데이터 정책을 사용하여 SIG로 트래픽 리디렉션 구성: 라우팅으로 대체

목차

소개

이 문서에서는 SIG 터널이 실패할 때 트래픽이 라우팅으로 대체되도록 데이터 정책을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco SDWAN(Software Defined Wide Area Network) 솔루션에 대한 지식이 있는 것이 좋습니다.

애플리케이션 트래픽을 SIG에 리디렉션하기 위해 데이터 정책을 적용하기 전에 SIG 터널을 구성해야 합니다.

사용되는 구성 요소

이 문서의 정책은 소프트웨어 버전 20.9.1 및 Cisco IOS-XE 17.9.1에서 테스트되었습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경

이 기능을 사용하면 모든 SIG 터널이 다운되었을 때 Cisco SD-WAN 오버레이를 통해 라우팅되도록 인터넷 바인딩 트래픽을 폴백 메커니즘으로 구성할 수 있습니다.

이 기능은 Cisco IOS XE Release 17.8.1a 및 Cisco vManage Release 20.8.1에 도입되었습니다

문제 정의

20.8 버전 이전에는 기본적으로 데이터 정책의 SIG 작업이 엄격합니다. SIG 터널이 다운되면 트래픽이 삭제됩니다.

소프트웨어 아키텍처

엄격하지 않도록 선택하고 라우팅을 대체하여 오버레이를 통해 트래픽을 전송하도록 선택할 수 있는 추가 옵션이 있습니다.

라우팅은 오버레이 또는 NAT-DIA와 같은 기타 포워딩 경로로 이어질 수 있습니다.

요약하면, 예상되는 동작은 다음과 같습니다.

- SIG 작업을 기본 strict 또는 fallback-to-routing으로 선택할 **수 있습니다**.
- 기본 동작은 **엄격합니다**. SIG 터널이 다운되면 트래픽이 삭제됩니다.
- 대체**-라우팅**이 활성화된 경우 SIG 터널이 UP인 경우 트래픽은 SIG를 통해 전송됩니다.SIG 터널이 다운되면 트래픽은 삭제되지 않습니다. 트래픽은 정상적인 라우팅을 거칩니다. **참고**: 사용자가 SIG 경로(컨피그레이션 또는 정책 작업을 통해)와 NAT DIA를 모두 구성한 경우(ip nat route vrf 1 0.0.0 0 0.0.0.0 global) NAT DIA를 통해 라우팅할 수 있으며 터널이 다운되면 라우팅이 NAT DIA를 가리킵니다. 보안에 관심이 있는 경우(즉, 모든 트래픽이 DIA가 아닌 오버레이 또는 SIG를 통해 이동할 수 있는 경우) NAT DIA를 구성하지 않아야 합니다.SIG 터널이 UP가 되면 새 플로우만 SIG를 통해 전송됩니다. 현재 흐름에서는 SIG 작업을 수행하지 않습니다 .SIG 터널이 DOWN이 되면 모든 트래픽은 라우팅을 통해 라우팅되며, 모든 현재 흐름과 새 흐름이 모두 수행됩니다. **참고**:현재 흐름은 SIG 터널에서 시작되어 라우팅으로 전환되어 엔드 투 엔드 세션을 중단할 수 있습니다. 새 플로우가 라우팅을 거침

