データポリシーを使用したSIGへのトラフィックリダイレクションの設定：ルーティングへのフォールバック

内容

概要

このドキュメントでは、SIGトンネルに障害が発生したときにトラフィックがルーティングにフォールバックできるようにデータポリシーを設定する方法について説明します。

前提条件

要件

Cisco Software Defined Wide Area Network(SDWAN)ソリューションに関する知識があることが推奨されます。

SIGへのアプリケーショントラフィックのリダイレクトにデータポリシーを適用する前に、SIGトンネルを設定する必要があります。

使用するコンポーネント

この記事のポリシーは、ソフトウェアバージョン20.9.1およびCisco IOS-XE 17.9.1でテストされています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景

この機能を使用すると、すべてのSIGトンネルがダウンしたときに、フォールバックメカニズムとしてCisco SD-WANオーバーレイを介してインターネットに送信されるトラフィックをルーティングするように設定できます。

この機能は、Cisco IOS XEリリース17.8.1aおよびCisco vManageリリース20.8.1で導入されました

問題の定義

20.8より前のバージョンでは、データポリシーのSIGアクションはデフォルトで厳密です。
SIGトンネルがダウンすると、トラフィックはドロップされます。

ソフトウェア アーキテクチャ

また、トラフィックをオーバーレイ経由で送信するルーティングに対して、厳密でなくフォールバックを選択するオプションもあります。

ルーティングは、オーバーレイまたはNAT-DIAのような他の転送パスにつながる可能性があります。

要約すると、予想される動作は次のようになります。

- SIGアクションをデフォルトの厳密または**fallback-to-routing**として選択するオプションがあります。
- デフォルトの動作は**strict**です。 SIGトンネルがダウンすると、トラフィックはドロップされます。
- **fallback-to-routing**が有効な場合、 SIGトンネルがUPの場合、トラフィックはSIGを介して送信されます。SIGトンネルがダウンしている場合、トラフィックはドロップされません。トラフィックは通常のルーティングを受けます。 **注**：ルーティングもNAT DIAを経由する可能性があります。ユーザにSIGルート（設定経由またはポリシーアクション経由）とNAT DIAの両方が設定されていて(ip nat route vrf 1 0.0.0.0 0.0.0.0 global)、トンネルがダウンした場合、ルーティングはNAT DIAを指します。セキュリティに関心がある場合（つまり、すべてのトラフィックがオーバーレイまたはSIGを経由して送信され、DIAを経由しない場合）、NAT DIAを設定しないでください。SIGトンネルがアップ状態になると、新しいフローだけがSIGを介して送信されます。現在のフローはSIGアクションを受けません。SIGトンネルがDOWNになると、すべてのトラフィックはルーティングを経由し、現在のフローと新しいフローの両方を通過します。 **注**：現在のフローは以前にSIGトンネルに入り、ルーティングに切り替えられると、エンドツーエンドセッションを中断する可能性があります。新しいフロ

