

使用資料策略配置到SIG的流量重定向：回退到路由

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景](#)

[問題定義](#)

[軟體體系結構](#)

[組態](#)

[vSmart策略](#)

[在CEdge上驗證](#)

[政策](#)

[確認](#)

[檢查資料策略計數器](#)

[封包追蹤軌跡](#)

[資料包12](#)

[資料包13](#)

[驗證回退到路由](#)

[在Umbrella門戶上](#)

[生產資料策略示例](#)

[相關資訊](#)

簡介

本文檔介紹如何配置資料策略，以允許流量在SIG隧道失敗時回退到路由。

必要條件

需求

思科建議您瞭解思科軟體定義廣域網(SDWAN)解決方案。

在應用資料策略將應用流量重定向到SIG之前，必須配置SIG隧道。

採用元件

本文中的策略在軟體版本20.9.1和Cisco IOS-XE 17.9.1上進行了測試。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景

通過此功能，您可以配置當所有SIG隧道都關閉時，作為回退機制通過Cisco SD-WAN重疊路由的網際網路繫結流量。

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

問題定義

在20.8之前的版本中，資料策略中的SIG操作在預設情況下是嚴格的。如果SIG隧道關閉，則丟棄流量。

軟體體系結構

您還可以選擇不嚴格並回退到路由以通過重疊傳送流量。

路由可能導致重疊或其他轉發路徑（如NAT-DIA）。

總之，預期行為如下：

- 您可以選擇將SIG操作選擇為預設嚴格或回退到路由。
- 預設行為是strict。如果SIG隧道關閉，則會丟棄流量。
- 如果啟用回退到路由，
 - 如果SIG隧道為UP，則通過SIG傳送流量。
 - 如果SIG隧道關閉，則不會丟棄流量。流量進行正常路由。

 附註：路由也可以通過NAT DIA，如果使用者同時配置了SIG路由（通過配置或策略操作）和NAT DIA(ip nat route vrf 1 0.0.0.0 0.0.0.0 global)，並且如果隧道關閉，路由將指向NAT DIA。如果您擔心安全性（即，所有流量可以經過重疊或SIG，但不能通過DIA），則不得配置NAT DIA。

- 如果SIG隧道變為UP，則僅通過SIG傳送新流。任何當前流量都不會經過SIG操作。
- 如果SIG隧道關閉，所有流量都會通過路由，包括任何當前流和新流。

 注意：當前流量先進入SIG隧道，然後切換到路由可以中斷端到端會話。新流經過路由

組態

vSmart策略

資料策略

<#root>

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
!
!
!
```

應用策略

<#root>

vSmart-1#

show running-config apply-policy

```
apply-policy
site-list Site300
data-policy _VPN10_sig-default-fallback-to-routing all
!
!
```

使用vSmart策略的策略生成器時，選中Fallback to Routing覈取方塊，以便在所有SIG隧道都關閉時通過Cisco SD-WAN覆蓋路由網際網路流量。

Custom
Data

+ Sequence Rule
Drag and drop to re-arrange rules

Match

Actions

☒ Accept
 ☐ Drop

Protocol

IPv4

Optimization

Loss Correction

TLOC

VPN

Secure Internet Gateway

Match Conditions

Source Data Prefix List

DEFAULT

x

Source: IP Prefix

Example: 10.0.0.0/12

Actions

Accept

Enabled

Counter Name

COUNT

Secure Internet Gateway

Enabled

☐ Fallback to Routing

Cancel

Save Match And Actions

在UI上選擇Fallback to Routing操作時，會將fallback-to-routing和sig-action新增到action accept下的配置中。

在CEdge上驗證

政策

<#root>

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
```

確認

使用ping確認流量正在路由。

<#root>

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命令驗證流量預計採用的路徑。

<#root>

Site300-cE1#

show sdwan policy service-path vpn 10 interface GigabitEthernet 3 source-ip 10.30.1.1 dest-ip 8.8.8.8 pr

```
Number of possible next hops: 1
Next Hop: Remote
  Remote IP: 0.0.0.0, Interface  Index: 29
```

