# Configurer la redirection du trafic vers SIG avec la politique de données : Fallback to Routing

## Table des matières



## Introduction

Ce document décrit comment configurer une politique de données pour permettre au trafic de revenir au routage lorsque les tunnels SIG échouent.

## Conditions préalables

### Exigences

Cisco vous recommande de connaître la solution Cisco SDWAN (Software Defined Wide Area Network).

Avant d'appliquer une politique de données pour la redirection du trafic d'application vers un SIG, vous devez configurer des tunnels SIG.

### Composants utilisés

La stratégie de cet article a été testée sur la version logicielle 20.9.1 et Cisco IOS-XE 17.9.1.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

# Fond

Grâce à cette fonctionnalité, vous pouvez configurer le trafic Internet pour qu'il soit routé via la superposition SD-WAN de Cisco, comme mécanisme de secours, lorsque tous les tunnels SIG sont hors service.

Cette fonctionnalité est introduite dans Cisco IOS XE version 17.8.1a et Cisco vManage version 20.8.1

# Définition du problème

Avant la version 20.8, l'action SIG dans la politique de données est stricte par défaut.  Si les tunnels SIG sont désactivés, le trafic est abandonné.

# Architecture logicielle

Vous pouvez avoir une option supplémentaire pour choisir de ne pas être strict et de revenir au routage pour envoyer le trafic sur la superposition.

Le routage peut conduire à la superposition ou à d'autres chemins de transfert comme NAT-DIA.

En résumé, le comportement attendu est le suivant :

- Vous avez la possibilité de choisir l'action SIG comme étant stricte par défaut ou **de revenir au routage**.
- Le comportement par défaut est **strict**. Si les tunnels SIG sont désactivés, le trafic est abandonné.
- Si le **routage de secours** est activé,  Si les tunnels SIG sont UP, le trafic est envoyé via SIG.Si les tunnels SIG sont INACTIFS, le trafic n'est PAS abandonné. Le trafic subit un routage normal. **Remarque** : le routage peut également être via NAT DIA, si l'utilisateur a à la fois une route SIG (via une configuration ou une action de stratégie) et NAT DIA configurée (ip nat route vrf 1 0.0.0.0 0.0.0.0 global) et si le tunnel tombe en panne, le routage pointe vers NAT DIA. Si vous êtes concerné par la sécurité (c'est-à-dire que tout le trafic peut passer par superposition ou par SIG mais pas par DIA), alors NAT DIA NE DOIT pas être configuré.Si le tunnel SIG devient UP, seuls les nouveaux flux sont envoyés sur SIG. Les flux actuels ne seraient pas soumis à l'action SIG.Si le tunnel SIG devient DOWN, tout le trafic passe par le routage, les flux actuels et les nouveaux flux. **Remarque** : les flux actuels passent par le tunnel SIG avant et le passage au routage peut interrompre la session de bout en bout. Les nouveaux flux subissent un routage

