Configureer de omleiding van verkeer naar SIG met databeleid: terugval naar routing

Inhoud

Inleiding

Dit document beschrijft hoe u een gegevensbeleid moet configureren om verkeer in staat te stellen terug te vallen op routing wanneer SIG-tunnels uitvallen.

Voorwaarden

Vereisten

Cisco raadt u aan bekend te zijn met Cisco Software Defined Wide Area Network (SDWAN)-oplossing.

Alvorens u een gegevensbeleid voor omleiding van toepassingsverkeer op een SIG toepast, moet u tunnels vormen SIG.

Gebruikte componenten

Het beleid in dit artikel is getest op versie 20.9.1 en Cisco IOS-XE 17.9.1.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrond

Met deze functie kunt u internetgebonden verkeer dat via de Cisco SD-WAN overlay moet worden gerouteerd, configureren als fallback-mechanisme, wanneer alle SIG-tunnels zijn uitgeschakeld.

Deze functie wordt geïntroduceerd in Cisco IOS XE release 17.8.1a en Cisco vManager release 20.8.1

Probleemdefinitie

Voorafgaand aan versie 20.8, is de SIG-actie in het databeleid standaard streng. Als SIG-tunnels uitvallen wordt het verkeer verbroken.

Softwarearchitectuur

U kunt een extra optie hebben om te kiezen niet streng te zijn en terug te vallen op routing om verkeer via de overlay te verzenden.

Routing kan leiden tot de overlay of andere doorsturen paden zoals NAT-DIA.

Samenvattend kan worden gesteld dat de verwachte gedragingen als volgt zijn:

- U hebt de optie om SIG-actie te kiezen als standaard strikt of **reserve-naar-routing**.
- Standaardgedrag is **strikt**. Als SIG-tunnels uitvallen wordt het verkeer verbroken.
- Als **fallback-to-routing** is ingeschakeld, Als de SIG-tunnels omhoog zijn, wordt het verkeer via SIG verzonden.Als de SIG-tunnels zijn INGEDRUKT, wordt het verkeer NIET gedropt. Het verkeer ondergaat de normale routing. **Opmerking**: Routing kan ook via NAT DIA lopen, als de gebruiker zowel SIG-route (via configuratie of via beleidsactie) als NAT DIA geconfigureerd heeft (ip Nat-route vrf 1 0.0.0 0.0.0.0 wereldwijd) en als de tunnel neervalt, zou de routing naar NAT DIA wijzen. Als u zich zorgen maakt over beveiliging (d.w.z. dat al het verkeer kan gaan via overlay of via SIG maar niet via DIA), dan MOET NAT DIA niet worden geconfigureerd.Als de SIG-tunnel omhoog komt, worden alleen nieuwe stromen over SIG verzonden. De SIG-actie is niet van toepassing op de huidige stromen.Als de SIG-tunnel omlaag gaat, gaat al het verkeer via routing, zowel alle huidige stromen als nieuwe stromen. **Opmerking**:de huidige stromen verlopen via SIG-tunnels en overgeschakeld op routing kan end-to-end sessies onderbreken. Nieuwe stromen ondergaan routing

