

Solucionar problemas de conexiones del plano de datos y detección de reenvío bidireccional de vEdge

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Información del plano de control](#)

[Comprobar propiedades locales del control](#)

[Comprobar conexiones de control](#)

[Protocolo de administración de superposición](#)

[Verificar que los OMP TLOC se anuncian desde vEdges](#)

[Verificar que vSmart recibe y anuncia los TLOC](#)

[Bidireccional Forwarding Detection](#)

[Comprender el comando show bfd sessions](#)

[Comando show tunnel statistics](#)

[Lista de acceso](#)

[Traducción de direcciones de red](#)

[Cómo Utilizar las Herramientas stun-client para Detectar Mapas y Filtros NAT.](#)

[Tipos de NAT compatibles para túneles de plano de datos"Enviando" utilizados en CLI](#)

[Firewalls](#)

[Security](#)

[Problemas del ISP con el tráfico marcado DSCP](#)

[Debug BFD](#)

[Utilizar Packet-Trace para capturar paquetes BFD \(20.5 y posteriores\)](#)

[Información Relacionada](#)

Introducción

Este documento describe los problemas de conexión del plano de datos de vEdge después de una conexión del plano de control; sin embargo, no hay conectividad del plano de datos entre sitios.

Prerequisites

Requirements

Cisco recomienda conocer la **Cisco Software Defined Wide Area Network (SDWAN)** solución.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware. Este documento se centra en las plataformas vEdge.

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.

Para los routers Cisco Edge (routers Cisco IOS® XE en modo de controlador) , lea .

Información del plano de control

Comprobar propiedades locales del control

Para verificar el estado de las **Wide Area Network (WAN)** interfaces en un vEdge, utilice el comando, **show control local-properties wan-interface-list**.

En esta salida, puede ver el RFC 4787 **Network Address Translation (NAT) Type**.

Cuando vEdge está detrás de un dispositivo NAT (firewall, router, etc.), se utilizan direcciones IPv4 públicas y privadas, **User Datagram Protocol (UDP)** puertos de origen públicos y privados para crear los túneles del plano de datos.

También puede encontrar el estado de la interfaz de túnel, el color y el número máximo de conexiones de control configuradas.

```
vEdge1# show control local-properties wan-interface-list NAT TYPE: E -- indicates End-point independent mapping A -- indicates Address-port dependent
```

Con estos datos, puede identificar cierta información sobre cómo se deben construir los túneles de datos y qué puertos puede esperar (desde la perspectiva de los routers) utilizar cuando forme los túneles de datos.

Comprobar conexiones de control

Es importante asegurarse de que el color que no forma los túneles del plano de datos tenga una conexión de control establecida con los controladores en la superposición.

De lo contrario, el vEdge no envía la **Transport Locator (TLOC)** información al vSmart a través de **Overlay Management Protocol (OMP)**.

Puede comprobar si está operativo con el uso del **show control connections** comando y buscar el **connect** estado.


```
vEdge1# show control connections PEER PEER CONTROLLER PEER PEER PEER SITE DOMAIN PEER PRIV PEER PUB GROUP TYPE PROT SY
```

Si la interfaz (que no forma túneles de datos) intenta conectarse, solúcelo con un inicio exitoso de las conexiones de control a través de ese

color.

O bien, establezca el **max-control-connections 0** en la interfaz seleccionada en la sección de interfaz de túnel.

```
vpn 0 interface ge0/1 ip address 10.20.67.10/24 tunnel-interface encapsulation ipsec color mpls restrict max-control-connections 0 no allow-service bgp all
```

 **Nota:** A veces, puede utilizar el **no control-connections** comando para lograr el mismo objetivo. Sin embargo, ese comando no establece un número máximo de conexiones de control. Este comando está obsoleto desde la versión 15.4 y no se utiliza en software más reciente.

Protocolo de administración de superposición

Verificar que los OMP TLOC se anuncian desde vEdges

No se pueden enviar las TLOC de OMP porque la interfaz intenta formar conexiones de control a través de ese color y no puede alcanzar los controladores.

Compruebe si el color (que los túneles de datos) envía el TLOC para ese color en particular a la vsmarts.


Utilice el comando para verificar **show omp tlocs advertised** los TLOC que se envían a los pares OMP.

Ejemplo: Colores **mpls** y **gold**. No se envía TLOC a vSmart para mpls de color.

```
vEdge1# show omp tlocs advertised C -> chosen I -> installed Red -> redistributed Rej -> rejected L -> looped R -> resolved S -> stale Ext -> extranet Stg
```

Ejemplo: Colores **mpls** y **gold**. Se envía TLOC para ambos colores.

```
vEdge2# show omp tlocs advertised C -> chosen I -> installed Red -> redistributed Rej -> rejected L -> looped R -> resolved S -> stale Ext -> extranet Stg
```

 **Nota:** Para cualquier información del plano de control generado localmente, el campo "**FROM PEER**" se establece en 0.0.0.0. Cuando busque información originada localmente, asegúrese de que coincide según este valor.

Verificar que vSmart recibe y anuncia los TLOC

Los TLOC se anuncian ahora a vSmart. Confirme que recibe las TLOC del par correcto y las anuncia al otro vEdge.

Ejemplo: vSmart recibe las TLOC de 10.1.0.2 vEdge1.