# Configuration

## Politique vSmart

## Politique de données

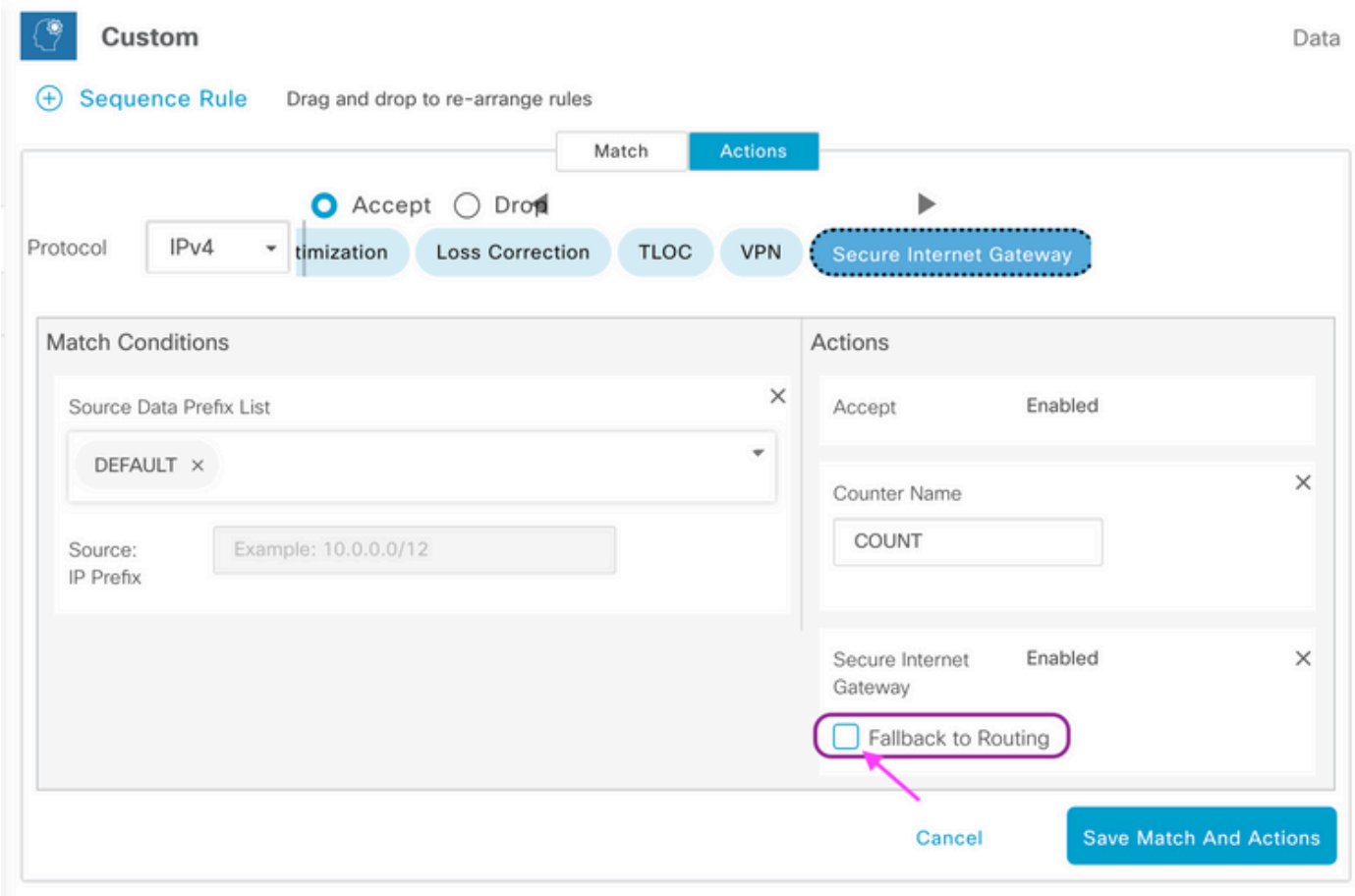
```
vSmart-1# show running-config policy
policy
 data-policy _VPN10_sig-default-fallback-to-routing
  vpn-list VPN10
   sequence 1
    match
     source-data-prefix-list Default
    !
    action accept
     count Count_26488854
     sig
```

sig-action fallback-to-routing! ! default-action drop ! ! lists vpn-list VPN10 vpn 10 ! data-prefix-list Default ip-prefix 0.0.0.0/0 ! site-list Site300 site-id 300 ! ! !

## Appliquer la stratégie

```
vSmart-1# show running-config apply-policy
apply-policy
 site-list Site300
  data-policy _VPN10_sig-default-fallback-to-routing all
 !
!
```

Lorsque le générateur de politiques pour la politique vSmart est utilisé, cochez la case **Fallback to Routing** pour acheminer le trafic Internet via la superposition Cisco SD-WAN lorsque tous les tunnels SIG sont désactivés.




Lorsque l'action **Fallback to Routing** est sélectionnée sur l'interface utilisateur, **fallback-to-routing**

et **sig-action** sont ajoutés à la configuration sous *action accept.*

# Vérification sur cEdge

## Policy (politique)

```
Site300-cE1#show sdwan policy from-vsmart
from-vsmart data-policy _VPN10_sig-default-fallback-to-routing
direction all vpn-list VPN10 sequence 1 match source-data-prefix-list Default action accept
count Count_26488854 sig sig-action fallback-to-routing default-action drop from-vsmart lists vpn-list
VPN10 vpn 10
from-vsmart lists data-prefix-list Default
ip-prefix 0.0.0.0/0
```

## Confirmer

Vérifiez que le trafic est acheminé à l'aide de la commande **ping**.

```
Site300-cE1# ping vrf 10 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/6/9 ms
Site300-cE1#
```

Vous pouvez vérifier le chemin que le trafic est censé prendre avec la commande **show sdwan policy service-path**.

```
Site300-cE1# show sdwan policy service-path vpn 10 interface GigabitEthernet 3 source-ip
10.30.1.1 dest-ip 8.8.8.8 protocol  6 all
Number of possible next hops: 1
Next Hop: Remote
  Remote IP: 0.0.0.0, Interface  Index: 29

Site300-cE1# show sdwan policy service-path vpn 10 interface GigabitEthernet 3 source-ip
10.30.1.1 dest-ip 8.8.8.8 protocol  17  all
Number of possible next hops: 1
Next Hop: Remote
  Remote IP: 0.0.0.0, Interface  Index: 29
```