<#root>

Site300-cE1#

show sdwan policy service-path vpn 10 interface GigabitEthernet 3 source-ip 10.30.1.1 dest-ip 8.8.8.8 pr

```
Number of possible next hops: 1
Next Hop: Remote
  Remote IP: 0.0.0.0, Interface  Index: 29
```

檢查資料策略計數器

首先，使用命令clear sdwan policy data-policy從0開始清除計數器。 您可以使用show sdwan policy data-policy-filter命令驗證計數器是否已運行。

<#root>

Site300-cE1#

clear sdwan policy data-policy

<#root>

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傳送幾個您預計要透過SIG通道路由的封包。

<#root>

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命令檢驗ICMP資料包是否命中您的資料策略序列。

<#root>

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
```

封包追蹤軌跡

設定資料包跟蹤以瞭解路由器對資料包的響應。

```
<#root>
```

```
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)

資料包12

來自資料包12的片段顯示在資料策略中的流量命中序列1，並且被重定向到SIG。

```
<#root>
```

```
Feature: SDWAN Data Policy IN
  VPN ID      : 10
  VRF         : 1
  Policy Name : sig-default-fallback-VPN10 (CG:1)
  Seq        :
```

```
DNS Flags      : (0x0) NONE
Policy Flags   : 0x10110000
Nat Map ID     : 0
SNG ID        : 0
Action         :
```

REDIRECT_SIG Success 0x3

```
Action        :
```

SECONDARY_LOOKUP Success

輸出介面的輸入查詢顯示隧道介面（邏輯）。

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

IPSec加密後，輸入介面將被填充。

```
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
```

路由器會執行其他幾個動作，然後在GigabitEthernet1介面上傳輸封包。

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

路由器收到來自遠端IP(8.8.8.8)的回應，但不確定要由誰傳送回應，如Output:<unknown>輸出。

```
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
```

由於封包是在內部產生的，因此路由器會使用它，並且輸出顯示為<internal0/0/rp:0>。

<#root>

```
Feature: INTERNAL_TRANSMIT_PKT_EXT
  Entry      : Output - 0x813ebe6c
  Input      : Tunnel100001
  Output     :
```

internal0/0/rp:0

```
Lapsed time : 5785 ns
```

之後，封包會被傳送到Cisco IOSd程式，該程式會記錄對封包執行的動作。VRF 10中的本地介面IP地址為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
```

驗證回退到路由

您可以在傳輸介面(TLOC)(GigabitEthernet1) (即Biz-Internet) 上模擬故障切換，執行管理性關閉。 它有網際網路連線。

GigabitEthernet2 - MPLS TLOC為UP/UP，但沒有網際網路連線。 可以在show sdwan control local-properties wan-interface-list輸出中看到控制狀態。

<#root>

Site300-cE1#

show sdwancontrollocal-properties wan-interface-list

INTERFACE	PUBLIC IPv4	PUBLIC PORT	PRIVATE IPv4	PRIVATE IPv6
GigabitEthernet1	10.2.6.2	12346	10.2.6.2	::
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	::

在show ip interface brief 輸出中，GigabitEthernet1介面顯示為管理性關閉。

<#root>

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

通道100001路處於UP/DOWN狀態。

<#root>

Tunnel100001 10.2.6.2 YES TFTP

up

down

現在沒有網際網路連線，因此從VRF 10到8.8.8.8的連通性失敗。

```
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 命令顯示預期將採用要轉到DC (資料中心) 的OMP預設路由 (回退到路由) 。

本地路由器MPLS TLOC IP地址為10.1.6.2。

<#root>

```
Site300-cE1#
show sdwan policy service-path vpn 10 interface GigabitEthernet 3 source-ip 10.30.1.1 dest-ip 8.8.8.8 pr

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

Site300-cE1#
show sdwan policy service-path vpn 10 interface GigabitEthernet 3 source-ip 10.30.1.1 dest-ip 8.8.8.8 pr

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
```

在Umbrella門戶上

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	...

生產資料策略示例

典型的生產資料策略示例。

```
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
```

如果有問題，它會與來自任何來源的Google Apps匹配，並返回到路由。

相關資訊

[Cisco IOS-XE SDWAN策略文檔](#)

[Cisco IOS-XE資料路徑資料包跟蹤功能文檔](#)

[技術支援與文件 - Cisco Systems](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。