ーはルーティングされる

コンフィギュレーション

vSmartポリシー

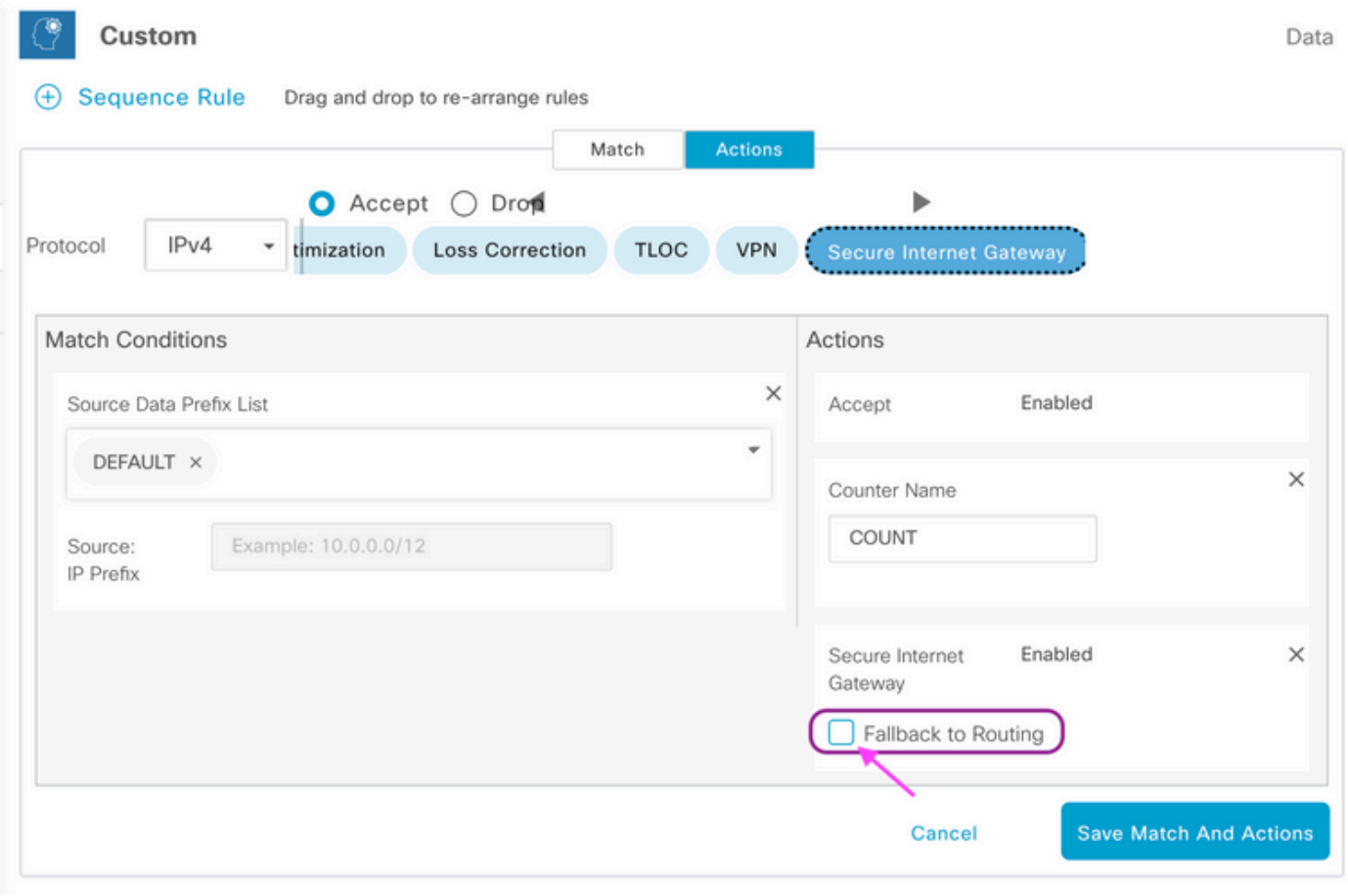
データポリシー

```
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 ! ! !
```

ポリシーの適用

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

vSmartポリシーのポリシービルダーを使用する場合は、[Fallback to Routing] チェックボックスをオンにして、インターネットに送信されるトラフィックを、すべてのSIGトンネルがダウンした場合にCisco SD-WANオーバーレイを介してルーティングします。



UIで**Fallback to Routing**アクションが選択されている場合、action accept**の下の設定にfallback-to-routing**とsig-action**が追加されます。**

cEdgeでの確認

ポリシー

```
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
```

Confirm

pingを使用して、トラフィックがルーティングされていることを確認します。

```
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#
```

show sdwan policy service-pathコマンドを使用して、トラフィックが通過すると予想されるパスを確認できます。

```
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
```