<#root>

vSmart1# show omp tlocs received

C -> chosen I -> installed

Red -> redistributed Rej -> rejected L -> looped

R -> resolved

S -> stale Ext -> extranet Stg -> staged Inv -> invalid PUBLIC PRIVATE ADDRESS PSEUDO PUBLIC PRIVATE P

10.1.0.2 mpls ipsec 10.1.0.2 C,I,R 1 10.20.67.20 12386 10.20.67.20 12386 :: 0 :: 0 -

10.1.0.2 blue ipsec 10.1.0.2 C,I,R 1 198.51.100.187 12406 10.19.146.2 12406 :: 0 :: 0 -

10.1.0.30 mpls ipsec 10.1.0.30 C,I,R 1 10.20.67.30 12346 10.20.67.30 12346 :: 0 :: 0 - 10.1.0.30 gold

Si no ve los TLOC o si ve cualquier otro código aquí, compruebe lo siguiente:

<#root>

vSmart-vIPtela-MEX# show omp tlocs received

C -> chosen

I -> installed

Red -> redistributed

Rej -> rejected

L -> looped

R -> resolved

S -> stale Ext -> extranet Stg -> staged

Inv -> invalid

PUBLIC PRIVATE ADDRESS PSEUDO PUBLIC PRIVATE PUBLIC IPV6 PRIVATE IPV6 BFD FAMILY TLOC IP COLOR ENCAP F

10.1.0.2 mpls ipsec 10.1.0.2 C,I,R 1 10.20.67.20 12386 10.20.67.20 12386 :: 0 :: 0 -

10.1.0.2 blue ipsec 10.1.0.2 Rej,R,Inv 1 198.51.100.187 12406 10.19.146.2 12406 :: 0 :: 0 -

10.1.0.30 mpls ipsec 10.1.0.30 C,I,R 1 10.20.67.30 12346 10.20.67.30 12346 :: 0 :: 0 - 10.1.0.30 gold

Verifique que no haya ninguna política que bloquee los TLOC.

show run policy control-policy - busque cualquier lista tloc que rechace sus TLOC como **advertised** o **received** en vSmart.

<#root>

```
vSmart1(config-policy)# sh config policy lists tloc-list SITE20
```

```
tloc 10.1.0.2 color blue encap ipsec
```

```
!! control-policy SDWAN
```

```
sequence 10 match tloc tloc-list SITE20 ! action reject ---->
```

here we are rejecting the TLOC 10.1.0.2,blue,ipsec !! default-action accept !

```
apply-policy
```

```
site-list SITE20
```

```
control-policy SDWAN in ----->
```

the policy is applied to control traffic coming IN the vSmart, it will filter the tlocs before adding i



Nota: Si un TLOC es **Rejected** o **Invalid**, no se anuncia a los otros vEdges.

Asegúrese de que una política no filtre el TLOC cuando se anuncie desde vSmart. Puede ver que el TLOC se recibe en el vSmart, pero no lo ve en el otro vEdge.

Ejemplo 1: vSmart con TLOC en C,I,R.

```
<#root>
```

```
vSmart1# show omp tlocs
```

```
C -> chosen I -> installed
```

```
Red -> redistributed Rej -> rejected L -> looped
```

```
R -> resolved
```

```
S -> stale Ext -> extranet Stg -> staged Inv -> invalid PUBLIC PRIVATE ADDRESS PSEUDO PUBLIC PRIVATE P
```

```
10.1.0.2 mpls ipsec 10.1.0.2 C,I,R 1 10.20.67.20 12386 10.20.67.20 12386 :: 0 :: 0 - 10.1.0.2 blue ipse
```

```
10.1.0.30 mpls ipsec 10.1.0.30 C,I,R 1 10.20.67.30 12346 10.20.67.30 12346 :: 0 :: 0 - 10.1.0.30 gold
```

Ejemplo 2: vEdge1 no ve el TLOC del color azul que viene de vEdge2. Solo ve MPLS TLOC.

```
<#root>
```

```
vEdge1# show omp tlocs C -> chosen I -> installed Red -> redistributed Rej -> rejected L -> looped R -> resolved S -> stale Ext -> extranet Stg -> staged I
```

```
10.1.0.2 mpls ipsec 10.1.0.3 C,I,R 1 10.20.67.20 12386 10.20.67.20 12386 :: 0 :: 0 up
```

```
10.1.0.30 mpls ipsec 10.1.0.3 C,I,R 1 10.20.67.30 12346 10.20.67.30 12346 :: 0 :: 0 up 10.1.0.30 gold
```

Al comprobar la directiva, puede ver por qué TLOC no aparece en vEdge1.

```
<#root>
```

```
vSmart1# show running-config policy policy lists tloc-list SITE20
```

```
tloc 10.1.0.2 color blue encap ipsec
! site-list SITE10 site-id 10 !! control-policy SDWAN sequence 10 match tloc
tloc-list SITE20
! action reject !! default-action accept !
apply-policy
site-list SITE10
control-policy SDWAN out
!
!
```

Bidirectional Forwarding Detection

Comprender el comando [show bfd sessions](#)

Estos son los aspectos clave que se deben buscar en el resultado:

<#root>

```
vEdge-2# show bfd sessions SOURCE TLOC REMOTE TLOC DST PUBLIC DST PUBLIC DETECT TX SYSTEM IP SITE ID STATE COLOR COLOR
10.1.0.5 10 down blue gold 10.19.146.2 203.0.113.225 4501 ipsec 7 1000 NA 7
10.1.0.30 30 up blue gold 10.19.146.2 192.0.2.129 12386 ipsec 7 1000 0:00:00:22 2 10.1.0.4 40 up blue
10.1.0.4 40 up mpls mpls 10.20.67.10
```

- **SYSTEM IP:** Peers system-ip
- **SOURCE and REMOTE TLOC COLOR:** Esto es útil para saber qué se espera que reciba y envíe el TLOC.
- **SOURCE IP:** es la IP de **private** origen. Si está detrás de una NAT, esta información se muestra aquí (se puede ver con el uso de **show control local-properties <wan-interface-list>**).
- **DST PUBLIC IP:** es el destino que utiliza el vEdge para formar el **Data Plane** túnel, esté o no detrás de NAT. (Ejemplo: vEdges conectado directamente a Internet o **Multi-Protocol Label Switching (MPLS)** enlaces)
- **DST PUBLIC PORT** Puerto NAT-ed público que utiliza vEdge para formar el **Data Plane** túnel al vEdge remoto.
- **TRANSITIONS:** número de veces que la sesión BFD ha cambiado su estado, de **NA** a **UP** y viceversa.

