# 使用数据策略配置到SIG的流量重定向：回退到路由

## 目录



## 简介

本文档介绍如何配置数据策略，以允许流量在SIG隧道失败时回退到路由。

## 先决条件

### 要求

思科建议您了解思科软件定义广域网(SDWAN)解决方案。

在应用数据策略将应用流量重定向到SIG之前，必须配置SIG隧道。

### 使用的组件

本文中的策略在软件版本20.9.1和Cisco IOS-XE 17.9.1上进行了测试。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

# 背景

通过此功能，您可以配置在所有SIG隧道关闭时通过思科SD-WAN重叠路由的互联网绑定流量，作为回退机制。

此功能在Cisco IOS XE 17.8.1a版和Cisco vManage 20.8.1版中引入

# 问题定义

在20.8版本之前，默认情况下，数据策略中的SIG操作是严格的。 如果SIG隧道关闭，流量将被丢弃。

# 软件架构

您还可以选择不严格并回退到路由以通过重叠发送流量。

路由可能导致重叠或其他转发路径（如NAT-DIA）。

总之，预期行为如下：

- 您可以选择将SIG操作设为默认严格或**回退到路由**。
- 默认行为是**strict**。 如果SIG隧道关闭，流量将被丢弃。
- 如果**回退到路由**已启用， 如果SIG隧道为UP状态，则通过SIG发送流量。如果SIG隧道关闭，流量不会丢弃。流量通过正常路由。 **注意**：如果用户同时配置了SIG路由（通过配置或通过策略操作）和NAT DIA(ip nat route vrf 1 0.0.0.0 0.0.0.0 global)，并且如果隧道关闭，则路由将指向NAT DIA，路由也可以通过NAT DIA。如果您关注安全性（即所有流量可以经过重叠或通过SIG，但不能通过DIA），则不得配置NAT DIA。如果SIG隧道变为UP，则仅通过SIG发送新流。任何当前流量都不会执行SIG操作。如果SIG隧道关闭，所有流量都会通过路由，包括任何当前流和新流。 **注意**：当前流量先于SIG隧道传输，然后切换到路由会中断端到端会话。新流经过路由

