Configure Traffic Redirection to SIG with Data Policy: Fallback to Routing

Contents

Introduction

This document describes how to configure a data policy to allow traffic to fallback to routing when SIG tunnels fail.

Prerequisites

Requirements

Cisco recommends that you have knowledge of Cisco Software Defined Wide Area Network (SDWAN) solution.

Before you apply a data policy for redirection of application traffic to a SIG, you must configure SIG tunnels.

Components Used

The policy in this article was tested on software version 20.9.1 and 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. If your network is live, ensure that you understand the potential impact of any command.

Background

With this feature, you can configure internet-bound traffic to be routed through the Cisco SD-WAN overlay, as a fallback mechanism, when all SIG tunnels are down.

This feature is introduced in Cisco IOS XE Release 17.8.1a and Cisco vManage Release 20.8.1

Problem Definition

Prior to 20.8 version, the SIG action in the data-policy is strict by default.   If SIG tunnels are down, traffic is dropped.

Software Architecture

You can have an additional option to choose not to be strict and fallback to routing to send traffic over the overlay.

Routing could lead to the overlay or other forwarding paths like NAT-DIA.

In summary, the expected behavior be as:

- You have option to choose SIG action to be default strict or **fallback-to-routing**.
- Default behavior is **strict**. If SIG tunnels are down, traffic is dropped.
- If **fallback-to-routing** is enabled, If the SIG tunnels are UP, the traffic is sent over SIG.If the SIG tunnels are DOWN, the traffic is NOT dropped. The traffic undergoes normal routing. **Note**: Routing could be via NAT DIA as well, if the user has both SIG route (via configuration or via policy action) and NAT DIA configured (ip nat route vrf 1 0.0.0.0 0.0.0.0 global) and if the tunnel goes down, the routing would point to NAT DIA. If you are concerned with security (i.e all the traffic can either go via overlay or via SIG but not via DIA), then NAT DIA MUST not be configured.If the SIG tunnel becomes UP, only new flows are sent over SIG. Any current flows would not undergo the SIG action.If the SIG tunnel becomes DOWN, all traffic goes via routing, both any current flows and new flows. **Note**:Current flows goes on SIG tunnel before and switched to routing can break end-to-end session. New flows undergo routing

Configuration

vSmart Policy

Data Policy

```
vSmart-1# show running-config policy
policy
 data-policy _VPN10_sig-default-fallback-to-routing
```

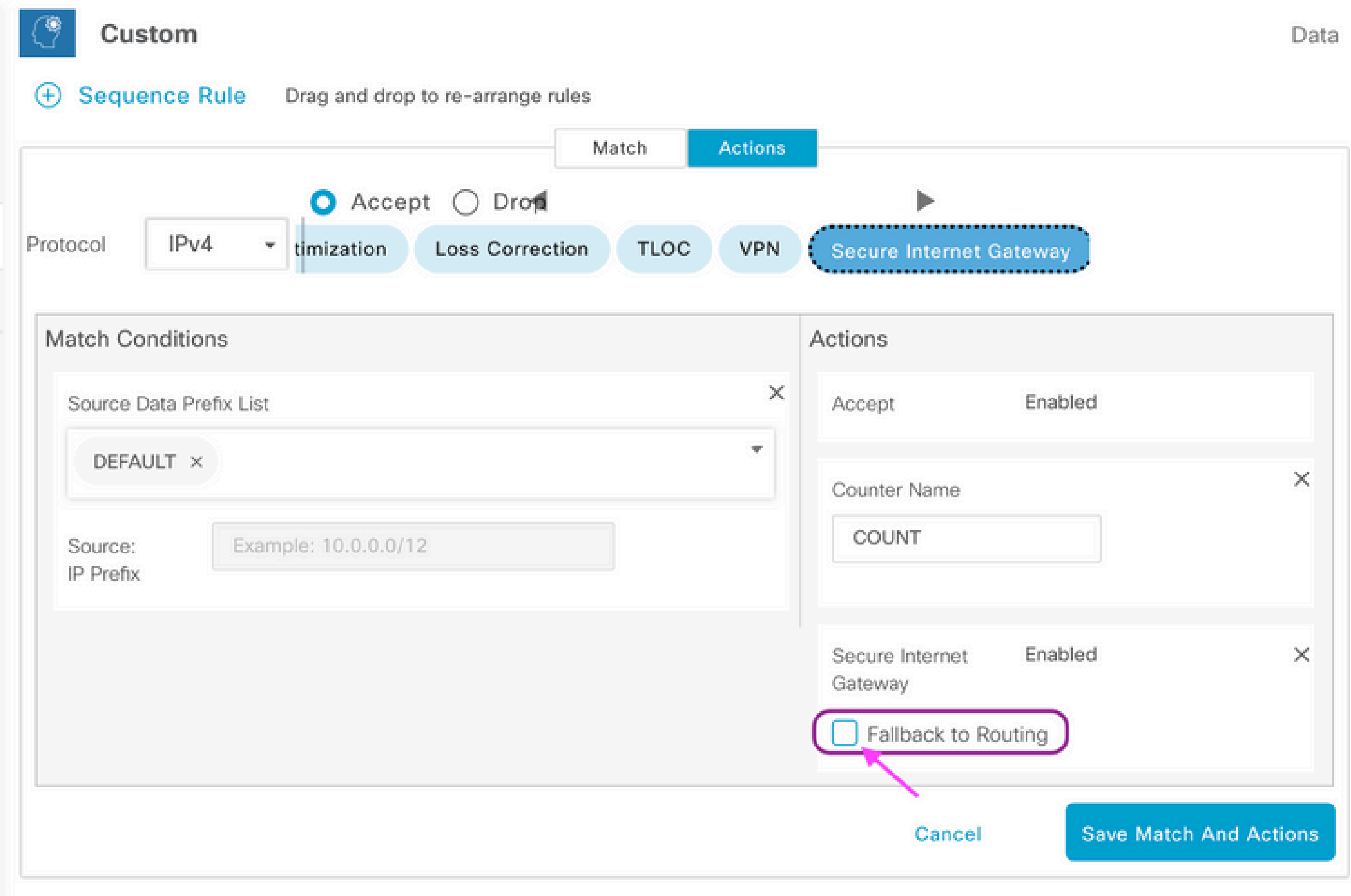
```
  vpn-list VPN10
   sequence 1
    match
     source-data-prefix-list Default
    !
    action accept
     count Count_26488854
     sig
```

