Implementación de acceso directo a Internet (DIA) para SD-WAN

Contenido

Introducción

Este documento describe cómo implementar Cisco SD-WAN DIA. Se refiere a la configuración cuando el tráfico de Internet sale directamente del router de la sucursal.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Red de área extensa definida por software de Cisco (SD-WAN)
- traducción de Dirección de Red (NAT)

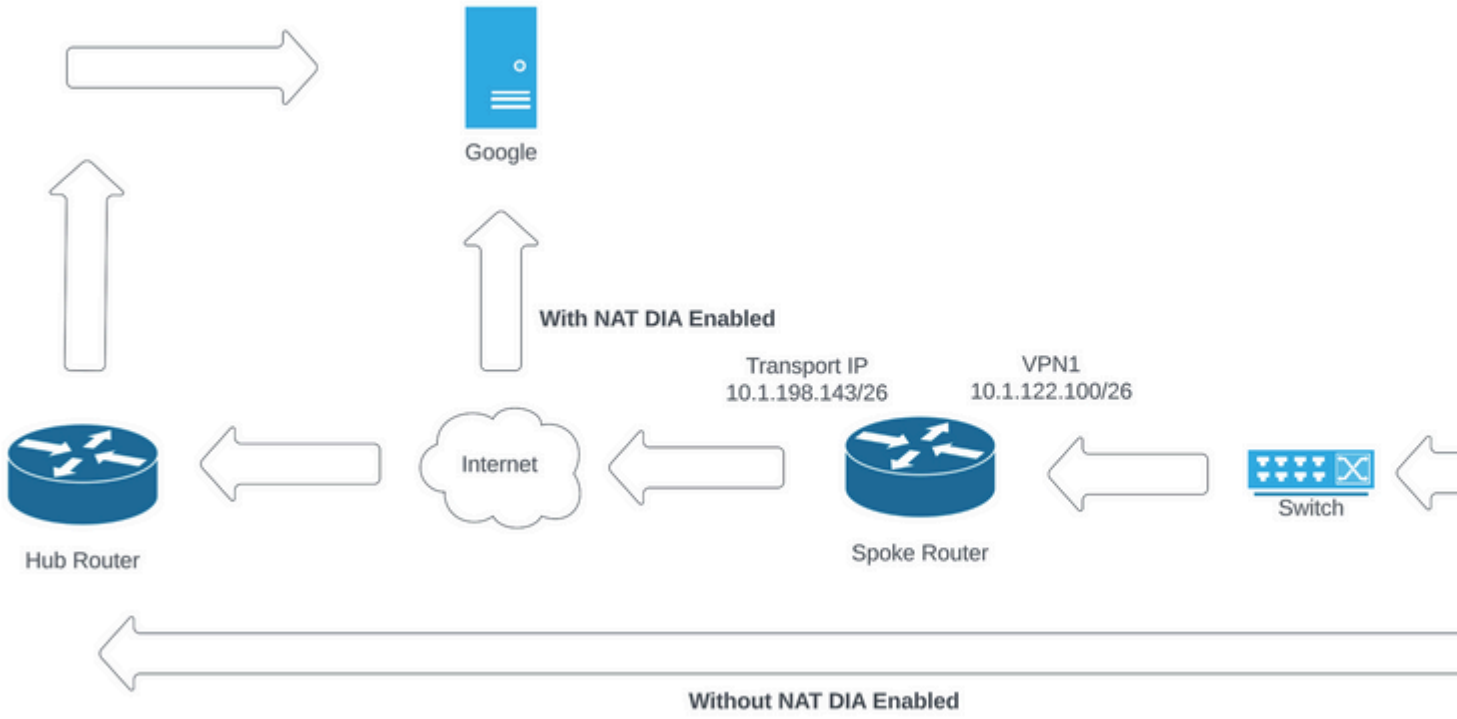
Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco vManager versión 20.6.3
- Cisco WAN Edge Router 17.4.2

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.