## Vérifier les compteurs de politique de données

Tout d'abord, effacez les compteurs avec la commande **clear sdwan policy data-policy** pour commencer à 0.  Vous pouvez vérifier que le compteur a été détecté à l'aide de la commande **show sdwan policy data-policy-filter** .

```
Site300-cE1#clear sdwan policy data-policy

Site300-cE1#show sdwan policy data-policy-filter _VPN10_sig-default-fallback-to-routing
data-policy-filter _VPN10_sig-default-fallback-to-routing
data-policy-vpnlist VPN10
  data-policy-counter Count_26488854
   packets 0
   bytes   0
  data-policy-counter default_action_count
```

```
   packets 0
   bytes   0
```

Utilisez la commande **ping** pour envoyer quelques paquets que vous prévoyez d'acheminer via le tunnel SIG.

```
Site300-cE1# ping vrf 10 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/7/11 ms
Site300-cE1#
```

Vérifiez que les paquets ICMP atteignent votre séquence de stratégie de données avec la commande **show sdwan policy data-policy-filter**.

```
Site300-cE1#show sdwan policy data-policy-filter _VPN10_sig-default-fallback-to-routing
data-policy-filter _VPN10_sig-default-fallback-to-routing
data-policy-vpnlist VPN10
  data-policy-counter Count_26488854
   packets 5
   bytes   500
  data-policy-counter default_action_count
   packets 0
   bytes   0
```

## Packet Trace

Configurez un suivi de paquet pour comprendre ce qui arrive aux paquets avec le routeur.

```
Site300-cE1#show platform packet-trace summary
Pkt   Input                   Output                  State  Reason
12    INJ.2                   Gi1                     FWD
13    Tu100001                internal0/0/rp:0        PUNT   11  (For-us data)
14    INJ.2                   Gi1                     FWD
15    Tu100001                internal0/0/rp:0        PUNT   11  (For-us data)
16    INJ.2                   Gi1                     FWD
17    Tu100001                internal0/0/rp:0        PUNT   11  (For-us data)
18    INJ.2                   Gi1                     FWD
19    Tu100001                internal0/0/rp:0        PUNT   11  (For-us data)
20    INJ.2                   Gi1                     FWD
21    Tu100001                internal0/0/rp:0        PUNT   11  (For-us data)
```

### Paquet 12

Un extrait du paquet 12 montre la séquence d'accès au trafic 1 dans la politique de données et est redirigé vers SIG.

```
Feature: SDWAN Data Policy IN
    VPN ID       : 10
    VRF          : 1
    Policy Name  : sig-default-fallback-VPN10 (CG:1)
    Seq          : 1
    DNS Flags    : (0x0) NONE
    Policy Flags : 0x10110000
    Nat Map ID   : 0
    SNG ID       : 0
    Action       : REDIRECT_SIG Success 0x3
```

```
  Action       : SECONDARY_LOOKUP Success
```

La recherche Input pour l'interface de sortie affiche l'interface de tunnel (logique).

```
Feature: IPV4_INPUT_LOOKUP_PROCESS_EXT
  Entry       : Input - 0x81418130
  Input       : internal0/0/rp:0
  Output      : Tunnel100001
  Lapsed time : 446 ns
```

Après le cryptage IPSec, l'interface d'entrée est remplie.

```
Feature: IPSec
  Result    : IPSEC_RESULT_SA
  Action    : ENCRYPT
  SA Handle : 42
  Peer Addr : 8.8.8.8
  Local Addr: 10.30.1.1

Feature: IPV4_OUTPUT_IPSEC_CLASSIFY
  Entry       : Output - 0x81417b48
  Input       : GigabitEthernet1
  Output      : Tunnel100001
  Lapsed time : 4419 ns
```

Le routeur effectue plusieurs autres actions, puis transmet le paquet sur l'interface GigabitEthernet1.

```
Feature: MARMOT_SPA_D_TRANSMIT_PKT
  Entry       : Output - 0x8142f02c
  Input       : GigabitEthernet1
  Output      : GigabitEthernet1
  Lapsed time : 2223 ns
```

## Paquet 13

Le routeur reçoit la réponse de l'adresse IP distante (8.8.8.8), mais ne sait pas qui l'enverra, comme indiqué par **Output: <unknown>** dans le résultat.

```
Feature: IPV4(Input)
  Input       : Tunnel100001
  Output      : <unknown>
  Source      : 8.8.8.8
  Destination : 10.30.1.1
  Protocol    : 1 (ICMP)
Feature: DEBUG_COND_INPUT_PKT
  Entry       : Input - 0x813eb360
  Input       : Tunnel100001
  Output      : <unknown>
  Lapsed time : 109 ns
```

Comme le paquet est généré en interne, il est consommé par le routeur et la sortie est affichée sous la forme **<internal0/0/rp:0>**.

```
Feature: INTERNAL_TRANSMIT_PKT_EXT
  Entry       : Output - 0x813ebe6c
  Input       : Tunnel100001
  Output      : internal0/0/rp:0
```

```
    Lapsed time : 5785 ns
```

