Configuración de la redirección del tráfico a SIG con política de datos: reserva al routing

Contenido

Introducción

Este documento describe cómo configurar una política de datos para permitir que el tráfico se repliegue al ruteo cuando los túneles SIG fallan.

Prerequisites

Requirements

Cisco recomienda conocer la solución de red de área extensa definida por software (SDWAN) de Cisco.

Antes de aplicar una política de datos para la redirección del tráfico de aplicaciones a un SIG, debe configurar los túneles SIG.

Componentes Utilizados

La política de este artículo se probó en la versión de software 20.9.1 y Cisco IOS-XE 17.9.1.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Background

Con esta función, puede configurar el tráfico enlazado a Internet para que se rutee a través de la superposición SD-WAN de Cisco, como mecanismo de reserva, cuando todos los túneles SIG estén inactivos.

Esta función se introduce en Cisco IOS XE Release 17.8.1a y Cisco vManage Release 20.8.1

Definición del problema

Antes de la versión 20.8, la acción SIG en la política de datos es estricta de forma predeterminada. Si los túneles SIG están inactivos, el tráfico se interrumpe.

Arquitectura del software

Puede tener una opción adicional para elegir no ser estricto y recurrir al ruteo para enviar tráfico a través de la superposición.

El ruteo podría llevar a la superposición u otras trayectorias de reenvío como NAT-DIA.

En resumen, el comportamiento esperado debe ser el siguiente:

- Tiene la opción de elegir que la acción SIG sea estricta por defecto o **de repliegue al ruteo**.
- El comportamiento predeterminado es **estricto**. Si los túneles SIG están inactivos, el tráfico se interrumpe.
- Si se habilita **fallback-to-routing**, Si los túneles SIG están ACTIVOS, el tráfico se envía a través de SIG.Si los túneles SIG están INACTIVOS, el tráfico NO se interrumpe. El tráfico experimenta un ruteo normal. **Nota**: El ruteo también podría realizarse a través de NAT DIA, si el usuario tiene tanto ruta SIG (mediante configuración o acción de política) como NAT DIA configurados (ip nat route vrf 1 0.0.0.0 0.0.0.0 global) y si el túnel deja de funcionar, el ruteo apuntaría a NAT DIA. Si le preocupa la seguridad (es decir, todo el tráfico puede pasar por superposición o a través de SIG pero no a través de DIA), NAT DIA NO DEBE configurarse.Si el túnel SIG se activa, sólo se envían nuevos flujos a través de SIG. Los flujos actuales no se someterían a la acción SIG.Si el túnel SIG se DESACTIVA, todo el tráfico pasa por el ruteo, tanto los flujos actuales como los nuevos flujos. **Nota**: Los flujos actuales pasan por el túnel SIG antes de que el routing conmutado pueda interrumpir la sesión de extremo a extremo. Los nuevos flujos se enrutan