Comando show tunnel statistics

El **show tunnel statistics** puede mostrar información sobre los túneles del plano de datos. Puede determinar si envía o recibe paquetes para un túnel IPSEC determinado entre los vEdges.

Esto puede ayudarle a entender si los paquetes llegan a cada extremo y a aislar los problemas de conectividad entre los nodos.

En el ejemplo, cuando ejecuta el comando varias veces, puede observar un incremento o ningún incremento en el **tx-pkts** o **rx-pkts**.



Sugerencia: Si su contador para el incremento tx-pkts, transmite datos hacia el peer. Si su rx-pkts no aumenta, significa que no se reciben datos de su par. En este caso, verifique el otro extremo y confirme si el tx-pkts aumenta.

<#root>

```
TCP vEdge2# show tunnel statistics
```

```
TUNNEL SOURCE DEST TUNNEL MSS PROTOCOL SOURCE IP DEST IP PORT PORT SYSTEM IP LOCAL COLOR REMOTE COLOR MTU tx-
ipsec 172.16.16.147 10.88.244.181 12386 12406 10.1.0.5 public-internet default 1441 38282 5904968 38276
ipsec 172.16.16.147 10.152.201.104 12386 63364 10.1.0.0 public-internet default 1441 33421 5158814 334
```

TUNNEL PROTOCOL	SOURCE IP	DEST IP	SOURCE PORT	DEST PORT	SYSTEM IP	LOCAL COLOR	REMOTE COLOR	MTU
ipsec	172.16.16.147	10.88.244.181	12386	12406	10.1.0.5	public-internet	default	38276
ipsec	172.16.16.147	10.152.201.104	12386	63364	10.1.0.0	public-internet	default	33421
ipsec	172.16.16.147	10.152.204.31	12386	58851	10.1.0.7	public-internet	public-internet	38276
ipsec	172.24.90.129	10.88.244.181	12426	12406	10.1.0.5	biz-internet	default	38276
ipsec	172.24.90.129	10.152.201.104	12426	63364	10.1.0.0	biz-internet	default	33421
ipsec	172.24.90.129	10.152.204.31	12426	58851	10.1.0.7	biz-internet	public-internet	38276

Otro comando útil es **show tunnel statistics bfd** que se puede utilizar para verificar el número de paquetes BFD enviados y recibidos dentro de un túnel de plano de datos determinado:

```
vEdge1# show tunnel statistics bfd BFD BFD BFD BFD BFD BFD PMTU PMTU PMTU PMTU TUNNEL SOURCE DEST ECHO TX ECHO RX BFD
```

Lista de acceso

Una lista de acceso es un paso útil y necesario después de ver el **show bfd sessions** resultado.

Ahora que se conocen las IP y los puertos privados y públicos, puede crear una **Access Control List (ACL)** para que coincida con SRC_PORT, DST_PORT, SRC_IP, DST_IP.

Esto puede ayudar a verificar los mensajes BFD enviados y recibidos.

Aquí, puede encontrar un ejemplo de una configuración ACL:

```
policy access-list checkbfd-out sequence 10 match source-ip 192.168.0.92/32 destination-ip 198.51.100.187/32 source-port 12426 destination-port 12426 !
default-action accept
!
access-list checkbfd-in sequence 20 match source-ip 198.51.100.187/32 destination-ip 192.168.0.92/32 source-port 12426 destination-port 12426 ! action a
vpn 0
interface ge0/0
access-list checkbfd-in in
access-list checkbfd-out out
!
!
!
```

En el ejemplo, esta ACL utiliza dos secuencias. La secuencia 10 coincide con los mensajes BFD que se envían desde este vEdge al par. La secuencia 20 hace lo contrario.

Coincide con los puertos de origen (**Private**) y de destino (**Public**). Si vEdge utiliza NAT, asegúrese de verificar los puertos de origen y destino correctos.

Para comprobar los resultados de cada contador de secuencia, ejecute el comando **show policy access-list counters <access-list name>**

```
vEdge1# show policy access-list-counters NAME COUNTER NAME PACKETS BYTES ----- checkbfd bfd-out-to
```

Traducción de direcciones de red

Cómo Utilizar las Herramientas stun-client para Detectar Mapas y Filtros NAT.

Si ha realizado todos los pasos y está detrás de NAT, el siguiente paso es identificar el **UDP NAT Traversal (RFC 4787) Map and Filter** comportamiento.

Esta herramienta se utiliza para detectar la dirección IP externa de vEdge local cuando vEdge se encuentra detrás de un dispositivo NAT.

Este comando obtiene un mapeo de puertos para el dispositivo y, opcionalmente, descubre propiedades sobre la NAT entre el dispositivo local y un servidor (servidor público: ejemplo de google stun server).



