Implementatie van Direct Internet Access (DIA) voor SD-WAN

Inhoud

Inleiding

Dit document beschrijft hoe de Cisco SD-WAN DIA moet worden geïmplementeerd. Het verwijst naar de configuratie wanneer het internetverkeer direct uit takrouter breekt.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco softwaregedefinieerde Wide Area Network (SD-WAN)
- Netwerkadresomzetting (NAT)

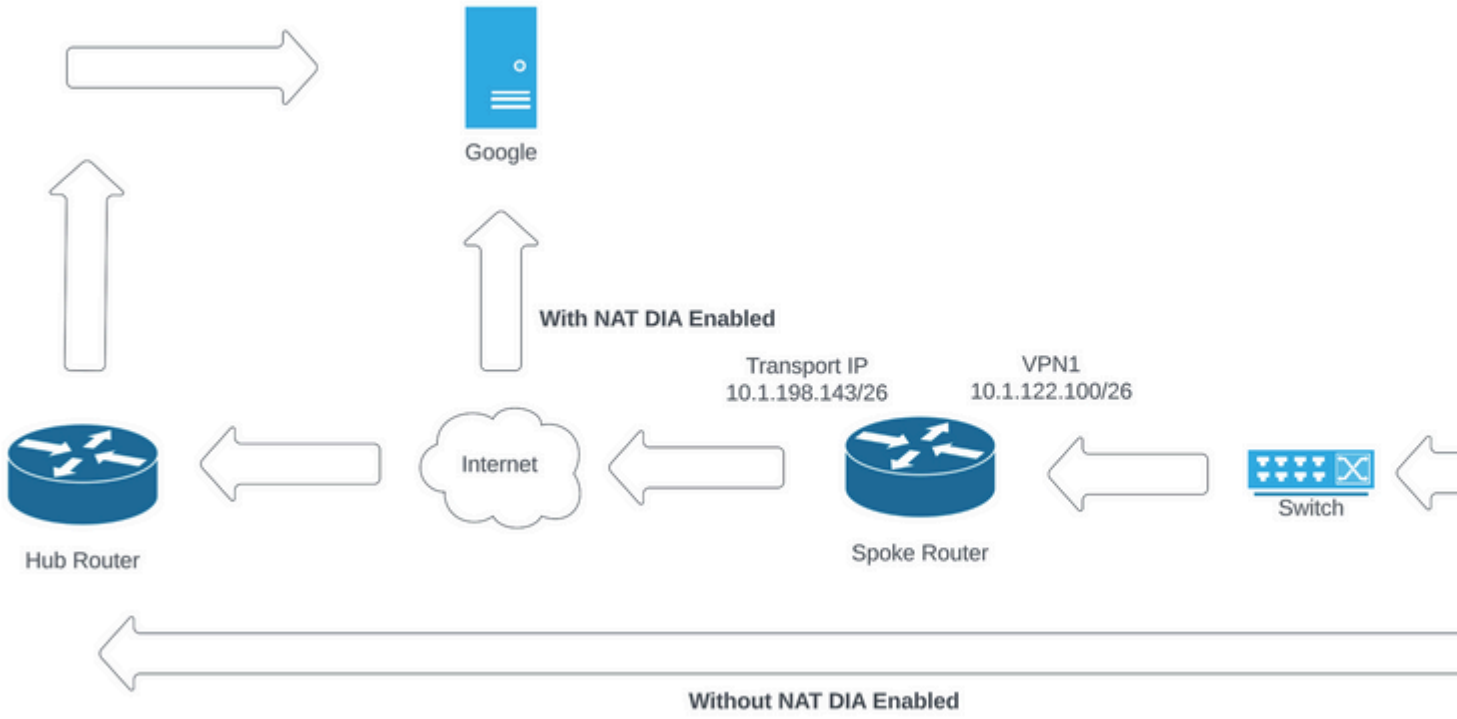
Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco vManagement versie 20.6.3
- Cisco WAN Edge-router 17.4.2