Configuración

Política vSmart

Política de datos

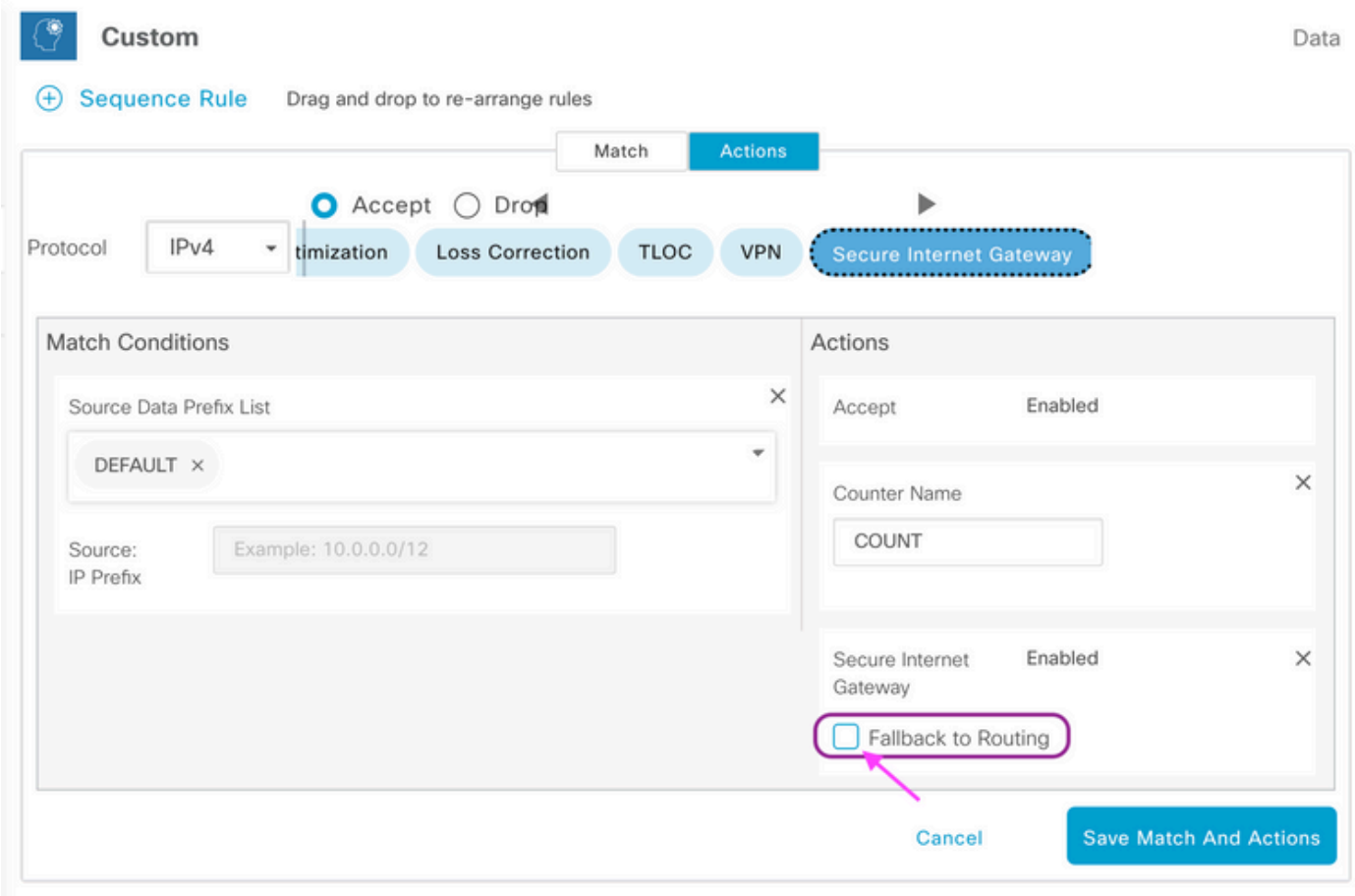
```
vSmart-1# show running-config policy
policy
 data-policy _VPN10_sig-default-fallback-to-routing
  vpn-list VPN10
   sequence 1
    match
     source-data-prefix-list Default
    !
    action accept
     count Count_26488854
     sig
```

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 ! ! !

Aplicar política

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

Cuando se utiliza el Policy Builder para la política vSmart, marque la casilla de verificación **Fallback to Routing** para enrutar el tráfico con destino a Internet a través de la superposición SD-WAN de Cisco cuando todos los túneles SIG estén desactivados.



Cuando se selecciona la acción **Fallback to Routing** en la interfaz de usuario, **fallback-to-routing** y

sig-action se agregan a la configuración en action accept.