Diagrama de la red



Topología de red

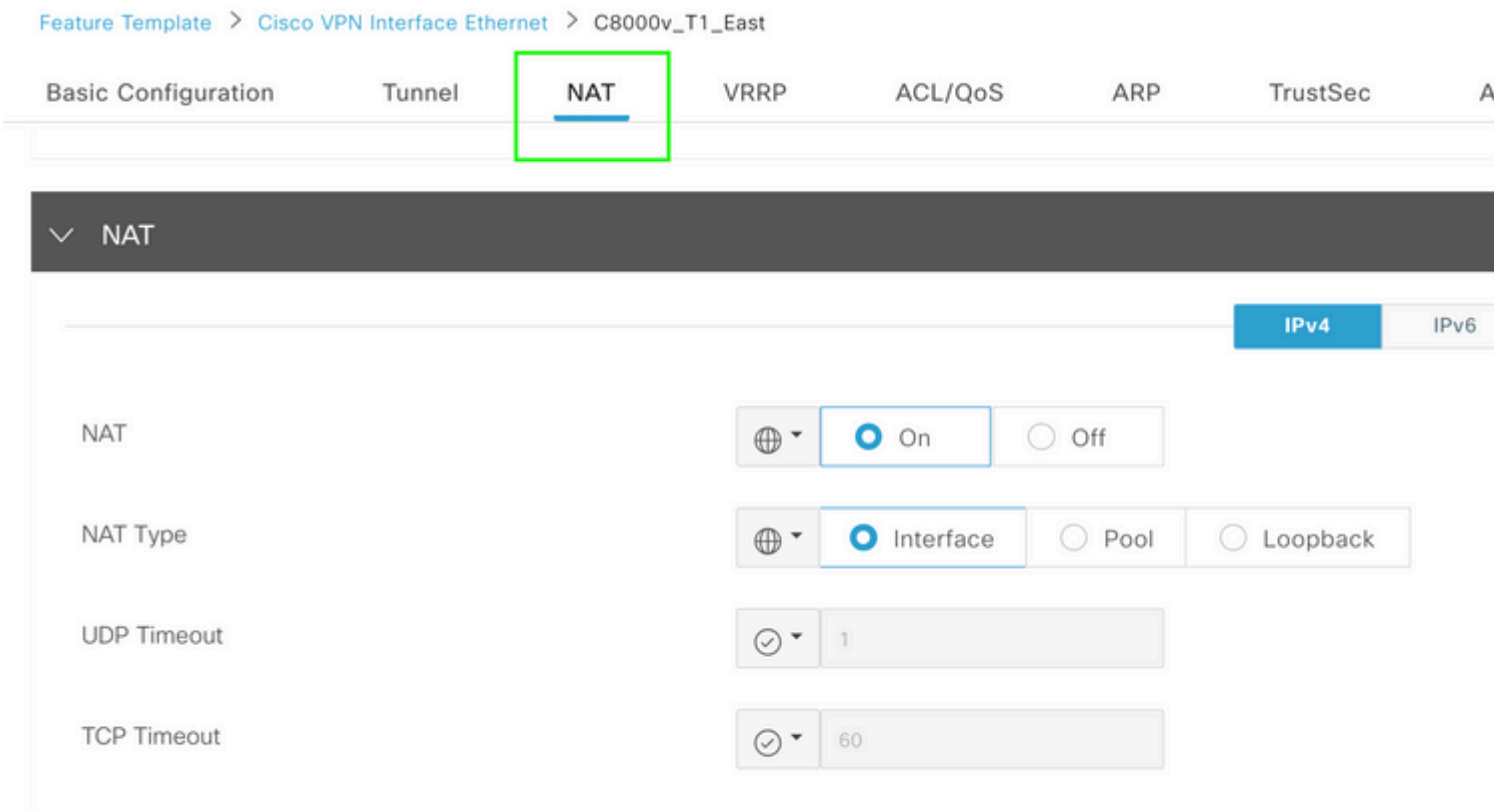
Configuración

El DIA en los routers SD-WAN de Cisco se habilita en dos pasos:

1. Habilite NAT en la interfaz de transporte.

2. Tráfico directo desde el servicio VPN con una ruta estática o una política de datos centralizada.

Habilitar NAT en la interfaz de transporte



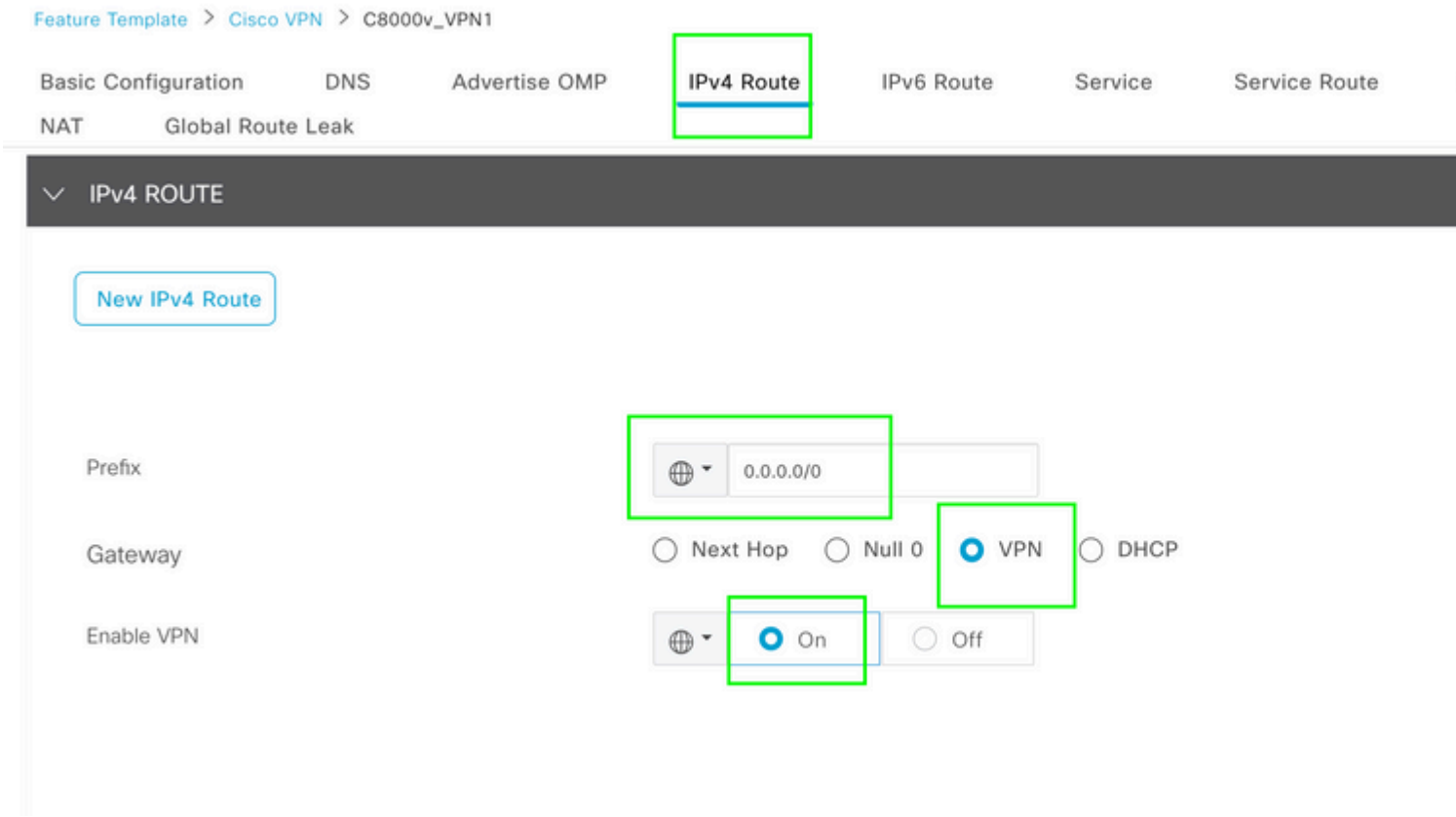
```
ip nat translation tcp-timeout 3600
ip nat translation udp-timeout 60

interface GigabitEthernet2
ip nat outside
```

Tráfico directo desde VPN de servicio

Esto se puede lograr de dos maneras:

1. Static NAT Route (Ruta NAT estática): se debe crear una ruta NAT estática en la plantilla de la función Service VPN 1.



Plantilla de ruta IPV4 de VPN 1

Esta línea se inserta como parte de la configuración.

```
ip nat route vrf 1 0.0.0.0 0.0.0.0 global
```

2. Política de datos centralizada:

Cree una lista de prefijos de datos para que usuarios específicos puedan obtener acceso a Internet mediante DIA.

Lista de prefijos de datos personalizados de política centralizada

```
viptela-policy:policy
 data-policy _DIA_VPN_DIA
  vpn-list DIA_VPN
    sequence 1
     match
      source-data-prefix-list DIA_Prefix_Allow
     !
     action accept
      nat use-vpn 0
      count DIA_1164863292
     !
    !
  default-action accept
 !
 lists
  data-prefix-list DIA_Prefix_Allow
   ip-prefix 10.1.122.106/32
  !
  site-list DIA_Site_list
   site-id 100004
  !
  vpn-list DIA_VPN
   vpn 1
  !
 !
!
apply-policy
 site-list DIA_Site_list
  data-policy _DIA_VPN_DIA from-service
 !
!
```