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 ! ! !

Apply Policy

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

When the Policy Builder for the vSmart Policy is used, check the **Fallback to Routing** check box to route internet-bound traffic through the Cisco SD-WAN overlay when all SIG tunnels are down.



Source Data Prefix List: DEFAULT

Source: IP Prefix: Example: 10.0.0.0/12

Accept Enabled

Counter Name: COUNT

Secure Internet Gateway Enabled

□ Fallback to Routing

When **Fallback to Routing** action is selected on UI, **fallback-to-routing** and **sig-action** are added to the configuration under *action accept.*

Verify On 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
```

Confirm

Confirm that traffic is routing with the use of **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#
```

You can verify the path the traffic is expected to take with the **show sdwan policy service-path** command.

```
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
```

Check Data-Policy Counters

First, clear the counters with the command **clear sdwan policy data-policy** to start at 0. You can verify the counter was with the **show sdwan policy data-policy-filter** command.

```
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 **ping** to send a few packets that you expect to route via the SIG tunnel.

```
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#
```

Verify the ICMP packets hit your data policy sequence with the **show sdwan policy data-policy-filter** command.

```
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
```

Packet Trace

Set up a packet trace to understands what happens to the packets with the 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)
```

Packet 12

A snippet from packet 12 shows the traffic hit sequence 1 in the data policy and is redirected to 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
```

The Input lookup for the output interface shows the Tunnel Interface (Logical).

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

After the IPSec Encryption, the input interface is populated.

```
  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
```

The router takes a several other actions and then transmits the packet out on the GigabitEthernet1 interface.

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

Packet 13

The router receives the response from Remote IP (8.8.8.8), but is unsure who to send it so as indicated by **Output: <unknown>** in the 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
```

Since the packet is internally generated, it is consumed by the router, and the Output is shown as **<internal0/0/rp:0>**.

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

After this, the packet is punted to Cisco IOSd process, which records the actions take on the packet. The local interface ip address 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
```

Verify Fallback-to-Routing

You can simulate the failover with an administrative shutdown on the Transport Interface (TLOC) (GigabitEthernet1), which is Biz-Internet. It has the internet connection.

GigabitEthernet2 - MPLS TLOC is UP/UP, but has no internet connection. The control status can be seen in the **show sdwan control local-properties wan-interface-list** output.

```
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
```

From the **show ip interface brief** output, the GigabitEthernet1 interface shows administratively down.

```
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 an **UP/DOWN** state.

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

There is no internet connection now, so reachability to 8.8.8.8 fails from 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)
```

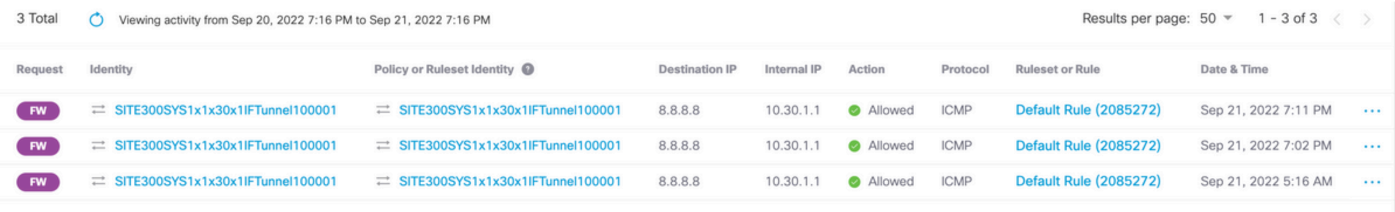
The **show sdwan policy service-path** command shows that the OMP default-route (fallback-to-routing) to go to the DC (data center) is expected to be taken.

The local router MPLS TLOC IP address 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
```

On 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

Example Production Data Policy

A typical production data policy example.

```
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
```

It matches the Google Apps from any source and falls back to routing, if there is an issue.

Related Information

[Cisco IOS-XE SDWAN Policy Documentation]

[Cisco IOS-XE Datapath Packet Trace Feature Documentation]

[Technical Support & Documentation - Cisco Systems]