

# Implementazione dell'accesso diretto a Internet (DIA) per SD-WAN

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Esempio di rete](#)

[Configurazione](#)

[Abilita NAT sull'interfaccia di trasporto](#)

[Traffico diretto da VPN servizio](#)

[Verifica](#)

[Senza DIA](#)

[Con DIA](#)

## Introduzione

Questo documento descrive come implementare Cisco SD-WAN DIA. Fa riferimento alla configurazione quando il traffico Internet si interrompe direttamente dal router della succursale.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- SD-WAN (Wide Area Network) definito dal software Cisco
- NAT (Network Address Translation)

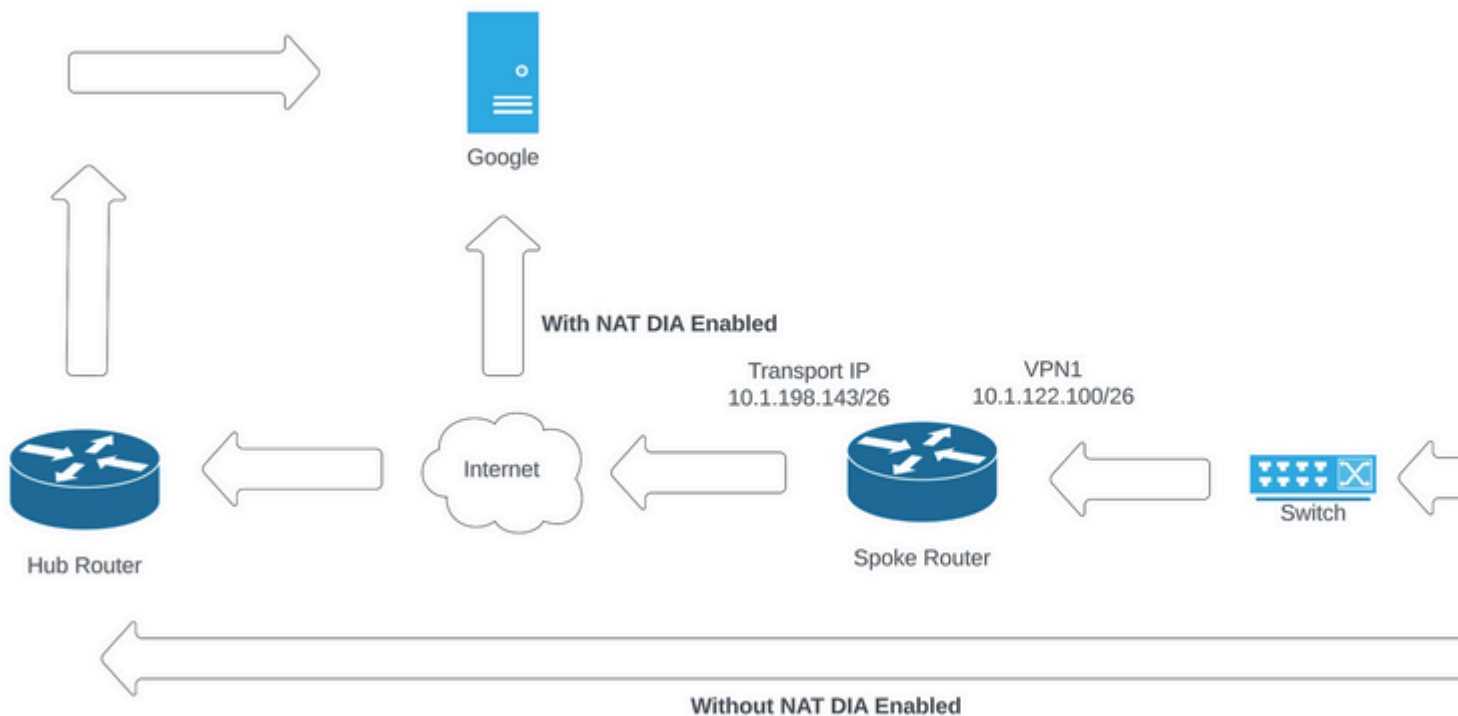
### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco vManage versione 20.6.3
- Cisco WAN Edge Router 17.4.2

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Esempio di rete



Topologia della rete

## Configurazione

DIA su router Cisco SD-WAN è abilitata in due passaggi:

1. Abilitare NAT sull'interfaccia di trasporto.
2. Traffico diretto da VPN di servizio con una route statica o una policy di dati centralizzata.

### Abilita NAT sull'interfaccia di trasporto

Feature Template > Cisco VPN Interface Ethernet > C8000v\_T1\_East

Basic Configuration Tunnel **NAT** VRRP ACL/QoS ARP TrustSec A

▼ NAT

IPv4 IPv6

NAT

On  Off

NAT Type

Interface  Pool  Loopback

UDP Timeout

1

TCP Timeout

60

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

interface GigabitEthernet2
ip nat outside
```

## **Traffico diretto da VPN servizio**

Tale obiettivo può essere conseguito in due modi:

1. Route NAT statica: è necessario creare una route NAT statica nel modello della funzionalità VPN 1 del servizio.

IPv4 ROUTE

[New IPv4 Route](#)

Prefix:

Gateway:  Next Hop     Null 0     **VPN**     DHCP

Enable VPN:  **On**     Off

Modello route VPN 1 IPV4

Questa riga viene inserita come parte della configurazione.

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

## 2. Politica centralizzata dei dati:

Creare un elenco di prefissi di dati, in modo da consentire a utenti specifici di accedere a Internet tramite DIA.

Select a list type on the left and start creating your groups of interest

**Data Prefix**

[+ New Data Prefix List](#)

Name	Entries	Internet Protocol	Reference Count	Updated By
DIA_Prefix_Allow	10.1.122.106/32	IPv4	1	admin

Elenco prefissi dati personalizzati criteri centralizzati

```

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€f

## Verifica

### Senza DIA

L'output successivo viene acquisito quando NAT DIA non è abilitato sul lato servizio.

```
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#

Per impostazione predefinita, gli utenti della VPN 1 non dispongono di accesso 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. Route NAT statica: l'output successivo acquisisce il DIA NAT abilitato sul lato servizio.

```
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#
```

Gli utenti della VPN 1 possono ora accedere 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>
```

L'output successivo acquisisce le traduzioni 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
```

Il comando successivo acquisisce il percorso che il pacchetto deve accettare.

```
cEdge_Site1_East_01#show sdwan policy service-path vpn 1 interface GigabitEthernet 4 source-ip 10.1.122.106
Next Hop: Remote
  Remote IP: 10.1.198.129, Interface GigabitEthernet2 Index: 8
```

## 2. Politica centralizzata dei dati:

Una volta implementata la politica dei dati centralizzati su vSmart, `show sdwan policy from-vsmart data-policy` può essere usato sul dispositivo edge WAN per verificare quale criterio il dispositivo ha ricevuto.

```
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#
```

Gli utenti della VPN 1 possono ora accedere 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>
```

Il comando successivo acquisisce il percorso che il pacchetto deve accettare.

```
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
```

L'output successivo acquisisce le traduzioni 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
```

Questo output cattura gli incrementi del contatore.

```
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#
```

Questo output acquisisce il traffico bloccato in quanto l'IP di origine non appartiene all'elenco di prefissi dei dati.

```
cEdge_Site1_East_01#show sdwan policy service-path vpn 1 interface GigabitEthernet 4 source-ip 10.1.122.1  
Next Hop: Blackhole
```

```
cEdge_Site1_East_01#
```

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).