Konfigurieren der Datenverkehrsumleitung zu SIG mithilfe der Datenrichtlinie: Fallback zu Routing

Inhalt

Einleitung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Hintergrund
Problemdefinition
Software-Architektur
Konfiguration
vSmart-Richtlinie
Auf cEdge überprüfen
Richtlinie
Bestätigen
Zähler für Datenrichtlinien überprüfen
Paketnachverfolgung
Paket 12
Paket 13
Überprüfen von Fallback-zu-Routing
Auf Umbrella Portal
Beispiel für eine Produktionsdatenrichtlinie
Zugehörige Informationen

Einleitung

In diesem Dokument wird beschrieben, wie Sie eine Datenrichtlinie konfigurieren, die bei einem Ausfall von SIG-Tunneln einen Fallback zum Routing zulässt.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse der SDWAN-Lösung (Software Defined Wide Area Network) von Cisco verfügen.

Bevor Sie eine Datenrichtlinie für die Umleitung von Anwendungsdatenverkehr auf ein SIG anwenden, müssen Sie SIG-Tunnel konfigurieren.

Verwendete Komponenten

Die Richtlinie in diesem Artikel wurde mit Softwareversion 20.9.1 und Cisco IOS-XE 17.9.1 getestet.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrund

Mit dieser Funktion können Sie festlegen, dass internetgebundener Datenverkehr als Fallback-Mechanismus über das Cisco SD-WAN-Overlay geleitet wird, wenn alle SIG-Tunnel ausgefallen sind.

Diese Funktion wurde in Cisco IOS XE 17.8.1a und Cisco vManage 20.8.1 eingeführt

Problemdefinition

Vor der Version 20.8 ist die SIG-Aktion in der Datenrichtlinie standardmäßig strikt. Wenn SIG-Tunnel ausfallen, wird der Datenverkehr verworfen.

Software-Architektur

Sie können eine zusätzliche Option wählen, nicht streng zu sein, und auf das Routing zurückgreifen, um Datenverkehr über das Overlay zu senden.

Routing kann zum Overlay oder anderen Weiterleitungspfaden wie NAT-DIA führen.

Insgesamt wird folgendes Verhalten erwartet:

- Sie können die SIG-Aktion wahlweise als "strict" oder "**Fallback-to-Routing**" auswählen.
- Das Standardverhalten ist **strikt**. Wenn SIG-Tunnel ausfallen, wird der Datenverkehr verworfen.
- Wenn **Fallback-to-Routing** aktiviert ist, Wenn die SIG-Tunnel aktiv sind, wird der Datenverkehr über SIG gesendet.Wenn die SIG-Tunnel AUSFALLEN, wird der Datenverkehr NICHT verworfen. Der Datenverkehr wird einer normalen Weiterleitung unterzogen. **Hinweis:** Routing kann auch über NAT DIA erfolgen, wenn für den Benutzer sowohl SIG-Route (über die Konfiguration oder über eine Richtlinienaktion) als auch NAT DIA konfiguriert sind (ip nat route vrf 1 0.0.0.0 0.0.0.0 global) und wenn der Tunnel ausfällt, würde das Routing auf NAT DIA verweisen. Wenn Sie sich mit der Sicherheit befassen (d. h. der gesamte Datenverkehr kann entweder über Overlay oder SIG erfolgen, jedoch nicht über DIA), DARF NAT DIA nicht konfiguriert werden.Wenn der SIG-Tunnel aktiviert wird, werden nur neue Datenflüsse über SIG gesendet. Die SIG-Aktion wird für alle aktuellen Datenflüsse nicht durchgeführt.Wenn der SIG-Tunnel zu DOWN wird, erfolgt der gesamte Datenverkehr über Routing, sowohl der aktuelle Datenfluss als auch der neue Datenfluss. **Hinweis**: Der aktuelle Datenfluss verläuft über den SIG-Tunnel, bevor er aktiviert wurde. Wird auf Routing umgeschaltet, kann die End-to-End-Sitzung unterbrochen werden. Neue Datenflüsse werden weitergeleitet