Configuratie

vSmart-beleid

Gegevensbeleid

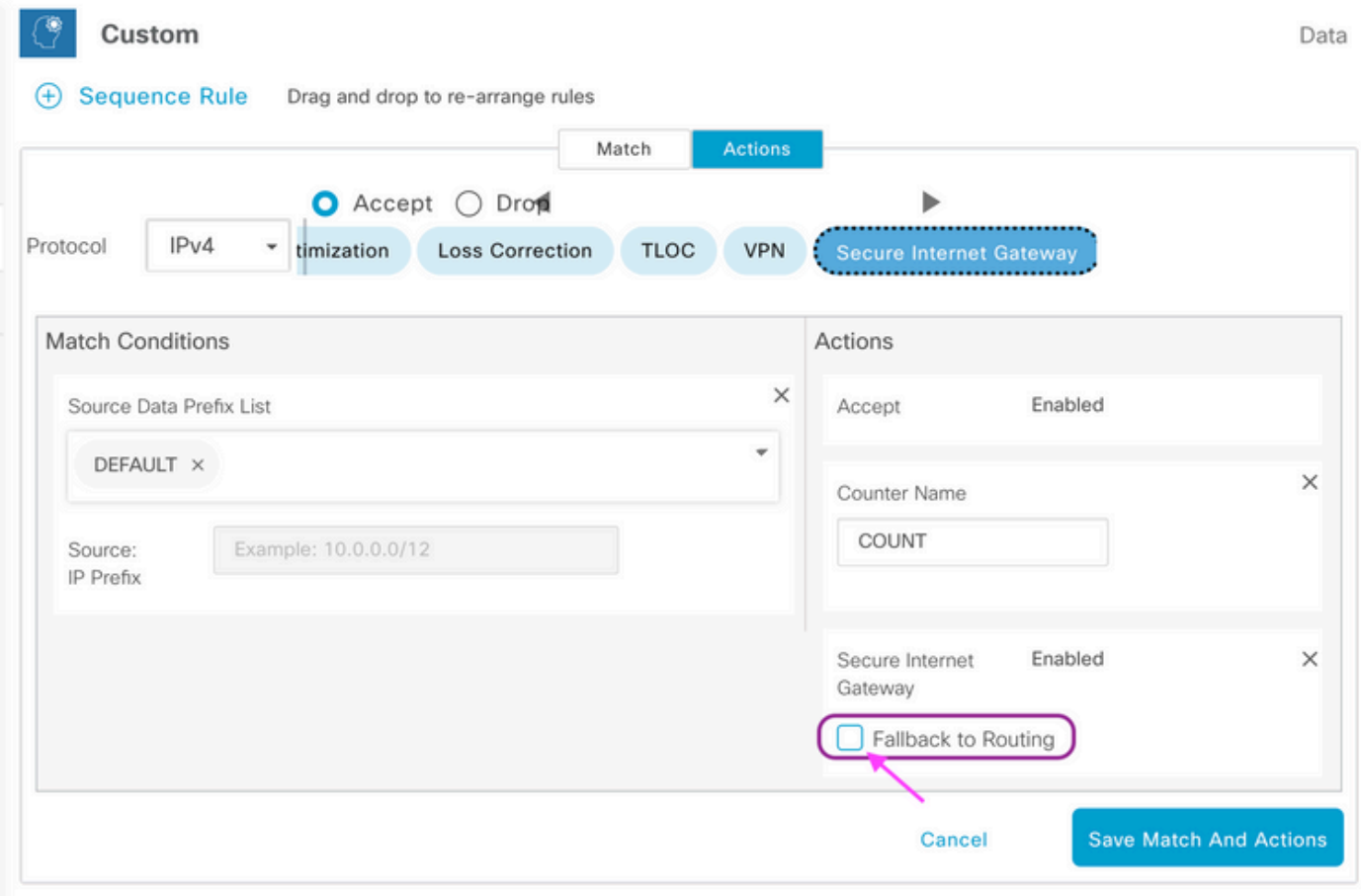
```
vSmart-1# show running-config policy
policy
 data-policy _VPN10_sig-default-fallback-to-routing
  vpn-list VPN10
   sequence 1
    match
     source-data-prefix-list Default
    !
    action accept
     count Count_26488854
     sig
```

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 ! ! !

Toepassingsbeleid

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

Wanneer de Policy Builder voor het vSmart Policy wordt gebruikt, schakelt u het selectievakje **Fallback to Routing in** om internetverkeer via de Cisco SD-WAN-overlay te leiden wanneer alle SIG-tunnels zijn uitgeschakeld.