설정

vSmart 정책

데이터 정책

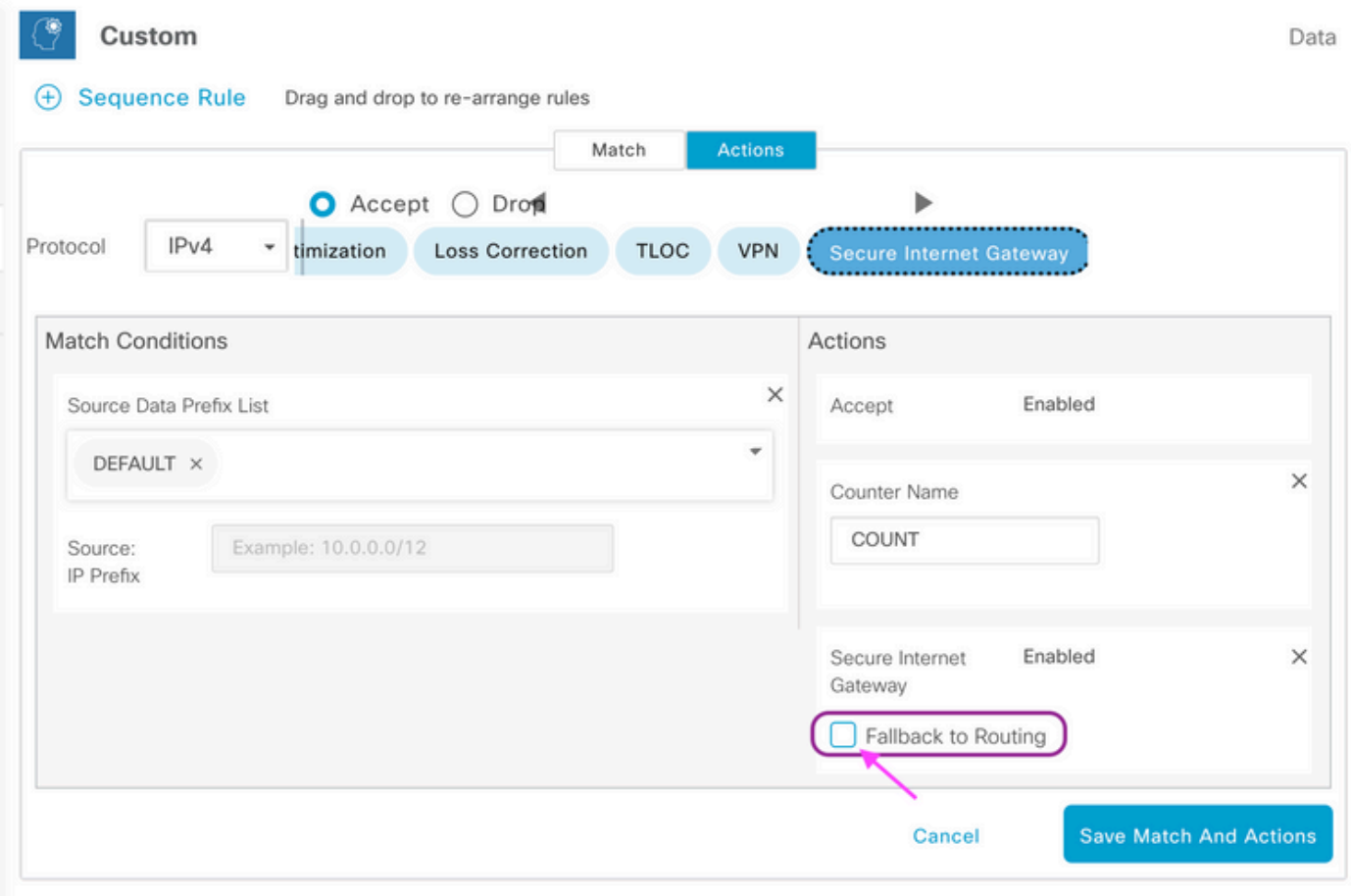
```
vSmart-1# show running-config policy
policy
 data-policy _VPN10_sig-default-fallback-to-routing
```

```
  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 ! ! !

정책 적용

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

vSmart Policy용 정책 구성기를 사용할 경우, 모든 SIG 터널이 다운되었을 때 Cisco SD-WAN 오버레이를 통해 인터넷 바인딩 트래픽을 라우팅하려면 Fallback **to Routing(라우팅**으로 대체) 확인란을 선택합니다.



UI에서 **Fallback to** Routing(라우팅으로 대체) 작업**을** 선택한 경우, Action accept(작업 수락) 아래에서 컨피그레이션에 Fallback-**to-routing(라우팅**으로 대체) 및 sig-action(sig-작업*)이 추가됩니다.*

cEdge에서 확인

정책

```
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
```

확인

Ping을 사용하여 트래픽이 라우팅되고 있는지 **확인합니다**.

```
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 명령을 사용하여 트래픽이 취할 것으로 예상되는 **경로를** 확인할 수 있습니다.

```
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
```

데이터 정책 카운터 확인

먼저 clear sdwan **policy data-**policy 명령을 **사용하여 카운터를 지우고** 0에서 시작합니다. **show sdwan policy data-policy-filter 명령**으로 **카운터를 확인할** 수 있습니다.

```
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**을** 사용하여 SIG 터널을 통해 라우팅할 것으로 예상되는 패킷 몇 개를 전송합니다.