Konfiguration

vSmart-Richtlinie

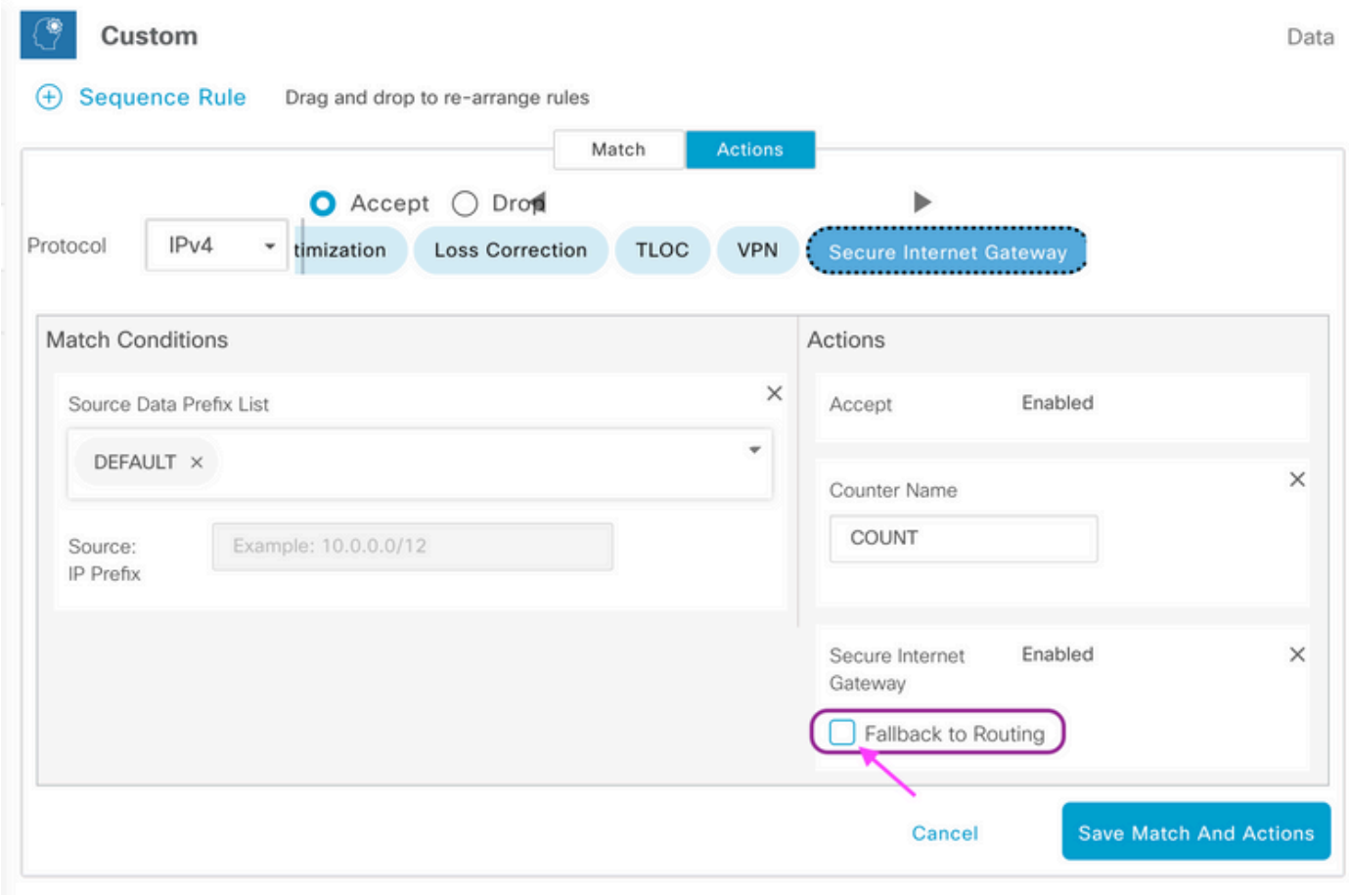
Datenrichtlinie

```
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 ! ! !
```

Richtlinie anwenden

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

Wenn der Policy Builder für die vSmart-Richtlinie verwendet wird, aktivieren Sie das Kontrollkästchen **Fallback to Routing (Fallback an Routing),** um den Internetdatenverkehr über das Cisco SD-WAN-Overlay weiterzuleiten, wenn alle SIG-Tunnel ausgefallen sind.



Wenn **die** Aktion **"Fallback to Routing"** auf der Benutzeroberfläche ausgewählt ist, werden **Fallback to Routing** und **sig-action** der Konfiguration unter "*Action accept" (Aktion annehmen) hinzugefügt.*

Auf cEdge überprüfen

Richtlinie

```
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
```

Bestätigen

Vergewissern Sie sich mit dem **Ping**-Befehl, dass der Datenverkehr weitergeleitet wird.

```
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#
```

Mit dem Befehl **show sdwan policy service-path** können Sie den Pfad überprüfen, den der

Datenverkehr voraussichtlich einnehmen wird.

```
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
```

