Configurar o redirecionamento de tráfego para SIG com a política de dados: Fallback para roteamento

Contents

Introduction

Este documento descreve como configurar uma política de dados para permitir que o tráfego volte para o roteamento quando os túneis SIG falharem.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento da solução Cisco Software Defined Wide Area Network (SDWAN).

Antes de aplicar uma política de dados para redirecionamento de tráfego de aplicação para um SIG, você deve configurar túneis SIG.

Componentes Utilizados

A política neste artigo foi testada na versão de software 20.9.1 e no Cisco IOS-XE 17.9.1.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Background

Com esse recurso, você pode configurar o tráfego vinculado à Internet para ser roteado através da sobreposição de SD-WAN da Cisco, como um mecanismo de retorno, quando todos os túneis SIG estiverem inoperantes.

Esse recurso é apresentado no Cisco IOS XE versão 17.8.1a e no Cisco vManage versão 20.8.1

Definição do problema

Antes da versão 20.8, a ação SIG na política de dados é estrita por padrão. Se os túneis SIG estiverem inoperantes, o tráfego será descartado.

Arquitetura de software

Você pode ter uma opção adicional para optar por não ser estrito e retornar ao roteamento para enviar tráfego pela sobreposição.

O roteamento pode levar à sobreposição ou a outros caminhos de encaminhamento, como o NAT-DIA.

Em resumo, o comportamento esperado é o seguinte:

- Você tem a opção de escolher a ação SIG para ser o padrão strict ou **fallback-to-routing**.
- O comportamento padrão é **strict**. Se os túneis SIG estiverem inoperantes, o tráfego será descartado.
- Se **fallback-to-routing** estiver habilitado, Se os túneis SIG estiverem ATIVADOS, o tráfego será enviado através do SIG.Se os túneis SIG estiverem INATIVOS, o tráfego NÃO será descartado. O tráfego passa por roteamento normal. **Observação**: o roteamento pode ser via NAT DIA também, se o usuário tiver a rota SIG (via configuração ou via ação de política) e a NAT DIA configuradas (ip nat route vrf 1 0.0.0.0 0.0.0.0 global) e se o túnel for desativado, o roteamento apontará para a NAT DIA. Se você estiver preocupado com a segurança (ou seja, todo o tráfego pode passar por sobreposição ou via SIG, mas não via DIA), o NAT DIA NÃO DEVERÁ ser configurado.Se o túnel SIG se tornar UP, somente novos fluxos serão enviados pelo SIG. Quaisquer fluxos atuais não seriam submetidos à ação SIG.Se o túnel SIG se tornar INATIVO, todo o tráfego passará por roteamento, tanto os fluxos atuais quanto os novos fluxos. **Nota**:Os fluxos atuais vão para o túnel SIG antes e comutados para o roteamento podem quebrar a sessão fim-a-fim. Novos fluxos passam por roteamento

Configuração

Política vSmart

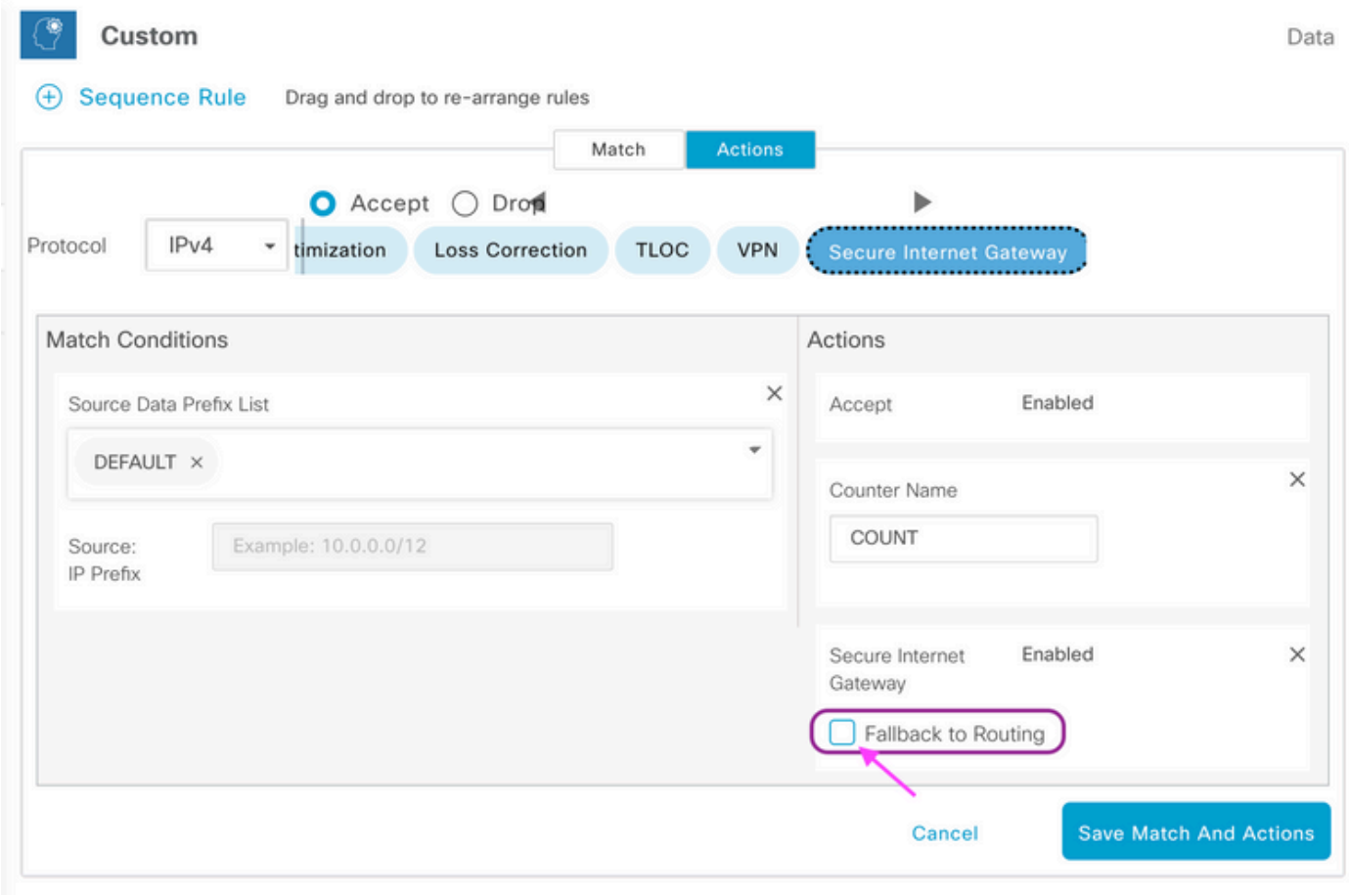
Política de dados

```
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
 !
!
```