â€ƒ

Verificación

Sin DIA

La siguiente salida captura cuando NAT DIA no está habilitado en el lado del servicio.

```
cEdge_Site1_East_01#show ip route vrf 1 nat-route

Routing Table: 1
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
```

```
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

cEdge_Site1_East_01#
```

De forma predeterminada, los usuarios de VPN 1 no tienen acceso a Internet.

```
C:\Users\Administrator>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 10.1.122.100: Destination host unreachable.
Reply from 10.1.122.100: Destination host unreachable.
Reply from 10.1.122.100: Destination host unreachable.
Reply from 10.1.122.100: Destination host unreachable.

Ping statistics for 8.8.8.8:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\Administrator>
```

Con DIA

1. Static NAT Route (Ruta NAT estática): la siguiente salida captura DIA de NAT habilitado en el lado del servicio.

```
cEdge_Site1_East_01#show ip route vrf 1 nat-route

Routing Table: 1
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

n*Nd  0.0.0.0/0 [6/0], 01:41:46, Null0

cEdge_Site1_East_01#
```

Los usuarios de VPN 1 ahora pueden conectarse a Internet.

```
C:\Users\Administrator>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=1ms TTL=52
Reply from 8.8.8.8: bytes=32 time=1ms TTL=52
Reply from 8.8.8.8: bytes=32 time=1ms TTL=52
Reply from 8.8.8.8: bytes=32 time=1ms TTL=52

Ping statistics for 8.8.8.8:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\Administrator>
```

El resultado subsiguiente captura las traducciones NAT.

```
cEdge_Site1_East_01#sh ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
icmp 10.1.198.143:1        10.1.122.106:1        8.8.8.8:1             8.8.8.8:1

Total number of translations: 1
```

El siguiente comando captura qué trayectoria debe tomar el paquete.

```
cEdge_Site1_East_01#show sdwan policy service-path vpn 1 interface GigabitEthernet 4 source-ip 10.1.122.
Next Hop: Remote
  Remote IP: 10.1.198.129, Interface GigabitEthernet2 Index: 8
```

2. Política de datos centralizada:

Una vez que la política de datos centralizados se aplica a vSmart, el show sdwan policy from-vsmart data-policy se puede utilizar en el dispositivo de extremo de la WAN para verificar qué política ha recibido el dispositivo.

```
cEdge_Site1_East_01#show sdwan policy from-vsmart data-policy
from-vsmart data-policy _DIA_VPN_DIA
 direction from-service
 vpn-list DIA_VPN
  sequence 1
   match
    source-data-prefix-list DIA_Prefix_Allow
   action accept
    count DIA_1164863292
    nat use-vpn 0
    no nat fallback
  default-action accept
```

```
cEdge_Site1_East_01#
```

Los usuarios de VPN 1 ahora pueden conectarse a Internet.

```
C:\Users\Administrator>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=4ms TTL=52
Reply from 8.8.8.8: bytes=32 time=1ms TTL=52
Reply from 8.8.8.8: bytes=32 time=1ms TTL=52
Reply from 8.8.8.8: bytes=32 time=1ms TTL=52

Ping statistics for 8.8.8.8:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 4ms, Average = 1ms

C:\Users\Administrator>
```

El siguiente comando captura qué trayectoria debe tomar el paquete.

```
cEdge_Site1_East_01#show sdwan policy service-path vpn 1 interface GigabitEthernet 4 source-ip 10.1.122.
Next Hop: Remote
  Remote IP: 10.1.198.129, Interface GigabitEthernet2 Index: 8
```

El resultado subsiguiente captura las traducciones NAT.

```
cEdge_Site1_East_01#sh ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
icmp 10.1.198.143:1        10.1.122.106:1        8.8.8.8:1             8.8.8.8:1

Total number of translations: 1
```

Esta salida captura los incrementos del contador.

```
cEdge_Site1_East_01#show sdwan policy data-policy-filter
data-policy-filter _DIA_VPN_DIA
 data-policy-vpnlist DIA_VPN
  data-policy-counter DIA_1164863292
   packets 4
   bytes   296
  data-policy-counter default_action_count
   packets 0
   bytes   0
```

```
cEdge_Site1_East_01#
```

Este resultado captura el tráfico que está en la negrita ya que la IP de origen no pertenece a la lista de prefijos de datos.

```
cEdge_Site1_East_01#show sdwan policy service-path vpn 1 interface GigabitEthernet 4 source-ip 10.1.122.
Next Hop: Blackhole

cEdge_Site1_East_01#
```

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).