Nota: Para obtener más información, visite: [Docs Viptela - STUN Client](#)

<#root>


```

vEdge1# tools stun-client vpn 0 options "--mode full --localaddr 192.168.12.100 12386 --verbosity 2 stun
stunclient --mode full --localaddr 192.168.12.100 stun.l.google.com in VPN 0 Binding test: success
Local address: 192.168.12.100:12386
Mapped address: 203.0.113.225:4501
Behavior test: success

Nat behavior: Address Dependent Mapping

Filtering test: success

Nat filtering: Address and Port Dependent Filtering

```

En las versiones más recientes del software, la sintaxis puede ser un poco diferente:

<#root>


```

vEdge1# tools stun-client vpn 0 options "--mode full --localaddr 192.168.12.100 --localport 12386 --verb

```

En este ejemplo, se realiza una prueba de detección NAT completa con el uso del puerto de origen UDP 12386 al servidor STUN de Google.

La salida de este comando le proporciona el comportamiento NAT y el tipo de filtro NAT basado en RFC 4787.

 **Nota:** Cuando utilice **tools stun**, recuerde permitir el servicio STUN en la interfaz de túnel; de lo contrario, no funcionará. Utilícelo para permitir **allow-service stun** el paso de los datos stun.

<#root>

```

vEdge1# show running-config vpn 0 interface ge0/0 vpn 0 interface ge0/0 ip address 10.19.145.2/30 ! tunnel-interface encapsulation ipsec color gold max-
allow-service stun

! no shutdown ! !

```

Muestra la asignación entre la terminología STUN (NAT de cono completo) y RFC 4787 (comportamiento de NAT para UDP).

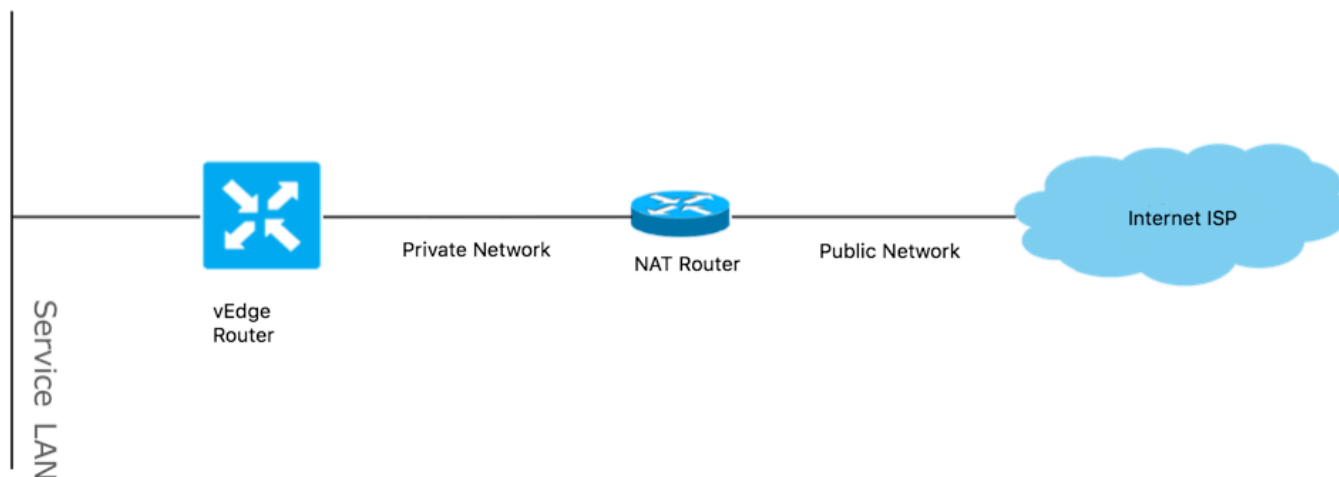
NAT Traversal Mapping Between used Viptela Terminologies		
STUN RFC 3489 Terminology	RFC 4787 Terminology	
	Mapping Behavior	Filtering Behavior
Full-cone NAT	Endpoint-Independent Mapping	Endpoint-Independent Filtering
Restricted Cone NAT	Endpoint-Independent Mapping	Address-Dependent Filtering
Port-Restricted Cone NAT	Endpoint-Independent Mapping	Address and Port-Dependent Filtering
Symmetric NAT	Address-and(or) Port-Dependent Mapping	Address-Dependent Filtering
		Address and Port-Dependent Filtering

Tipos de NAT compatibles para túneles de plano de datos "Enviando" utilizados en CLI

En la mayoría de los casos, los colores públicos como Internet de banda ancha o Internet público se pueden conectar directamente a Internet.

En otros casos, hay un dispositivo NAT detrás de la interfaz WAN de vEdge y el proveedor de servicios de Internet real.

De este modo, vEdge puede tener una IP privada y el otro dispositivo (router, firewall, etc.) puede ser el dispositivo con las direcciones IP públicas.



Si tiene un tipo de NAT incorrecto, podría ser una de las razones más comunes que no permiten la formación de túneles del plano de datos. Estos son los tipos de NAT soportados.

