Configura il reindirizzamento del traffico al SIG con il criterio dei dati: fallback al routing

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Sfondo
Descrizione del problema
Architettura software
Configurazione
Criterio vSmart
Verifica su cEdge
Policy
Conferma
Verifica contatori criteri dati
Traccia pacchetto
Pacchetto 12
Pacchetto 13
Verifica del fallback al routing
Su Umbrella Portal
Esempio di criteri dei dati di produzione
Informazioni correlate

Introduzione

In questo documento viene descritto come configurare una policy sui dati per consentire al traffico di tornare al routing quando i tunnel SIG hanno esito negativo.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza della soluzione SDWAN (Software Defined Wide Area Network) di Cisco.

Prima di applicare una policy sui dati per il reindirizzamento del traffico delle applicazioni a un SIG, è necessario configurare i tunnel SIG.

Componenti usati

La policy di questo articolo è stata testata sul software versione 20.9.1 e Cisco IOS-XE 17.9.1.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Sfondo

Con questa funzione, è possibile configurare il traffico Internet in modo che venga instradato attraverso la sovrimpressione Cisco SD-WAN, come meccanismo di fallback, quando tutti i tunnel SIG sono inattivi.

Questa funzione è stata introdotta in Cisco IOS XE release 17.8.1a e Cisco vManage release 20.8.1

Descrizione del problema

Nelle versioni precedenti alla 20.8, l'azione SIG nella policy sui dati è rigorosa per impostazione predefinita. Se i tunnel SIG sono inattivi, il traffico viene interrotto.

Architettura software

Èpossibile impostare un'opzione aggiuntiva per scegliere di non essere severi e di eseguire il fallback al routing per inviare il traffico sulla sovrapposizione.

Il routing potrebbe portare alla sovrapposizione o ad altri percorsi di inoltro come NAT-DIA.

In sintesi, il comportamento previsto è il seguente:

- Èpossibile scegliere l'azione SIG come azione strict predefinita o **fallback-to-routing**.
- Il comportamento predefinito è **rigoroso**. Se i tunnel SIG sono inattivi, il traffico viene interrotto.
- Se il **fallback-to-routing** è abilitato, Se i tunnel SIG sono attivi, il traffico viene inviato tramite SIG.Se i tunnel SIG sono inattivi, il traffico NON viene interrotto. Il traffico viene indirizzato normalmente. **Nota**: il routing potrebbe avvenire anche tramite NAT DIA, se l'utente ha sia il percorso SIG (tramite configurazione o azione criterio) sia il percorso NAT DIA configurato (percorso ip nat globale vrf 1 0.0.0.0 0.0.0) e se il tunnel non funziona, il routing punterà a NAT DIA. Per motivi di sicurezza (ossia tutto il traffico può passare attraverso la sovrimpressione o il SIG, ma non attraverso DIA), NAT DIA DEVE essere non configurato.Se il tunnel SIG diventa attivo, solo i nuovi flussi vengono inviati tramite SIG. Tutti i flussi di corrente non saranno sottoposti all'azione SIG.Se il tunnel SIG è guasto, tutto il traffico passa attraverso il routing, sia per i flussi correnti che per i nuovi flussi. **Nota**:i flussi correnti passano al tunnel SIG prima e passano al routing per interrompere la sessione end-to-end. I nuovi flussi vengono sottoposti a routing

Configurazione

Criterio vSmart

Criterio dati

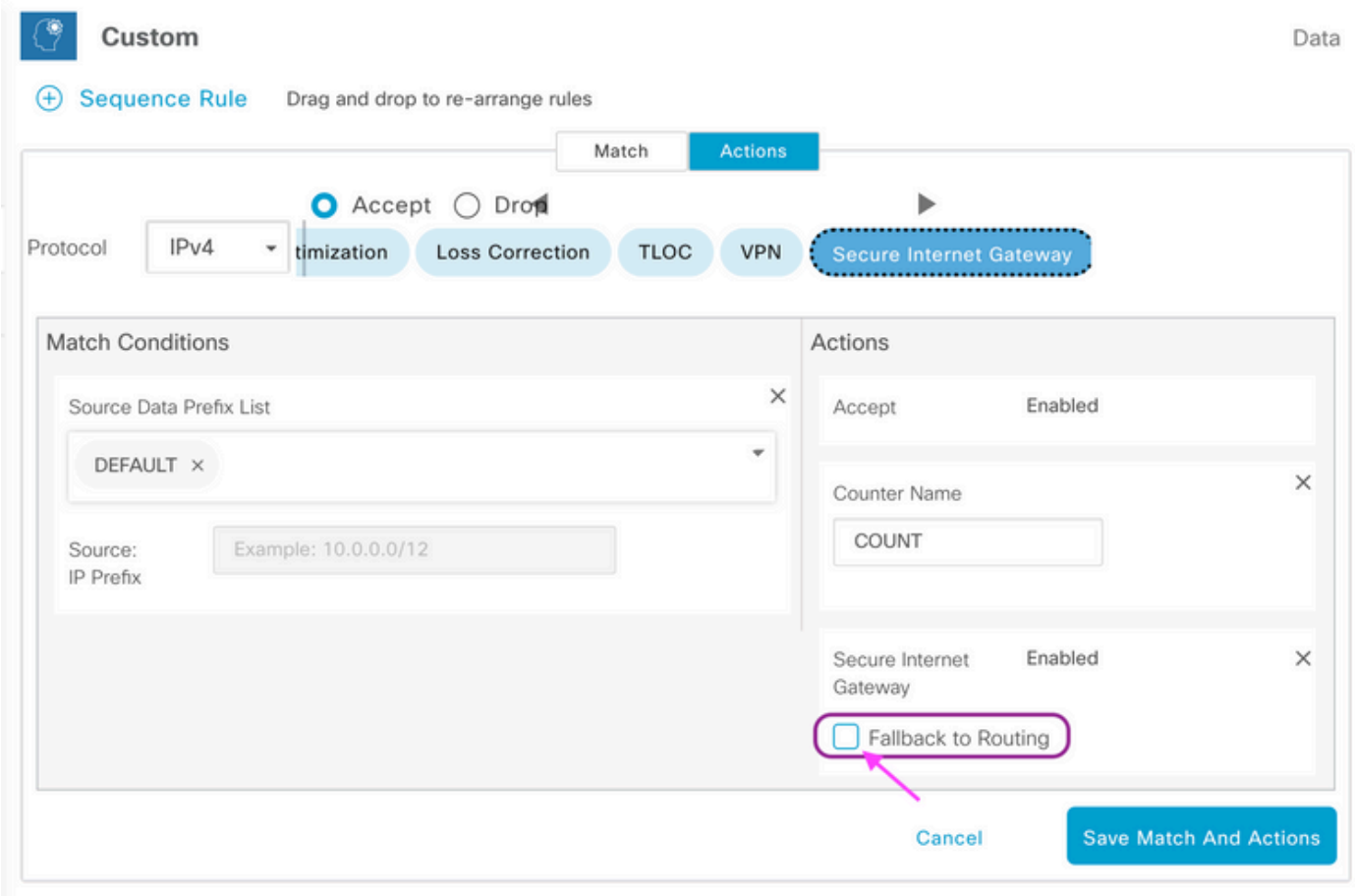
```
vSmart-1# show running-config policy
policy
 data-policy _VPN10_sig-default-fallback-to-routing
  vpn-list VPN10
   sequence 1
    match
     source-data-prefix-list Default
    !
    action accept
     count Count_26488854
     sig
```