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Netwerkdiagram



Netwerktopologie

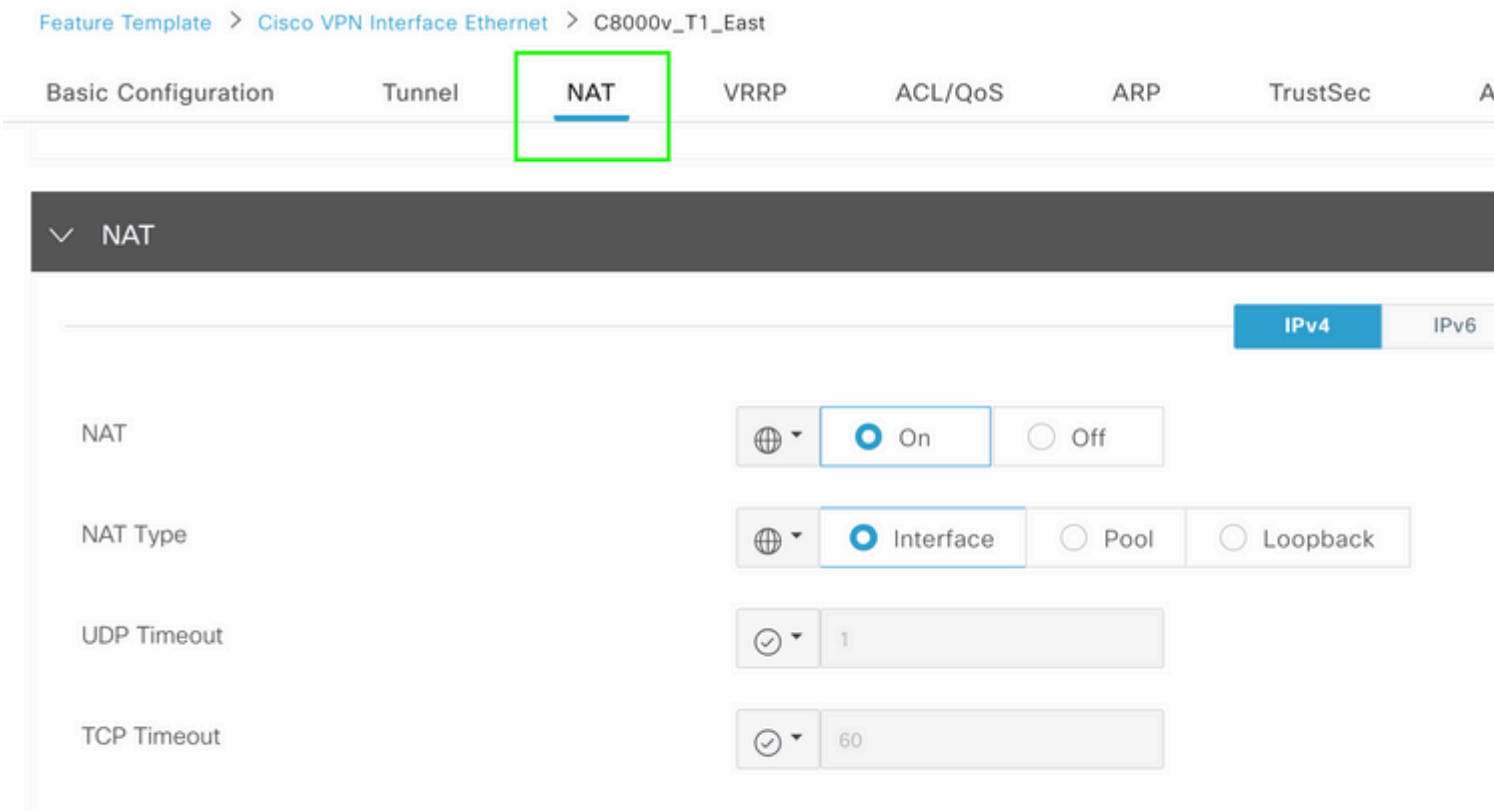
Configuratie

DICOM op Cisco SD-WAN routers is in twee stappen ingeschakeld:

1. Schakel NAT in op transportinterface.

2. Direct verkeer van service-VPN met een statische route of een gecentraliseerd gegevensbeleid.

NAT op transportinterface inschakelen



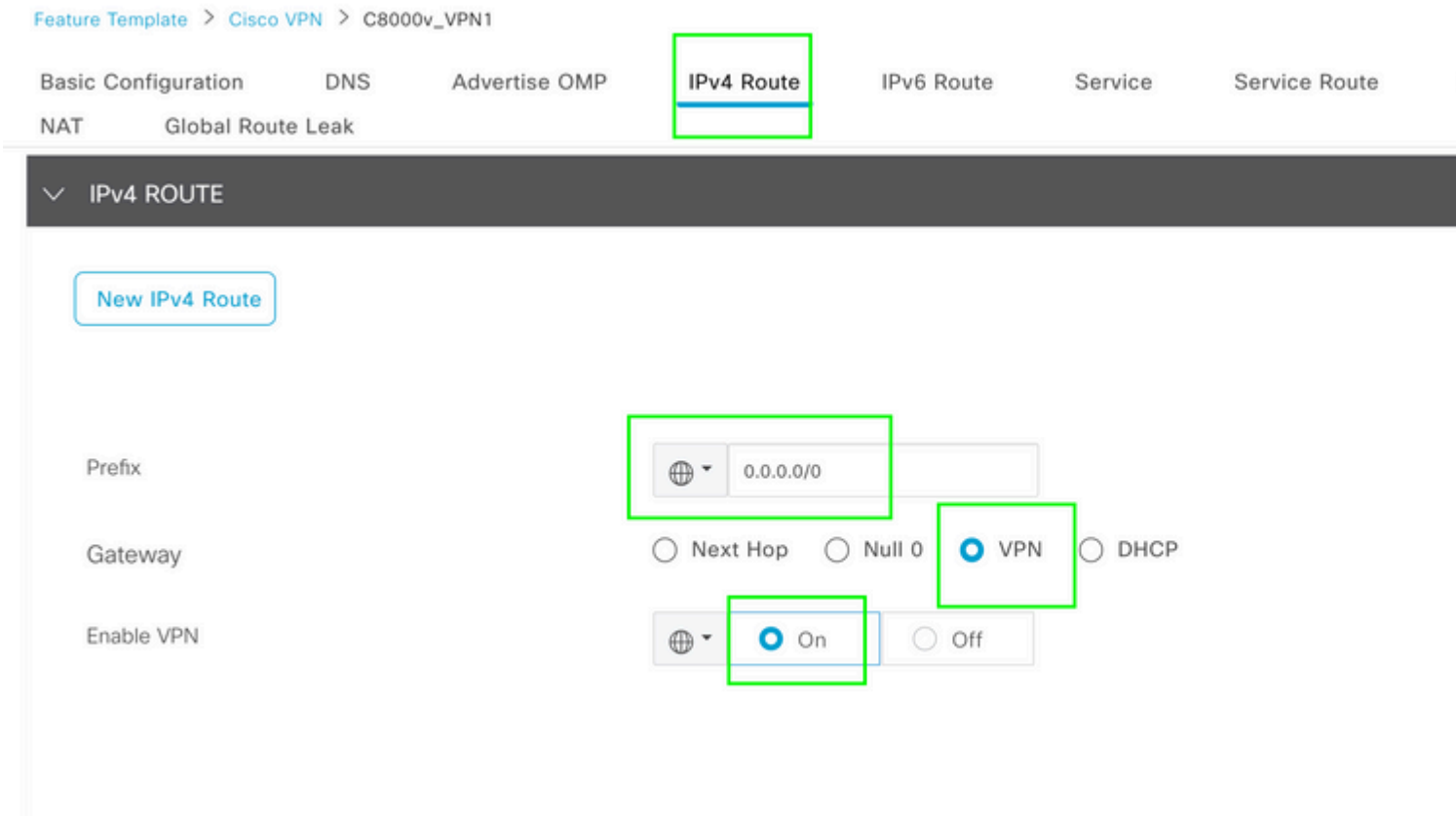
```
ip nat translation tcp-timeout 3600
ip nat translation udp-timeout 60

interface GigabitEthernet2
ip nat outside
```

Direct verkeer vanaf service-VPN

Dit kan op twee manieren worden bereikt:

1. Statische NAT-route: er moet een statische NAT-route worden gemaakt onder de functiemal van de service VPN 1.



VPN 1 IPV4-routesjabloon

Deze lijn wordt geduwd als deel van de configuratie.

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

2. Gecentraliseerd gegevensbeleid:

Maak een data prefixlijst, zodat specifieke gebruikers internettoegang kunnen krijgen via DIA.

Prefixlijst met aangepaste gegevens voor gecentraliseerd beleid

```
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

Verificatie

Zonder DIA

De volgende uitvoer legt vast wanneer NAT DIA niet aan de servicekant is ingeschakeld.

```
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#
```

Standaard hebben gebruikers op VPN 1 geen internettoegang.

```
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>
```

Met DIA

1. Statische NAT-route: met volgende uitvoer wordt NAT DIA ingeschakeld aan de servicekant.

```
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#
```

Gebruikers in VPN 1 kunnen nu het internet bereiken.

```
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>
```

De volgende output neemt NAT-omzettingen op.

```
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
```

Het volgende bevel vangt welke weg het pakket moet nemen.

```
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. Gecentraliseerd gegevensbeleid:

Als het beleid voor gecentraliseerde gegevens naar vSmart is doorgeschoven, wordt de show sdwan policy from-vsmart data-policy De opdracht kan op het WAN-randapparaat worden gebruikt om te controleren welk beleid het apparaat heeft ontvangen.

```
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#
```

Gebruikers in VPN 1 kunnen nu het internet bereiken.

```
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>
```

Het volgende bevel vangt welke weg het pakket moet nemen.

```
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
```

De volgende output neemt NAT-omzettingen op.

```
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
```

Deze uitvoer legt de teller-stappen vast.

```
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#
```

Deze output vangt het verkeer op dat wordt geblokkeerd aangezien de bron IP niet tot de lijst van de gegevensprefix behoort.

```
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#
```

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.