データポリシーカウンタの確認

最初に、コマンドclear sdwan policy data-policyを使用してカウンタをクリアし、0から開始します。 show sdwan policy data-policy-filterコマンドを使用して、カウンタの値を確認できます。

```
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
```

pingを使用して、SIGトンネル経由でルーティングする予定のパケットをいくつか送信します。

```
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#
```

show sdwan policy data-policy-filterコマンドを使用して、ICMPパケットがデータポリシーシーケンスにヒットすることを確認します。

```
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
```

パケットトレース

ルータでパケットに何が起こるかを理解するためのパケットトレースを設定します。

```
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)
```

パケット12

パケット12からのスニペットは、データポリシーのトラフィックヒットシーケンス1を示し、SIGにリダイレクトされます。

```
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
```

出力インターフェイスの入力ルックアップは、トンネルインターフェイス（論理）を示しています。

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

IPSec暗号化の後、入力インターフェイスにデータが入力されます。

```
  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
```

ルータは他のいくつかのアクションを実行してから、GigabitEthernet1インターフェイスにパケットを送信します。

```
  Feature: MARMOT_SPA_D_TRANSMIT_PKT
    Entry       : Output - 0x8142f02c
    Input       : GigabitEthernet1
    Output      : GigabitEthernet1
```

```
    Lapsed time : 2223 ns
```

パケット13

ルータはリモートIP(8.8.8.8)から応答を受信しますが、出力のOutput: <unknown>に示されているように、誰がそれを送信するのかわからない状態です。

```
  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
```

パケットは内部的に生成されるため、ルータによって消費され、出力は<internal0/0/rp:0>として表示されます。

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

その後、パケットはCisco IOSdプロセスにパントされ、パケットに対するアクションが記録されます。VRF 10のローカルインターフェイスのIPアドレスは10.30.1.1です。

```
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
```

フォールバックツールーティングの確認

Biz-InternetであるTransport Interface(TLOC)(GigabitEthernet1)で、管理シャットダウンを使用し

てフェールオーバーをシミュレートできます。 インターネットに接続されている。

GigabitEthernet2:MPLS TLOCはUP/UPですが、インターネット接続はありません。 制御ステータスは、**show sdwan control local-properties wan-interface-list**の出力で確認できます。

```
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
```

show ip interface briefの出力から、GigabitEthernet1インターフェイスはadministratively downと表示されます。

```
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
```

トンネル100001は**UP/DOWN**状態です。

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

現在インターネット接続がないため、VRF 10から8.8.8.8への到達可能性が失われます。

```
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コマンドは、DC（データセンター）に向かうOMPデフォルトルート（フォールバックツールーティング）が使用される予定であることを示します。

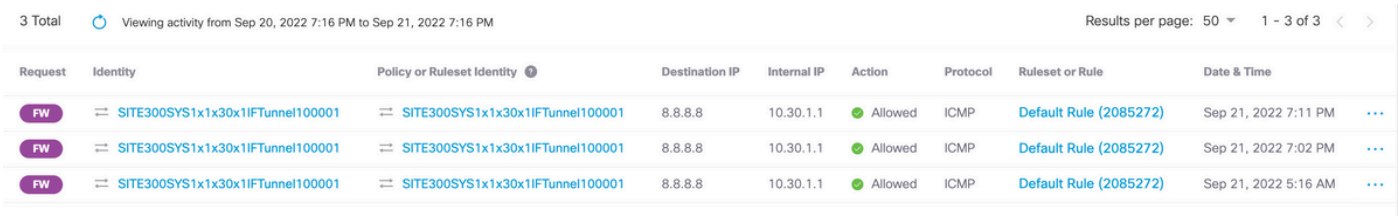
ローカルルータのMPLS TLOC IPアドレスは10.1.6.2です。

```
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
```

On Umbrellaポータル



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

本番データ・ポリシーの例

一般的な本番データ・ポリシーの例。

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

これは、任意のソースからGoogle Appsに一致し、問題がある場合はルーティングにフォールバックします。

関連情報

[Cisco IOS-XE SDWANポリシードキュメント]

[Cisco IOS XEデータパスパケットトレース機能に関するドキュメント]

[テクニカル サポートとドキュメント – Cisco Systems]

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。