NAT Traversal Support		
Source	Destination	Supported (YES/NO)
Full-Cone NAT	Full-cone NAT	Yes
Full-Cone NAT	Restricted Cone NAT	Yes
Full-Cone NAT	Port-Restricted Cone NAT	Yes
Full-Cone NAT	Symmetric NAT	Yes
Restricted Cone NAT	Full-cone NAT	Yes
Restricted Cone NAT	Restricted Cone NAT	Yes
Restricted Cone NAT	Port-Restricted Cone NAT	Yes
Restricted Cone NAT	Symmetric NAT	Yes
Port-Restricted Cone NAT	Full-cone NAT	Yes
Port-Restricted Cone NAT	Restricted Cone NAT	Yes
Port-Restricted Cone NAT	Port-Restricted Cone NAT	Yes
Port-Restricted Cone NAT	Symmetric NAT	No
Symmetric NAT	Full-cone NAT	Yes
Symmetric NAT	Restricted Cone NAT	yes
Symmetric NAT	Port-Restricted Cone NAT	No
Symmetric NAT	Symmetric NAT	No

Firewalls

Si ya verificó la NAT y no está en los tipos de **origen** y **destino** no admitidos, es posible que un firewall bloquee los puertos utilizados para formar los **Data Plane** túneles.

Asegúrese de que estos puertos estén abiertos en el firewall para las conexiones del plano de datos: **vEdge to vEdge Data Plane**:

UDP 12346 a 13156

Para conexiones de control desde vEdge a controladores:

UDP 12346 a 13156

TCP 23456 a 24156

Asegúrese de abrir estos puertos para lograr una conexión exitosa de los túneles del plano de datos.

Al comprobar los puertos de origen y destino utilizados para los túneles del plano de datos, puede utilizar **show tunnel statistics** o **show bfd sessions | tab** pero no **show bfd sessions**.

No muestra ningún puerto de origen, sólo puertos de destino, como puede ver:

```
vEdge1# show bfd sessions SOURCE TLOC REMOTE TLOC DST PUBLIC DST PUBLIC DETECT TX SYSTEM IP SITE ID STATE COLOR COLOR
```



Nota: Para obtener más información sobre los puertos de firewall SD-WAN utilizados, [haga clic aquí](#).

Security

Si observa que el contador ACL aumenta el tráfico entrante y saliente, verifique varias iteraciones **show system statistics diff** and ensure there are no drops.

<#root>

```
vEdge1# show policy access-list-counters NAME COUNTER NAME PACKETS BYTES -----
```

```
checkbfd bfd-out-to-dc1-from-br1 55 9405
```

```
bfd-in-from-dc1-to-br1 54 8478
```

En este resultado, **rx_replay_integrity_drops** aumentar con cada iteración de la **show system statistics diff** command.

<#root>

```
vEdge1#show system statistics diff
```

```
rx_pkts : 5741427
```

```
ip_fwd : 5952166
```

```
ip_fwd_arp : 3
```

```
ip_fwd_to_egress : 2965437
```

ip_fwd_null_mcast_group : 26
ip_fwd_null_nhop : 86846
ip_fwd_to_cpu : 1413393
ip_fwd_from_cpu_non_local : 15
ip_fwd_rx_ipsec : 1586149
ip_fwd_mcast_pkts : 26
rx_bcast : 23957
rx_mcast : 304
rx_mcast_link_local : 240
rx_implicit_acl_drops : 12832
rx_ipsec_decap : 21
rx_spi_ipsec_drops : 16

rx_replay_integrity_drops : 1586035

port_disabled_rx : 2
rx_invalid_qtags : 212700
rx_non_ip_drops : 1038073
pko_wred_drops : 3
bfd_tx_record_changed : 23
rx_arp_non_local_drops : 19893
rx_arp_reqs : 294
rx_arp_replies : 34330
arp_add_fail : 263
tx_pkts : 4565384
tx_mcast : 34406
port_disabled_tx : 3
tx_ipsec_pkts : 1553753
tx_ipsec_encap : 1553753
tx_pre_ipsec_pkts : 1553753
tx_pre_ipsec_encap : 1553753
tx_arp_replies : 377
tx_arp_reqs : 34337
tx_arp_req_fail : 2
bfd_tx_pkts : 1553675
bfd_rx_pkts : 21
bfd_tx_octets : 264373160
bfd_rx_octets : 3600
bfd_pmtu_tx_pkts : 78
bfd_pmtu_tx_octets : 53052
rx_icmp_echo_requests : 48
rx_icmp_network_unreach : 75465
rx_icmp_other_types : 47
tx_icmp_echo_requests : 49655
tx_icmp_echo_replies : 48
tx_icmp_network_unreach : 86849
tx_icmp_other_types : 7
vEdge1# show system statistics diff

rx_pkts : 151
ip_fwd : 157
ip_fwd_to_egress : 75
ip_fwd_null_nhop : 3
ip_fwd_to_cpu : 43
ip_fwd_rx_ipsec : 41
rx_bcast : 1

rx_replay_integrity_drops : 41

```
rx_invalid_qtags : 7
rx_non_ip_drops : 21
rx_arp_non_local_drops : 2
tx_pkts : 114
tx_ipsec_pkts : 40
tx_ipsec_encap : 40
tx_pre_ipsec_pkts : 40
tx_pre_ipsec_encap : 40
tx_arp_reqs : 1
bfd_tx_pkts : 40
bfd_tx_octets : 6800
tx_icmp_echo_requests : 1
vEdge1# show system statistics diff
```

```
rx_pkts : 126
ip_fwd : 125
ip_fwd_to_egress : 58
ip_fwd_null_nhop : 3
ip_fwd_to_cpu : 33
ip_fwd_rx_ipsec : 36
rx_bcast : 1
rx_implicit_acl_drops : 1
```