Ensuite, le paquet est envoyé au processus Cisco IOSd, qui enregistre les actions entreprises sur le paquet. L'adresse IP de l'interface locale dans VRF 10 est 10.30.1.1.

```
IOSd Path Flow: Packet: 13    CBUG ID: 79
  Feature: INFRA
  Pkt Direction: IN
    Packet Rcvd From DATAPLANE

  Feature: IP
  Pkt Direction: IN
    Packet Enqueued in IP layer
    Source      : 8.8.8.8
    Destination : 10.30.1.1
    Interface   : Tunnel100001

  Feature: IP
  Pkt Direction: IN
  FORWARDED To transport layer
    Source        : 8.8.8.8
    Destination   : 10.30.1.1
    Interface     : Tunnel100001

  Feature: IP
  Pkt Direction: IN
  CONSUMED Echo reply
    Source        : 8.8.8.8
    Destination   : 10.30.1.1
    Interface     : Tunnel100001
```

## Vérification du routage de secours

Vous pouvez simuler le basculement avec un arrêt administratif sur l'interface de transport (TLOC) (GigabitEthernet1), qui est Biz-Internet.  Il dispose d'une connexion Internet.

GigabitEthernet2 : le TLOC MPLS est UP/UP, mais n'a pas de connexion Internet.  L'état du contrôle peut être vu dans la sortie **show sdwan control local-properties wan-interface-list**.

```
Site300-cE1#show sdwancontrollocal-properties wan-interface-list

                        PUBLIC          PUBLIC PRIVATE         PRIVATE
        PRIVATE                              MAX   RESTRICT/           LAST         SPI TIME
NAT  VM
INTERFACE               IPv4            PORT   IPv4            IPv6
        PORT    VS/VM COLOR            STATE CNTRL CONTROL/     LR/LB  CONNECTION   REMAINING
TYPE CON REG

                                                 STUN
    PRF ID
-----------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------
-------------
GigabitEthernet1             10.2.6.2        12346  10.2.6.2        ::
            12346    0/0  biz-internet     down   2     yes/yes/no   No/No  0:19:51:05
0:10:31:41  N    5  Default
GigabitEthernet2             10.1.6.2        12346  10.1.6.2        ::
            12346    2/1  mpls             up     2     yes/yes/no   No/No  0:23:41:33
0:06:04:21  E    5  Default
```

Dans le résultat de la commande **show ip interface brief**, l'interface GigabitEthernet1 affiche

administratively down.

```
Site300-cE1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       10.2.6.2        YES other  administratively down down
GigabitEthernet2       10.1.6.2        YES other  up                    up
```

Le tunnel 100001 est dans un état **UP/DOWN**.

Tunnel100001 10.2.6.2 YES TFTP **up** **down**

Il n'y a pas de connexion Internet maintenant, donc l'accessibilité à 8.8.8.8 échoue à partir du VRF 10.

Site300-cE1# ping vrf 10 8.8.8.8 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds: U.U.U Success rate is 0 percent (0/5)

La commande **show sdwan policy service-path** montre que la route par défaut OMP (fallback-to-routing) pour aller au data center (data center) est attendue.

L'adresse IP TLOC MPLS du routeur local est 10.1.6.2.

```
Site300-cE1#show sdwan policy service-path vpn 10 interface GigabitEthernet 3 source-ip
10.30.1.1 dest-ip 8.8.8.8 protocol  6 all
Number of possible next hops: 1
Next Hop: IPsec
  Source: 10.1.6.2 12346 Destination: 10.1.2.2 12366 Local Color: mpls Remote Color: mpls Remote
System IP: 10.1.10.1

Site300-cE1#show sdwan policy service-path vpn 10 interface GigabitEthernet 3 source-ip
10.30.1.1 dest-ip 8.8.8.8 protocol  17 all
Number of possible next hops: 1
Next Hop: IPsec
  Source: 10.1.6.2 12346 Destination: 10.1.2.2 12366 Local Color: mpls Remote Color: mpls Remote
System IP: 10.1.10.1
```

# Sur le portail Umbrella


# Exemple de politique de données de production

Exemple type de politique de données de production.

data-policy _VPN10_SIG_Fall_Back vpn-list VPN10 sequence 1 match app-list Google_Apps source-ip 0.0.0.0/0 ! action accept sig sig-action fallback-to-routing ! ! default-action drop

Il correspond aux applications Google de n'importe quelle source et revient au routage, s'il y a un problème.

## Informations connexes

Documentation de la politique SDWAN Cisco IOS-XE

Documentation des fonctionnalités de suivi des paquets de données Cisco IOS-XE

Technical Support & Documentation - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.