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 ! ! !

Applica criterio

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

Quando si usa Policy Builder per il criterio vSmart, selezionare la casella di controllo **Fallback to Routing** per instradare il traffico in Internet attraverso la sovrapposizione Cisco SD-WAN quando tutti i tunnel SIG sono inattivi.



Quando l'azione **Fallback to Routing** è selezionata sull'interfaccia utente, le azioni **fallback to-**

routing e **sig** vengono aggiunte alla configurazione in *azione accetta.*

Verifica su cEdge

Policy

```
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
```

Conferma

Confermare che il traffico sia indirizzato con l'uso del comando **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#
```

Per verificare il percorso previsto del traffico, usare il 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
```

Verifica contatori criteri dati

Per prima cosa, cancellare i contatori con il comando **clear sdwan policy data-policy** per iniziare da 0. È possibile verificare che il contatore sia stato generato con il 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
```

Usare il comando **ping** per inviare alcuni pacchetti che si prevede di indirizzare tramite il tunnel 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#
```

Verificare che i pacchetti ICMP corrispondano alla sequenza di criteri specificata con il 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
```

Traccia pacchetto

Configurare una traccia dei pacchetti per comprendere cosa succede ai pacchetti con il 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)
```

Pacchetto 12

Un frammento di codice dal pacchetto 12 mostra la sequenza di traffico 1 nel criterio dei dati e viene reindirizzato al 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 ricerca di input per l'interfaccia di output visualizza l'interfaccia tunnel (logica).

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

Dopo la crittografia IPSec, l'interfaccia di input viene popolata.

```
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
```

Il router esegue diverse altre azioni e quindi trasmette il pacchetto sull'interfaccia Gigabit Ethernet1.

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

Pacchetto 13

Il router riceve la risposta dall'indirizzo IP remoto (8.8.8.8), ma non è sicuro di chi inviarlo come indicato da **Output: <sconosciuto>** nell'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
```

Poiché il pacchetto viene generato internamente, viene consumato dal router e l'output viene visualizzato come **<internal0/0/rp:0>**.

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

Successivamente, il pacchetto viene indirizzato al processo Cisco IOSd, che registra le azioni eseguite sul pacchetto. L'indirizzo IP dell'interfaccia locale in VRF 10 è 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
```

Verifica del fallback al routing

Èpossibile simulare il failover con uno shutdown amministrativo sull'interfaccia TLOC (Transport Interface) (Gigabit Ethernet1), ovvero Biz-Internet. Ha la connessione a Internet.

Gigabit Ethernet2 - MPLS TLOC è attivo/attivo, ma non dispone di una connessione Internet. Lo stato del controllo può essere visualizzato nell'output **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
```

Dall'output **show ip interface brief**, l'interfaccia Gigabit Ethernet1 è disattivata a livello

amministrativo.

```
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
```

Il tunnel 100001 è in stato **UP/DOWN**.

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

Attualmente non è disponibile una connessione a Internet, pertanto la possibilità di raggiungere la versione 8.8.8.8 non è disponibile nella versione 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)

Il comando **show sdwan policy service-path** visualizza la route predefinita (da fallback a routing) di OMP per il collegamento al controller di dominio (centro dati).

L'indirizzo IP MPLS TLOC del router locale è 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
```

Su Umbrella Portal

Esempio di criteri dei dati di produzione

Esempio tipico di politica dei dati di produzione.

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

Corrisponde alle applicazioni Google da qualsiasi origine e torna al routing, se c'è un problema.

Informazioni correlate

Documentazione sulle policy Cisco IOS-XE SDWAN

Documentazione della funzione Cisco IOS-XE Datapath Packet Trace

Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).