Verificar en cEdge

Política

```
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
```

Confirmar

Confirme que el tráfico está ruteando con el uso de **ping**.

```
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#
```

Puede verificar la trayectoria que se espera que tome el tráfico con el comando **show sdwan policy service-path**.

```
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
```

Comprobar contadores de políticas de datos

Primero, borre los contadores con el comando **clear sdwan policy data-policy** para comenzar en 0. Puede verificar que el contador fue ejecutado con el comando **show sdwan policy data-policy-filter**.

```
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
```

Utilice **ping** para enviar algunos paquetes que espera rutear a través del túnel SIG.

```
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#
```

Verifique que los paquetes ICMP alcancen la secuencia de política de datos con el comando **show 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
```

Seguimiento de paquetes

Configure un seguimiento de paquetes para comprender qué sucede con los paquetes con el router.

```
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)
```

Paquete 12

Un fragmento del paquete 12 muestra la secuencia de aciertos de tráfico 1 en la política de datos y se redirige a 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
```

La búsqueda de entrada para la interfaz de salida muestra la interfaz de túnel (lógica).

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

Después del Cifrado IPSec, la interfaz de entrada se llena.

```
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
```

El router realiza otras acciones y luego transmite el paquete a la interfaz GigabitEthernet1.

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

Paquete 13

El router recibe la respuesta de la IP remota (8.8.8.8), pero no está seguro de a quién enviarla, como indica **Output: <unknown>** en la salida.

```
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
```

Dado que el paquete se genera internamente, el router lo consume y el resultado se muestra como **<internal0/0/rp:0>**.

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

Después de esto, el paquete se envía al proceso Cisco IOSd, que registra las acciones que se realizan en el paquete. La dirección IP de la interfaz local en VRF 10 es 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
```

Verificación de Fallback-to-Routing

Puede simular la conmutación por error con un cierre administrativo en la interfaz de transporte (TLOC) (GigabitEthernet1), que es Biz-Internet. Dispone de conexión a Internet.

GigabitEthernet2: MPLS TLOC está ACTIVADO/DESACTIVADO, pero no dispone de conexión a Internet. El estado del control se puede ver en el resultado de **show sdwan control local-properties wan-interface-list**.

```
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
```

Desde el resultado de **show ip interface brief**, la interfaz GigabitEthernet1 muestra

administrativamente inactiva.

```
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
```

El túnel 100001 se encuentra en un estado **UP/DOWN**.

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

Ahora no hay conexión a Internet, por lo que el alcance de 8.8.8.8 falla desde VRF 10.

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)

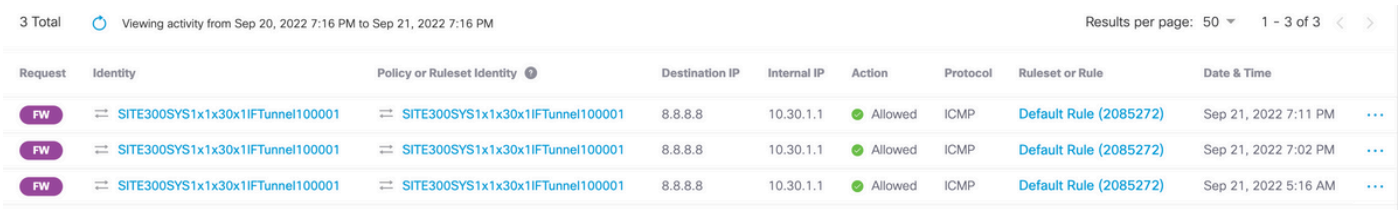
El comando **show sdwan policy service-path** muestra que se espera que se tome la ruta predeterminada de OMP (repliegue a ruteo) para ir al DC (centro de datos).

La dirección IP de MPLS TLOC del router local es 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
```

En Umbrella Portal



Ejemplo de política de datos de producción

Ejemplo típico de directiva de datos de producción.

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

Coincide con las aplicaciones de Google de cualquier fuente y vuelve al routing, si hay algún problema.

Información Relacionada

Documentación de la política SDWAN de Cisco IOS-XE

Documentación de la Función Cisco IOS-XE Datapath Packet Trace

Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).