```
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** 명령을 사용하여 ICMP 패킷이 **데이터 정책 시퀀스에 도달했는지** 확인합니다.

```
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
```

패킷 추적

라우터의 패킷에 어떤 일이 발생하는지 파악하기 위해 패킷 추적을 설정합니다.

```
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)
```

패킷 12

패킷 12의 스니펫은 데이터 정책의 트래픽 히트 시퀀스 1을 보여주며 SIG로 리디렉션됩니다.

```
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
```

출력 인터페이스에 대한 입력 조회는 터널 인터페이스(논리)를 표시합니다.

```
  Feature: IPV4_INPUT_LOOKUP_PROCESS_EXT
    Entry       : Input - 0x81418130
    Input       : internal0/0/rp:0
    Output      : Tunnel100001
```

```
    Lapsed time : 446 ns
```

IPSec 암호화 후 입력 인터페이스가 채워집니다.

```
  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
```

라우터는 다른 여러 작업을 수행한 다음 GigabitEthernet1 인터페이스에서 패킷을 전송합니다.

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

패킷 13

라우터는 원격 IP(8.8.8.8)로부터 응답을 수신하지만, 출력에 **<unknown>**으로 표시된 대로 누구에게 전송할지에 대해 확신할 수 없습니다.

```
  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
```

패킷은 내부에서 생성되므로 라우터에서 소비되고 출력은 **<internal0/0/rp:0>으로 표시됩니다**.

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

그런 다음 패킷은 Cisco IOSd 프로세스로 보내지며, 이 프로세스에서는 패킷에 대해 수행하는 작업을 기록합니다. VRF 10의 로컬 인터페이스 ip 주소는 10.30.1.1입니다.

```
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
```

라우팅 대체 확인

Biz-Internet인 TLOC(전송 인터페이스)(GigabitEthernet1)에서 관리 종료를 사용하여 장애 조치를 시뮬레이션할 수 있습니다. 인터넷 연결이 됩니다

GigabitEthernet2 - MPLS TLOC가 UP/UP이지만 인터넷에 연결되어 있지 않습니다. 제어 상태는 **show sdwan control local-properties wan-interface-list 출력에서 확인할** 수 있습니다.

```
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 출력에서 GigabitEthernet1 인터페이스는 관리상 다운된 상태로 표시됩니다.

```
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
```

터널 100001이 **UP/DOWN** 상태입니다.

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

현재 인터넷 연결이 없으므로 VRF 10에서 8.8.8.8에 연결할 수 없습니다.

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)

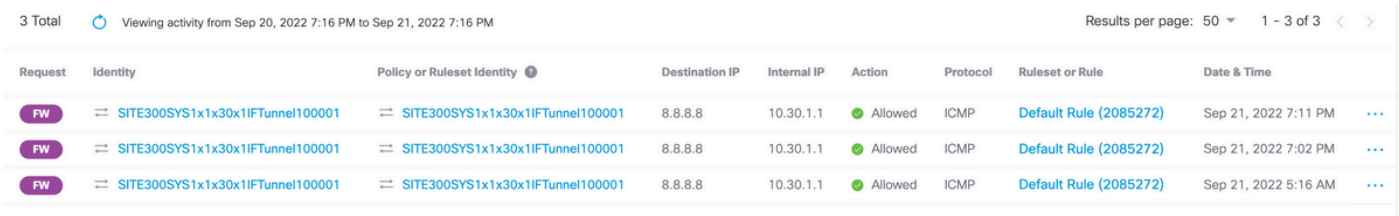
show sdwan policy service-path 명령은 DC(데이터 센터)로 이동할 OMP 기본 경로(fallback-to-routing)가 예상됨을 보여줍니다.

로컬 라우터 MPLS TLOC IP 주소는 10.1.6.2입니다.

```
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
```

Umbrella 포털



프로덕션 데이터 정책 예

일반적인 프로덕션 데이터 정책 예.

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

Google Apps와 어떤 소스에서든 매칭되며 문제가 있는 경우 라우팅으로 돌아갑니다.

관련 정보

Cisco IOS-XE SDWAN 정책 설명서

Cisco IOS-XE Datapath 패킷 추적 기능 설명서

기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.