rx_replay_integrity_drops : 35

```
rx_invalid_qtags : 6
rx_non_ip_drops : 22
rx_arp_replies : 1
tx_pkts : 97
tx_mcast : 1
tx_ipsec_pkts : 31
tx_ipsec_encap : 31
tx_pre_ipsec_pkts : 31
tx_pre_ipsec_encap : 31
bfd_tx_pkts : 32
bfd_tx_octets : 5442
rx_icmp_network_unreach : 3
tx_icmp_echo_requests : 1
tx_icmp_network_unreach : 3
vEdge1# show system statistics diff
```

```
rx_pkts : 82
ip_fwd : 89
ip_fwd_to_egress : 45
ip_fwd_null_nhop : 3
ip_fwd_to_cpu : 24
ip_fwd_rx_ipsec : 22
rx_bcast : 1
rx_implicit_acl_drops : 1
```

rx_replay_integrity_drops : 24

```
rx_invalid_qtags : 2
rx_non_ip_drops : 14
rx_arp_replies : 1
tx_pkts : 62
tx_mcast : 1
tx_ipsec_pkts : 24
tx_ipsec_encap : 24
```

```
tx_pre_ipsec_pkts : 24
tx_pre_ipsec_encap : 24
tx_arp_reqs : 1
bfd_tx_pkts : 23
bfd_tx_octets : 3908
rx_icmp_network_unreach : 3
tx_icmp_echo_requests : 1
tx_icmp_network_unreach : 3
vEdge1# show system statistics diff
```

```
rx_pkts : 80
ip_fwd : 84
ip_fwd_to_egress : 39
ip_fwd_to_cpu : 20
ip_fwd_rx_ipsec : 24
```

```
rx_replay_integrity_drops : 22
```

```
rx_invalid_qtags : 3
rx_non_ip_drops : 12
tx_pkts : 66
tx_ipsec_pkts : 21
tx_ipsec_encap : 21
tx_pre_ipsec_pkts : 21
tx_pre_ipsec_encap : 21
bfd_tx_pkts : 21
bfd_tx_octets : 3571
```

En primer lugar, realice un **request security ipsec-rekey** análisis en vEdge. A continuación, realice varias iteraciones de **show system statistics diff** y vea si aún puede ver **rx_replay_integrity_drops**.

Si lo hace, compruebe la configuración de seguridad.

```
vEdge1# show running-config security security
ipsec
authentication-type sha1-hmac ah-sha1-hmac
!
```

Problemas del ISP con el tráfico marcado DSCP

De forma predeterminada, todo el tráfico de control y gestión del router vEdge a los controladores viaja a través de conexiones DTLS o TLS y se marca con un valor DSCP de CS6 (48 decimales).

En el caso del tráfico de túneles del lugar de datos, los routers vEdge utilizan la encapsulación IPsec o GRE para enviarse tráfico de datos entre sí.

Para la detección de fallas del plano de datos y la medición del rendimiento, los routers se envían periódicamente paquetes BFD entre sí.

Estos paquetes BFD también se marcan con un valor DSCP de CS6 (48 decimales).

Desde la perspectiva del ISP, este tipo de tráfico se ve como tráfico UDP con valor DSCP CS6 también porque los routers vEdge y los controladores SD-WAN copian DSCP que marca al encabezado IP externo de forma predeterminada.

Así es como se puede ver si tcpdump se ejecuta en un router ISP de tránsito:

```
14:27:15.993766 IP (tos 0xc0, ttl 64, id 44063, offset 0, flags [DF], proto UDP (17), length 168) 192.168.109.5.12366 > 192.168.20.2.12346: [udp sum ok]
```

Como se puede ver aquí, todos los paquetes están marcados con el byte TOS 0xc0 también conocido como campo DS (que es igual al decimal 192, o 110 000 00 en binario).

Los primeros 6 bits de orden superior corresponden al valor de bits DSCP 48 en decimal o CS6).

Los primeros 2 paquetes de la salida corresponden a un túnel de plano de control y los 2 que permanecen, a un tráfico de túnel de plano de datos.

Según la longitud del paquete y la marca TOS, puede concluir con alta confianza que se trataba de paquetes BFD (direcciones RX y TX). Estos paquetes también están marcados con CS6.

A veces, algunos proveedores de servicios (especialmente los proveedores de servicios MPLS L3 VPN/MPLS L2 VPN) mantienen SLA diferentes y pueden manejar una clase diferente de tráfico basado en las marcas DSCP de manera diferente.

Por ejemplo, si tiene un servicio premium para priorizar el tráfico de señalización y voz DSCP EF y CS6.

Dado que el tráfico prioritario casi siempre se controla, incluso si no se excede el ancho de banda total de un enlace ascendente, para este tipo de pérdida de paquetes de tráfico se puede ver y, por lo tanto, las sesiones BFD también pueden ser inestables.

En algunos casos, se observó que si la cola de prioridad dedicada en el router del proveedor de servicio se ve agotada, no se ve ninguna caída para el tráfico normal (por ejemplo, cuando ejecuta un **ping** simple desde el router vEdge).

Esto se debe a que dicho tráfico está marcado con el valor DSCP predeterminado 0, como se puede ver aquí (byte TOS):

```
15:49:22.268044 IP (tos 0x0, ttl 62, id 0, offset 0, flags [DF], proto UDP (17), length 142) 192.168.110.5.12366 > 192.168.109.7.12346: [no cksum] UDP,
```

Pero al mismo tiempo, sus sesiones de BFD flap:

```
show bfd history DST PUBLIC DST PUBLIC RX TX SYSTEM IP SITE ID COLOR STATE IP PORT ENCAP TIME PKTS PKTS DEL -----
```

Y aquí **nping** es útil para resolver problemas:

```
vedge2# tools nping vpn 0 options "--tos 0x0c --icmp --icmp-type echo --delay 200ms -c 100 -q" 192.168.109.7 Nping in VPN 0 Starting Nping 0.6.47 (ht
```

Debug BFD

Si se requiere una investigación más profunda, ejecute la depuración de BFD en el router vEdge.