Quando o Policy Builder for the vSmart Policy for usado, marque a caixa de seleção **Fallback to Routing** para rotear o tráfego vinculado à Internet através da sobreposição Cisco SD-WAN quando todos os túneis SIG estiverem inoperantes.



Quando a ação **Fallback to Routing** é selecionada na interface do usuário, fallback-to-routing **e** sig-action são adicionados à configuração sob a ação aceitar.

Verificar no 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 se o tráfego está sendo roteado com o uso do **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#
```

Você pode verificar o caminho que se espera que o tráfego siga com o 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
```

Verificar contadores de política de dados

Primeiro, limpe os contadores com o comando **clear sdwan policy data-policy** para iniciar em 0. Você pode verificar se o contador estava com o 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
```

Use o **ping** para enviar alguns pacotes que espera rotear através do 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 se os pacotes ICMP atingem sua sequência de política de dados com o 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
```

Rastreamento de pacotes

Configure um rastreamento de pacote para entender o que acontece com os pacotes com o roteador.

```
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)
```

Pacote 12

Um trecho do pacote 12 mostra a sequência de acerto de tráfego 1 na política de dados e é redirecionado para 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
```

A pesquisa de entrada para a interface de saída mostra a interface de túnel (lógica).

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

Após a Criptografia IPSec, a interface de entrada é preenchida.

```
  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
```

O roteador executa várias outras ações e, em seguida, transmite o pacote pela interface GigabitEthernet1.

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

```
    Lapsed time : 2223 ns
```

Pacote 13

O roteador recebe a resposta do IP remoto (8.8.8.8), mas não tem certeza de quem deve enviá-la, conforme indicado por **Output: <unknown>** na saída.

```
  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
```

Como o pacote é gerado internamente, ele é consumido pelo roteador e a Saída é mostrada como **<internal0/0/rp:0>**.

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

Depois disso, o pacote é apontado para o processo Cisco IOSd, que registra as ações tomadas no pacote. O endereço ip da interface local no VRF 10 é 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
```

Verificar Fallback-to-Routing

Você pode simular o failover com um desligamento administrativo na Interface de Transporte

(TLOC) (GigabitEthernet1), que é Biz-Internet. Ele tem a conexão com a Internet.

GigabitEthernet2 - MPLS TLOC é UP/UP, mas não tem conexão com a Internet. O status do controle pode ser visto na saída **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
```

Na saída **show ip interface brief**, a interface GigabitEthernet1 mostra inoperante administrativamente.

```
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
```

O 100001 do túnel está em um estado **UP/DOWN**.

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

Não há conexão com a Internet agora, portanto, o alcance do 8.8.8.8 falha no 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)
```

O comando **show sdwan policy service-path** mostra que se espera que a rota padrão OMP (fallback-to-routing) vá para o DC (data center).

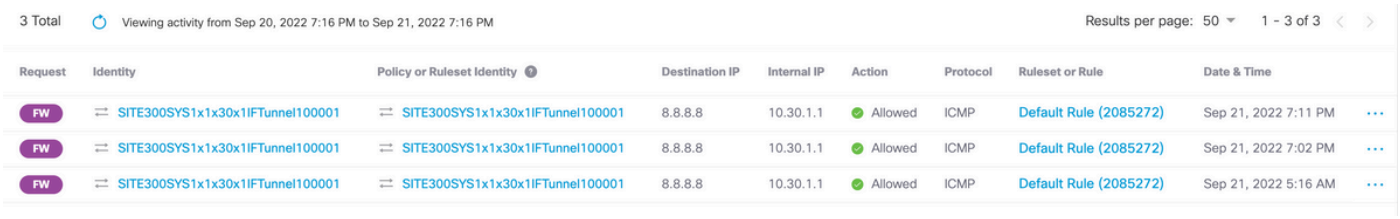
O endereço IP TLOC MPLS do roteador local é 10.1.6.2.

```
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
```

No portal Umbrella



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

Exemplo de política de dados de produção

Um exemplo típico de política de dados de produção.

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

Ele combina com o Google Apps de qualquer fonte e volta para o roteamento, se houver um problema.

Informações Relacionadas

Documentação da política SDWAN do Cisco IOS-XE

Documentação do recurso de rastreamento de pacote de caminho de dados do Cisco IOS-XE

Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.