# 配置

## vSmart策略

### 数据策略

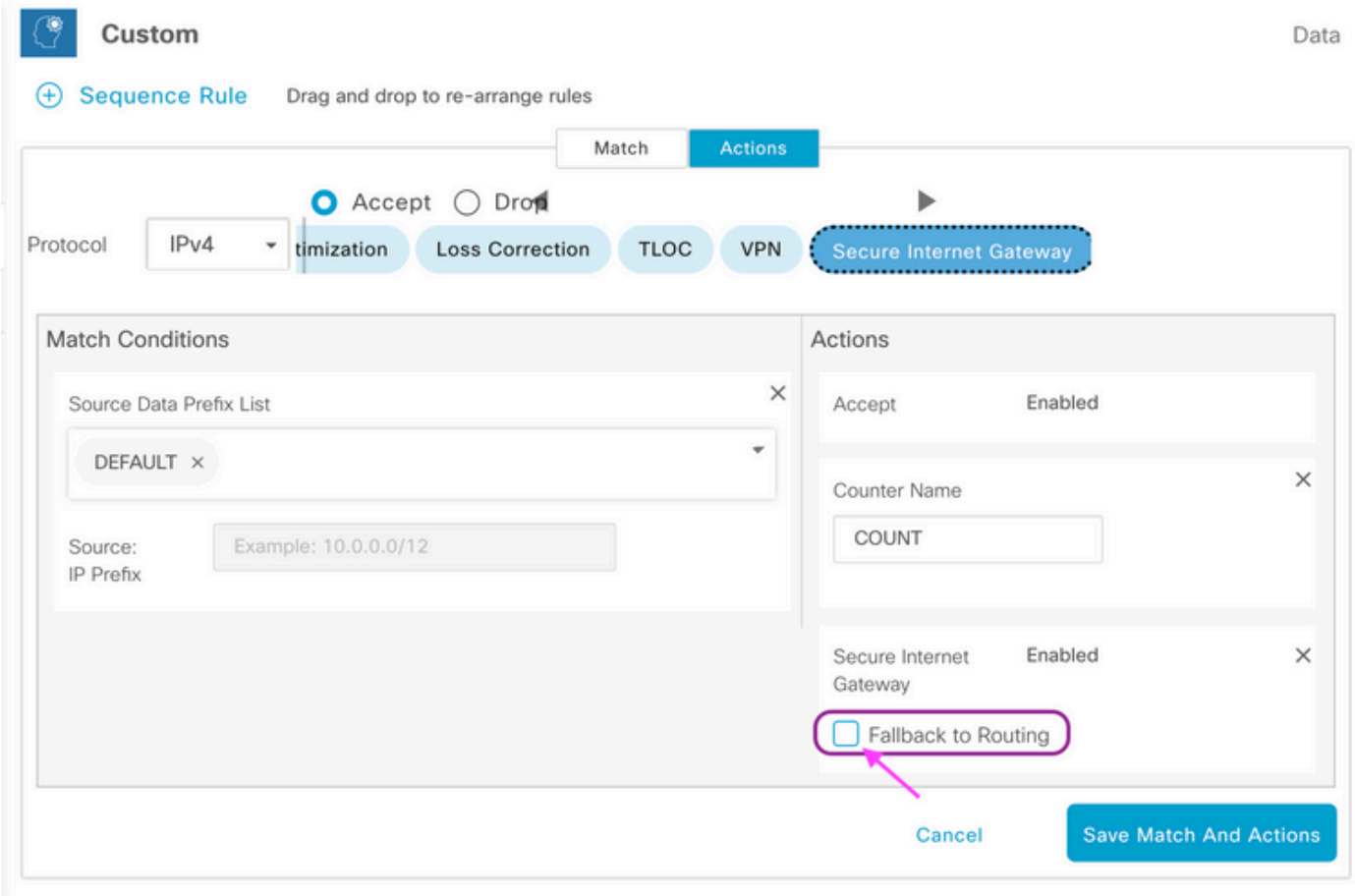
```
vSmart-1# show running-config policy
policy
 data-policy _VPN10_sig-default-fallback-to-routing
  vpn-list VPN10
   sequence 1
    match
     source-data-prefix-list Default
    !
    action accept
     count Count_26488854
     sig
```

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 ! ! !

### 应用策略

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

使用vSmart策略的策略生成器时，选中Fallback to Routing复选框，以便在所有SIG隧道关闭时通过思科SD-WAN重叠路由互联网绑定的流量。




在UI上选择**Fallback to Routing**操作时，**fallback-to-routing**和**sig-action**将添加到操作accept下的配置中。

# 在cEdge上验证

### 策略

```
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

## 确认

使用ping确认流量正在路由。

```
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#
```

您可以使用show sdwan policy service-path命令验证流量预期采用的路径。

```
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
```

## 检查数据策略计数器

首先，使用clear sdwan policy data-policy命令清除计数器，使其从0开始。 您可以使用show sdwan policy data-policy-filter命令验证计数器是否处于活动状态。

```
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
```

使用ping发送您期望通过SIG隧道路由的一些数据包。

```
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#
```

使用show sdwan policy data-policy-filter命令验证ICMP数据包是否到达您的数据策略序列。

```
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
```

## 数据包跟踪

设置数据包跟踪以了解路由器对数据包的响应。

```
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)
```

### 数据包12

来自数据包12的片段显示在数据策略中的流量命中序列1，并且被重定向到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
```

输出接口的Input lookup显示隧道接口（逻辑）。

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

在IPSec加密后，输入接口将被填充。

```
  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
```

路由器会执行其他几项操作，然后将数据包通过GigabitEthernet1接口传输出去。

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

**数据包13**

路由器收到来自远程IP(8.8.8.8)的响应，但不确定发送该响应的人员，如输出中的**Output: <unknown>**所示。

```
  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
```