Forwarding Traffic Manager (FTM) es responsable de las operaciones de BFD en los routers vEdge y, por lo tanto, es necesario **debug ftm bfd**.

Todos los resultados de la depuración se almacenan en un **/var/log/tmplog/vdebug** archivo y, si desea tener esos mensajes en la consola (similar al **terminal monitor** comportamiento de Cisco IOS), puede utilizar **monitor start /var/log/tmplog/vdebug**.

Para detener el registro, puede utilizar **monitor stop /var/log/tmplog/vdebug**

A continuación se muestra cómo el resultado busca una sesión BFD que se interrumpe debido al tiempo de espera (TLOC remoto con dirección IP 192.168.110.6 ya no es accesible):

```
log:local7.debug: May 7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_update_state[1008]: BFD-session TNL 192.168.110.5:12366->192.168.110.6:123
```

Otra depuración valiosa para habilitar la depuración de **Tunnel Traffic Manager (TTM)** eventos es **debug ttm events**.

Así es como se ve el **BFD DOWN** evento desde la perspectiva de TTM:

```
log:local7.debug: May 7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[194]: Received TTM Msg LINK_BFD, Client: ftmd, AF: LINK log:loc
```

Utilizar Packet-Trace para capturar paquetes BFD (20.5 y posteriores)

Otra herramienta útil introducida en 20.5.1 y en software posterior es packet-trace for vEdges.

Debido a que la sesión BFD utiliza los mismos puertos estándar, generalmente 12346, es más simple filtrar en función de la dirección IP par.

Por ejemplo:

```
vedge# show bfd sessions SOURCE TLOC REMOTE TLOC DST PUBLIC DST PUBLIC DETECT TX SYSTEM IP SITE ID STAT
```

El seguimiento de paquetes se configuraría:

```
vedge# debug packet-trace condition ingress-if ge0/0 vpn 0 source-ip 192.168.29.39
```

```
vedge# debug packet-trace condition start
```



```
vedge# debug packet-trace condition stop
```

Los resultados se pueden mostrar mediante los comandos show indicados a continuación. Para los paquetes de ingreso, hay un indicador 'isBFD' que se establece en '1' (true) para el tráfico BFD.

```
vedge# show packet-trace statistics
packet-trace statistics 0
source-ip          192.168.29.39
source-port        12346
destination-ip     192.168.16.29
destination-port   12346
source-interface   ge0_0
destination-interface loop0.1
decision           FORWARD
duration           25
```

```
packet-trace statistics 1
source-ip          192.168.29.39
source-port        12346
destination-ip     192.168.16.29
destination-port   12346
source-interface   ge0_0
destination-interface loop0.1
decision           FORWARD
duration           14
```

```
packet-trace statistics 2
source-ip          192.168.29.39
source-port        12346
destination-ip     192.168.16.29
destination-port   12346
source-interface   ge0_0
destination-interface loop0.1
decision           FORWARD
duration           14
```

```
vedge# show packet-trace detail 0
```

```
=====
Pkt-id          src_ip(ingress_if)          dest_ip(egress_if)          Duration          Decision
=====
0              192.168.29.39:12346 (ge0_0)    192.168.16.29:12346 (loop0.1)    25 us            FORWARD
INGRESS_PKT:
00 50 56 84 79 be 00 50 56 84 3c b5 08 00 45 c0 00 96 ab 40 40 00 3f 11 e0 c1 c0 a8 1d 27 c0
a8 10 1d 30 3a 30 3a 00 82 00 00 a0 00 01 02 00 00 0e 3f 4b 65 07 bc 61 03 38 71 93 53 58
88 d8 08 41 95 7c 1a ff 8b cc b4 d0 d8 61 44 40 67 cc 1a 01 fd 1f c4 45 95 ea 7e 15 c9 08
2e b6 63 84 00
EGRESS_PKT:
a1 5e fe 11 00 00 00 00 00 00 00 00 00 00 04 00 0c 04 00 41 01 02 00 00 00 00 00 00 00 00
00 00 00 00 00 00 04 00 00 00 00 00 00 00 02 00 3a 30 3a 30 1d 10 a8 c0 00 00 00 00 00 00
00 00 00 00 00 00 01 00 00 00 27 1d a8 c0 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00
a4 00 01 00 00
Feature Data
-----
TOUCH : fp_proc_packet
core_id: 2
DSCP: 48
-----
TOUCH : fp_proc_packet2
core_id: 2
DSCP: 48
-----
```

```

TOUCH : fp_ip_forward
core_id: 2
DSCP: 48
-----
TOUCH : fp_ipsec_decrypt
core_id: 2
DSCP: 48
-----
FP_TRACE_FEAT_IPSEC_DATA:
src_ip : 192.168.29.39
src_port : 3784
dst_ip : 192.168.16.29
dst_port : 3784
isBFD : 1
core_id: 2
DSCP: 48
-----
TOUCH : fp_send_pkt
core_id: 2
DSCP: 48
-----
TOUCH : fp_hw_x86_pkt_free
core_id: 2
DSCP: 48
-----
TOUCH : fp_proc_remote_bfd_
core_id: 2
DSCP: 48
-----
TOUCH : BFD_ECHO_REPLY
core_id: 2
DSCP: 48
-----
TOUCH : fp_hw_x86_pkt_free
core_id: 2
DSCP: 48

