD
route-target import 1:$VN1_RD
exit-address-family
!
interface Vlan $Fusion1_VN1_VLAN
vrf forwarding $VN1
ip address $Fusion1_VN1_IP $Fusion1_VN1_MASK
!
```

```
interface Vlan $Fusion1_VN2_VLAN
vrf forwarding $VN2
ip address $Fusion1_VN2_IP $Fusion1_VN2_MASK
!
router bgp $FUSION_BGP_AS
bgp log-neighbor-changes
!
address-family ipv4
exit-address-family
!
address-family ipv4 vrf $VN1
neighbor $VN1_border1_neighbor_IP remote-as $BORDER_BGP_AS
neighbor $VN1_border1_neighbor_IP update-source Vlan $Fusion1_VN1_VLAN
neighbor $VN1_border1_neighbor_IP activate
exit-address-family
!
address-family ipv4 vrf $VN2
neighbor $VN2_border1_neighbor_IP remote-as $BORDER_BGP_AS
neighbor $VN2_border1_neighbor_IP update-source $Fusion1_VN2_VLAN
neighbor $VN2_border1_neighbor_IP activate
exit-address-family

ip prefix-list ${VN1}_Prefix seq 5 permit $VN1_prefixes
ip prefix-list Global_Prefix seq 5 permit $Global_prefixes
ip prefix-list ${VN2}_Prefix seq 5 permit $VN2_prefixes

route-map ${VN2}_Map permit 10
match ip address prefix-list ${VN2}_Prefix
route-map Global_Map permit 10
match ip address prefix-list Global_Prefix
route-map ${VN1}_Map permit 10
match ip address prefix-list ${VN1}_Prefix

vrf definition $VN1
!
address-family ipv4
import ipv4 unicast map Global_Map
export ipv4 unicast map ${VN1}_Map
exit-address-family
!
vrf definition $VN2
!
address-family ipv4
import ipv4 unicast map Global_Map
export ipv4 unicast map ${VN2}_Map
exit-address-family
!
```

Fusão 2

```
interface $interface_Fusion2.$Fusion2_VN1_VLAN
encapsulation dot1Q $Fusion2_VN1_VLAN
vrf forwarding $VN1
ip address $Fusion2_VN1_IP2 $Fusion2_VN1_MASK
!
interface $interface_Fusion2.$Fusion2_VN2_VLAN
encapsulation dot1Q $Fusion2_VN2_VLAN
vrf forwarding $VN2
ip address $Fusion2_VN2_IP2 $Fusion2_VN2_MASK
!
vlan $Fusion2_VN1_VLAN
no shut
```

```
!
vlan $Fusion2_VN2_VLAN
no shut
!
vrf definition $VN1
rd 1:$VN1_RD
!
address-family ipv4
route-target export 1:$VN1_RD
route-target import 1:$VN1_RD
route-target import 1:$VN2_RD
exit-address-family
!
vrf definition $VN2
rd 1:$VN2_RD
!
address-family ipv4
route-target export 1:$VN2_RD
route-target import 1:$VN2_RD
route-target import 1:$VN1_RD
exit-address-family
!
router bgp $FUSION_BGP_AS
bgp log-neighbor-changes
!
address-family ipv4
exit-address-family
!
address-family ipv4 vrf $VN1
neighbor $VN1_border2_neighbor_IP remote-as $BORDER_BGP_AS
neighbor $VN1_border2_neighbor_IP update-source $interface_Fusion2.$Fusion2_VN1_VLAN
neighbor $VN1_bordre2_neighbor_IP activate
exit-address-family
!
address-family ipv4 vrf $VN2
neighbor $VN2_border2_neighbor_IP remote-as $BORDER_BGP_AS
neighbor $VN2_border2_neighbor_IP update-source $interface_Fusion2.$Fusion2_VN2_VLAN
neighbor $VN2_border2_neighbor_IP activate
exit-address-family

ip prefix-list ${VN1}_Prefix seq 5 permit $VN1_prefixes
ip prefix-list Global_Prefix seq 5 permit $Global_prefixes
ip prefix-list ${VN2}_Prefix seq 5 permit $VN2_prefixes

route-map ${VN2}_Map permit 10
match ip address prefix-list ${VN2}_Prefix
route-map Global_Map permit 10
match ip address prefix-list Global_Prefix
route-map ${VN}_Map permit 10
match ip address prefix-list ${VN1}_Prefix

vrf definition $VN1
!
address-family ipv4
import ipv4 unicast map Global_Map
export ipv4 unicast map ${VN1}_Map
exit-address-family
!
vrf definition $VN2
!
address-family ipv4
import ipv4 unicast map Global_Map
export ipv4 unicast map ${VN2}_Map
exit-address-family
```

!
End