Zähler für Datenrichtlinien überprüfen

Löschen Sie zunächst die Zähler mit dem Befehl **clear sdwan policy data-policy**, um bei 0 zu beginnen. Mit dem Befehl **show sdwan policy data-policy-filter** können Sie überprüfen, ob der Zähler **angezeigt wurde**.

```
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
```

Verwenden Sie **ping**, um einige Pakete zu senden, die Sie über den SIG-Tunnel weiterleiten möchten.

```
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#
```

Überprüfen Sie mit dem Befehl **show sdwan policy data-policy-filter, ob** die ICMP-Pakete Ihre Datenrichtliniensequenz erreicht haben.

```
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
```

Paketnachverfolgung

Richten Sie eine Paketverfolgung ein, um zu ermitteln, was mit den Paketen mit dem Router passiert.

```
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)
```

Paket 12

Ein Ausschnitt aus Paket 12 zeigt die Traffic-Treffersequenz 1 in der Datenrichtlinie und wird an SIG umgeleitet.

```
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
```

Die Eingabesuche für die Ausgabeschnittstelle zeigt die Tunnelschnittstelle (logisch) an.

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

Nach der IPSec-Verschlüsselung wird die Eingangsschnittstelle ausgefüllt.

```
  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
```

Der Router ergreift eine Reihe weiterer Aktionen und überträgt das Paket dann über die GigabitEthernet1-Schnittstelle.

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

Paket 13

Der Router empfängt die Antwort von Remote IP (8.8.8.8), ist sich jedoch nicht sicher, wer sie senden soll, wie in der Ausgabe **Output: <unknown>** angegeben.

```
  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
```

Da das Paket intern generiert wird, wird es vom Router verbraucht, und die Ausgabe wird als **<internal0/0/rp:0>** angezeigt.

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

Danach wird das Paket an den Cisco IOSd-Prozess gesendet, der die Aktionen aufzeichnet, die auf dem Paket ausgeführt werden. Die IP-Adresse der lokalen Schnittstelle in VRF 10 lautet 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
```

Überprüfen von Fallback-zu-Routing

Sie können das Failover simulieren, indem Sie die Transportschnittstelle (TLOC) (GigabitEthernet1), die Biz-Internet ist, herunterfahren. Es hat einen Internetanschluss.

GigabitEthernet2 - MPLS-TLOC ist aktiv/aktiv, hat aber keine Internetverbindung. Der Status des Steuerelements wird in der Ausgabe **show sdwan control local-properties wan-interface-list** angezeigt.

```
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
```

In der Ausgabe von **show ip interface brief** wird die GigabitEthernet1-Schnittstelle administrativ deaktiviert.

```
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 befindet sich im **UP/DOWN-**Status.

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

Es gibt keine Internetverbindung, daher ist die Erreichbarkeit von VRF 10 auf 8.8.8.8 nicht möglich.

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)

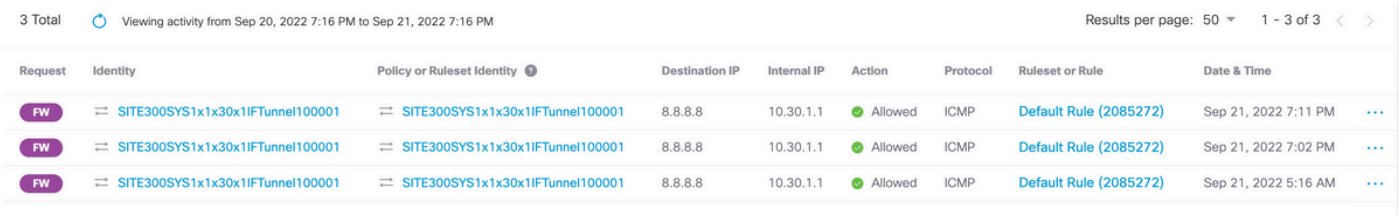
Der Befehl **show sdwan policy service-path** zeigt an, dass die OMP-Standardroute (Fallback-to-Routing) zum Rechenzentrum (Rechenzentrum) verwendet werden soll.

Die IP-Adresse des lokalen Routers mit MPLS-TLOC lautet 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
```

Auf Umbrella Portal



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

Beispiel für eine Produktionsdatenrichtlinie

Ein typisches Beispiel für eine Produktionsdatenrichtlinie.

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

Es vergleicht die Google-Apps von jeder Quelle und fällt zurück auf Routing, wenn es ein Problem gibt.

Zugehörige Informationen

[Dokumentation der Cisco IOS-XE SDWAN-Richtlinie]

[Dokumentation der Cisco IOS-XE DataPath Packet Trace-Funktion]

[Technischer Support und Dokumentation für Cisco Systeme]

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.