```

Los paquetes BFD de salida se capturan de manera similar. Estos resultados identifican el tipo específico, ya sea una solicitud de eco o una respuesta.

```

vedge# debug packet-trace condition vpn 0 destination-ip 192.168.29.39
vedge# debug packet-trace condition start
vedge# debug packet-trace condition stop

```

```

vedge# show packet-trace statistics
packet-trace statistics 0
source-ip          192.168.16.29
source-port        3784
destination-ip     192.168.29.39
destination-port   3784
source-interface   loop0.0
destination-interface ge0_0
decision           FORWARD
duration           15
packet-trace statistics 1
source-ip          192.168.16.29
source-port        3784
destination-ip     192.168.29.39
destination-port   3784

```

```

source-interface      loop0.0
destination-interface ge0_0
decision              FORWARD
duration              66
packet-trace statistics 2
source-ip             192.168.16.29
source-port           3784
destination-ip        192.168.29.39
destination-port      3784
source-interface      loop0.0
destination-interface ge0_0
decision              FORWARD
duration              17

```

```
vedge# show packet-trace details 0
```

```

=====
Pkt-id          src_ip(ingress_if)          dest_ip(egress_if)          Duration          Decision
=====
0               192.168.16.29:3784 (loop0.0)  192.168.29.39:3784 (ge0_0)  15 us            FORWARD
INGRESS_PKT:
45 c0 00 4f 00 00 40 00 ff 11 cc 48 c0 a8 10 1d c0 a8 1d 27 0e c8 0e c8 00 3b 00 00 80 c0 07
00 00 00 00 01 00 00 00 01 00 0f 42 40 00 0f 42 40 00 0f 42 40 01 00 0c 01 00 00 1d 3b b1
c9 89 d7 03 00 0f c0 a8 10 1d 30 3a c0 a8 1d 27 30 3a a3 96 07 3b 47 1c 60 d1 d5 76 4c 72
78 1f 9a 0d 00
EGRESS_PKT:
00 50 56 84 3c b5 00 50 56 84 79 be 08 00 45 c0 00 96 ab 40 40 00 3f 11 e0 c1 c0 a8 10 1d c0
a8 1d 27 30 3a 30 3a 00 82 00 00 a0 00 01 01 00 00 5c 3d 88 9a c7 28 23 1b e6 18 ea fe 73
1b b9 e3 79 bf d9 f4 72 41 96 c1 47 07 44 56 77 5a a2 fb 43 59 c1 97 59 47 62 21 77 d4 f4
47 8b 30 b0 00
Feature Data
-----
TOUCH : fp_send_bfd_pkt
core_id: 0
DSCP: 48
-----
TOUCH : BFD_ECHO_REPLY
core_id: 0
DSCP: 48
-----
TOUCH : fp_ipsec_loopback_f
core_id: 0
DSCP: 48
-----
TOUCH : fp_send_pkt
core_id: 0
DSCP: 48
-----
TOUCH : fp_ip_forward
core_id: 2
DSCP: 48
-----
TOUCH : fp_send_ip_packet
core_id: 2
DSCP: 48
-----
TOUCH : fp_send_pkt
core_id: 2
DSCP: 48
-----
TOUCH : fp_hw_x86_pkt_free
core_id: 2
DSCP: 48

```

vedge# show packet-trace details 1

```
=====
Pkt-id          src_ip(ingress_if)          dest_ip(egress_if)          Duration          Decision
=====
1              192.168.16.29:3784 (loop0.0)  192.168.29.39:3784 (ge0_0)    66 us            FORWARD
INGRESS_PKT:
45 c0 00 56 00 00 40 00 ff 11 cc 41 c0 a8 10 1d c0 a8 1d 27 0e c8 0e c8 00 42 00 00 80 c0 07
00 00 00 00 01 00 00 00 01 00 0f 42 40 00 0f 42 40 00 0f 42 40 01 00 0c 00 00 00 1d b8 35
a8 09 88 03 00 0f c0 a8 10 1d 30 3a c0 a8 1d 27 30 3a 04 00 07 01 00 05 a6 38 ff 7e 06 1e
da 23 19 d5 00
EGRESS_PKT:
00 50 56 84 3c b5 00 50 56 84 79 be 08 00 45 c0 00 9d ab 40 40 00 3f 11 e0 ba c0 a8 10 1d c0
a8 1d 27 30 3a 30 3a 00 89 00 00 a0 00 01 01 00 00 5c 3e 2d 3b 9e 81 aa 10 26 54 7f 47 5c
d8 81 4f 23 2e 3c 39 1e 94 b2 f4 fb a4 ba 98 54 73 99 8f 2e 95 d7 69 fb 91 41 96 93 03 5b
a4 e4 e8 82 00
Feature Data
-----
TOUCH : fp_send_bfd_pkt
core_id: 0
DSCP: 48
-----
TOUCH : BFD_ECHO_REQUEST
core_id: 0
DSCP: 48
-----
TOUCH : fp_ipsec_loopback_f
core_id: 0
DSCP: 48
-----
TOUCH : fp_send_pkt
core_id: 0
DSCP: 48
-----
TOUCH : fp_ip_forward
core_id: 2
DSCP: 48
-----
TOUCH : fp_send_ip_packet
core_id: 2
DSCP: 48
-----
TOUCH : fp_send_pkt
core_id: 2
DSCP: 48
-----
TOUCH : fp_hw_x86_pkt_free
core_id: 2
DSCP: 48
=====
```

Información Relacionada

- [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).