由于数据包是在内部生成的，因此由路由器使用，输出显示为**<internal0/0/rp:0>**。

```
  Feature: INTERNAL_TRANSMIT_PKT_EXT
    Entry       : Output - 0x813ebe6c
    Input       : Tunnel100001
    Output      : internal0/0/rp:0
    Lapsed time : 5785 ns
```

之后，数据包被传送到Cisco IOSd进程，该进程记录对数据包执行的操作。VRF 10中的本地接口IP地址为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
```

## 检验回退到路由

您可以通过管理关闭传输接口(TLOC)(GigabitEthernet1)（即Biz-Internet）来模拟故障切换。 它有Internet连接。

GigabitEthernet2 - MPLS TLOC为UP/UP，但没有互联网连接。 可以在**show sdwan control local-properties wan-interface-list**输出中看到控制状态。

```
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
```

从**show ip interface brief**输出中，GigabitEthernet1接口显示为管理性关闭。

```
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
```

隧道100001口处于**UP/DOWN**状态。

```
Tunnel100001 10.2.6.2 YES TFTP up                    down
```

现在没有互联网连接，因此从VRF 10到8.8.8.8的连通性失败。

```
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)
```

**show sdwan policy service-path**命令显示，预期将采用要转到DC（数据中心）的OMP默认路由（回退到路由）。

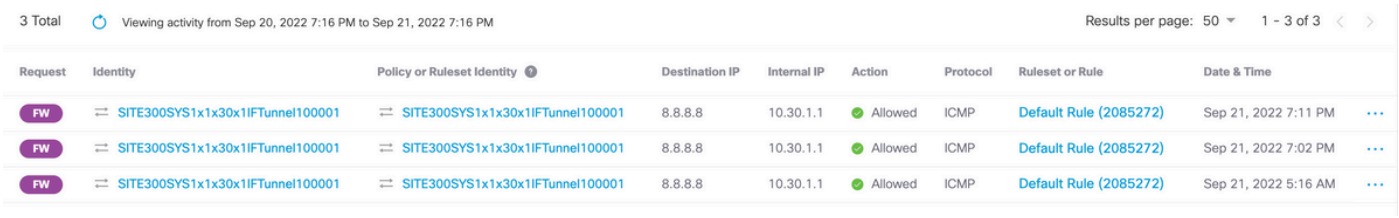
本地路由器MPLS TLOC IP地址为10.1.6.2。

```
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
```

# 在Umbrella门户上



3 Total  Viewing activity from Sep 20, 2022 7:16 PM to Sep 21, 2022 7:16 PM  Results per page: 50  1 - 3 of 3

| Request | Identity | Policy or Ruleset Identity | Destination IP | Internal IP | Action | Protocol | Ruleset or Rule | Date & Time |
|---|---|---|---|---|---|---|---|---|
| FW | SITE300SYS1x1x30x1IFTunnel100001 | SITE300SYS1x1x30x1IFTunnel100001 | 8.8.8.8 | 10.30.1.1 | Allowed | ICMP | Default Rule (2085272) | Sep 21, 2022 7:11 PM |
| FW | SITE300SYS1x1x30x1IFTunnel100001 | SITE300SYS1x1x30x1IFTunnel100001 | 8.8.8.8 | 10.30.1.1 | Allowed | ICMP | Default Rule (2085272) | Sep 21, 2022 7:02 PM |
| FW | SITE300SYS1x1x30x1IFTunnel100001 | SITE300SYS1x1x30x1IFTunnel100001 | 8.8.8.8 | 10.30.1.1 | Allowed | ICMP | Default Rule (2085272) | Sep 21, 2022 5:16 AM |

# 生产数据策略示例

典型的生产数据策略示例。

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

如果有问题，它会匹配来自任何来源的Google Apps，然后回退到路由。

# 相关信息

[Cisco IOS-XE SDWAN策略文档]

[Cisco IOS-XE数据路径数据包跟踪功能文档]

[技术支持和文档 - Cisco Systems]

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。