Wanneer de **reserve aan het Verpletteren van** actie op UI wordt geselecteerd, worden de **reserve-aan-routing** en **sig-action** toegevoegd aan de configuratie onder *actie accepteren.*

Verifiëren op cEdge

Beleid

```
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
```

Bevestigen

Bevestig dat het verkeer met het gebruik van **ping** routeert.

```
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#
```

U kunt het pad verifiëren dat het verkeer naar verwachting zal nemen met de opdracht **Service-path beleid van** de **show**.

```
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
```

Tellers voor gegevensbeleid controleren

Eerst, ontruim de tellers met het bevel **duidelijke sdwan beleid data-policy** om bij 0 te beginnen. U kunt controleren of de teller met de opdracht **Sdwan policy data-policy-filter** was.

```
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
```

Gebruik **ping** om een paar pakketten te verzenden die u verwacht via de SIG-tunnel te leiden.

```
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#
```

Controleer of de ICMP-pakketten uw gegevensbeleidssequentie raken met de opdracht **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
```

PacketTrace

Stel een pakketspoor in om te begrijpen wat er met de pakketten met de router gebeurt.

```
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)
```

Pakket 12

Een fragment van pakket 12 toont de traffic hit sequentie 1 in het gegevensbeleid en wordt omgeleid naar 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
```

De invoerraadpleging voor de uitvoerinterface toont de (logische) tunnelinterface.

```
  Feature: IPV4_INPUT_LOOKUP_PROCESS_EXT
```

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

Na de IPSec-encryptie wordt de invoerinterface gevuld.

```
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
```

De router neemt een aantal andere acties en verzendt vervolgens het pakket naar de Gigabit Ethernet1-interface.

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

Packet-over-13

De router ontvangt de reactie van Remote IP (8.8.8.8), maar is niet zeker wie het moet verzenden zoals aangegeven door **Output: <known>** in de output.

```
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
```

Aangezien het pakket intern wordt gegenereerd, wordt het door de router verbruikt en wordt de uitvoer weergegeven als **<internal0/0/rp:0>**.

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

Daarna wordt het pakket gepunteerd aan Cisco IOSd-proces, dat de acties op het pakket vastlegt. Het lokale IP-adres in VRF 10 is 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
```

Controleer Fallback-to-Routing

U kunt de failover simuleren met een administratieve shutdown op de Transport Interface (TLOC) (Gigabit Ethernet1), wat Biz-Internet is. Het heeft de internetverbinding.

Gigabit Ethernet2 - MPLS TLOC is UP/UP, maar heeft geen internetverbinding. De controlestatus kan in de output van de de **controle lokaal-eigenschappen van de showsdwan worden** gezien **wan-interface-lijst**.

```
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
```

Van de **korte** uitvoer van de **showip interface**, toont de Gigabit Ethernet1 interface administratief neer.

```
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
```

Tunnel 100001 is in een **UP/DOWN**-status.

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

Er is nu geen internetverbinding, dus bereikbaar via VRF 10 naar 8.8.8.8 mislukt.

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)

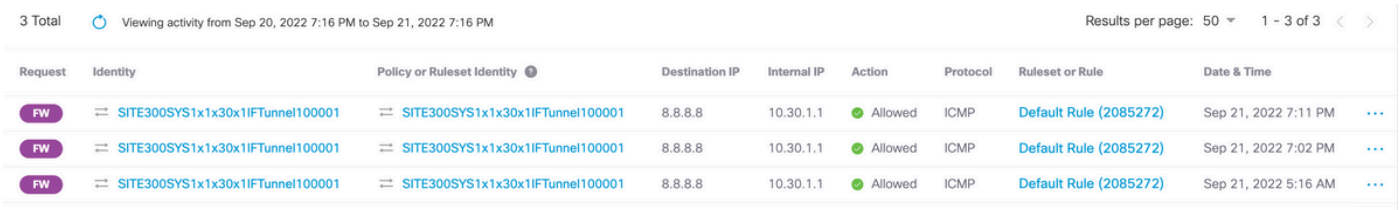
Het **service-path voor** beleid van de **show** toont aan dat de OMP standaard-route (fallback-to-routing) om naar de DC (datacenter) te gaan naar verwachting wordt genomen.

Het lokale router MPLS TLOC IP-adres is 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
```

Over de parapluportal



Voorbeeld van beleid inzake productiegegevens

Een typisch voorbeeld van het beleid van productiegegevens.

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

Het past de Google-apps uit elke bron en valt terug op routing, als er een probleem is.

Gerelateerde informatie

[Cisco IOS-XE SDWAN-beleidsdocumentatie]

Cisco IOS-XE Datapath Packet Trace-functiedocumentatie

Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.