

為SD-WAN實施直接網際網路接入(DIA)

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[網路圖表](#)

[組態](#)

[在傳輸介面上啟用NAT](#)

[來自服務VPN的直接流量](#)

[驗證](#)

[不使用DIA](#)

[使用DIA](#)

簡介

本檔案介紹如何實作Cisco SD-WAN DIA。它是指網際網路流量直接從分支機構路由器中斷時的配置。

必要條件

需求

思科建議您瞭解以下主題：

- [思科軟體定義廣域網路\(SD-WAN\)](#)
- [網路位址轉譯\(NAT\)](#)

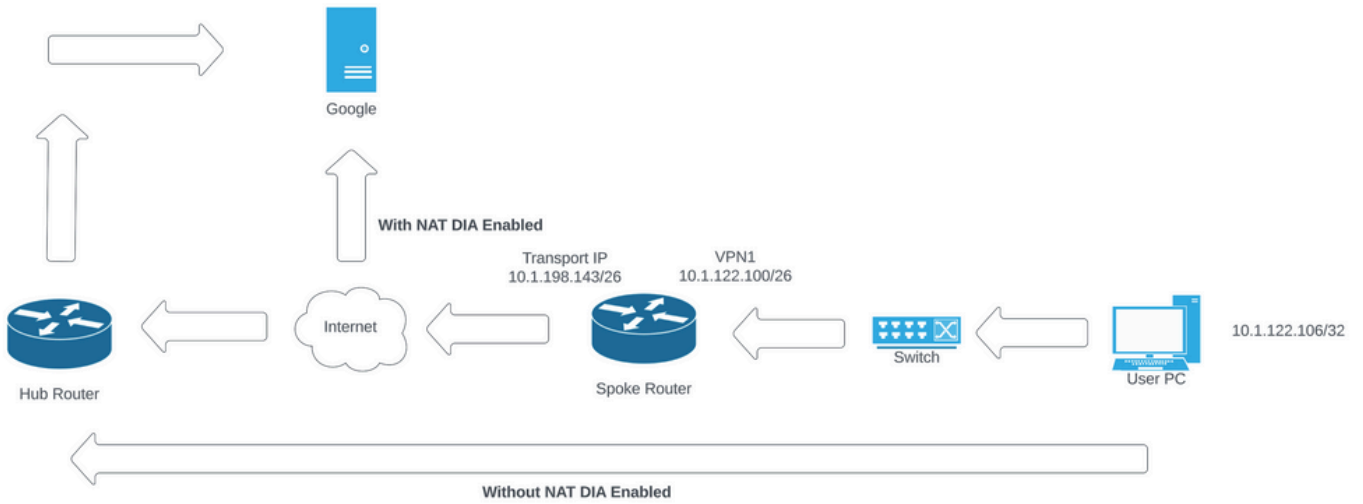
採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco vManage版本20.6.3
- Cisco WAN邊緣路由器17.4.2

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

網路圖表



網路拓撲

組態

Cisco SD-WAN路由器上的DIA通過兩個步驟啟用：

- 1.在傳輸介面上啟用NAT。
- 2.使用靜態路由或集中資料策略從服務VPN直接傳送流量。

在傳輸介面上啟用NAT

Feature Template > Cisco VPN Interface Ethernet > C8000v_T1_East

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

▼ NAT

IPv4 IPv6

NAT On Off

NAT Type Interface Pool Loopback

UDP Timeout

TCP Timeout

[New Static NAT](#)

VPN介面NAT模板

這是配置在啟用NAT後的外觀。

```
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet2 overload
ip nat translation tcp-timeout 3600
ip nat translation udp-timeout 60

interface GigabitEthernet2
ip nat outside
```

來自服務VPN的直接流量

這可以通過兩種方式實現：

1.靜態NAT路由：需要在服務VPN 1功能模板下建立靜態NAT路由。

The screenshot shows the configuration page for an IPv4 Route in a Cisco VPN feature template. The breadcrumb path is 'Feature Template > Cisco VPN > C8000v_VPN1'. The 'IPv4 Route' tab is selected. The configuration includes a 'Prefix' of 0.0.0.0/0, a 'Gateway' set to 'VPN', and 'Enable VPN' checked. The 'Add' button is highlighted.

VPN 1 IPV4路由模板

此行作為配置的一部分推送。

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

2.集中資料策略：

建立資料字首清單，以便允許特定使用者通過DIA訪問Internet。

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

Application

Color

Community

Data Prefix

Policer

Prefix

Site

App Probe Class

SLA Class

TLOC

VPN

New Data Prefix List

Name	Entries	Internet Protocol	Reference Count	Updated By	Last Updated	Action
DIA_Prefix_Allow	10.1.122.106/32	IPv4	1	admin	18 Jul 2023 9:31:26 AM CDT	Edit Delete

集中策略自定義資料字首清單

建立VPN清單，以便特定VPN使用者可以發起流量。

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

Application

Color

Community

Data Prefix

Policer

Prefix

Site

App Probe Class

SLA Class

TLOC

VPN

New VPN List

Name	Entries	Reference Count	Updated By	Last Updated	Action
DIA_VPN	1	1	admin	18 Jul 2023 9:56:21 AM CDT	Edit Delete

集中策略自定義VPN清單

建立站點清單，以便策略可應用於特定站點。

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

Application

Color

Community

Data Prefix

Policer

Prefix

Site

App Probe Class

SLA Class

TLOC

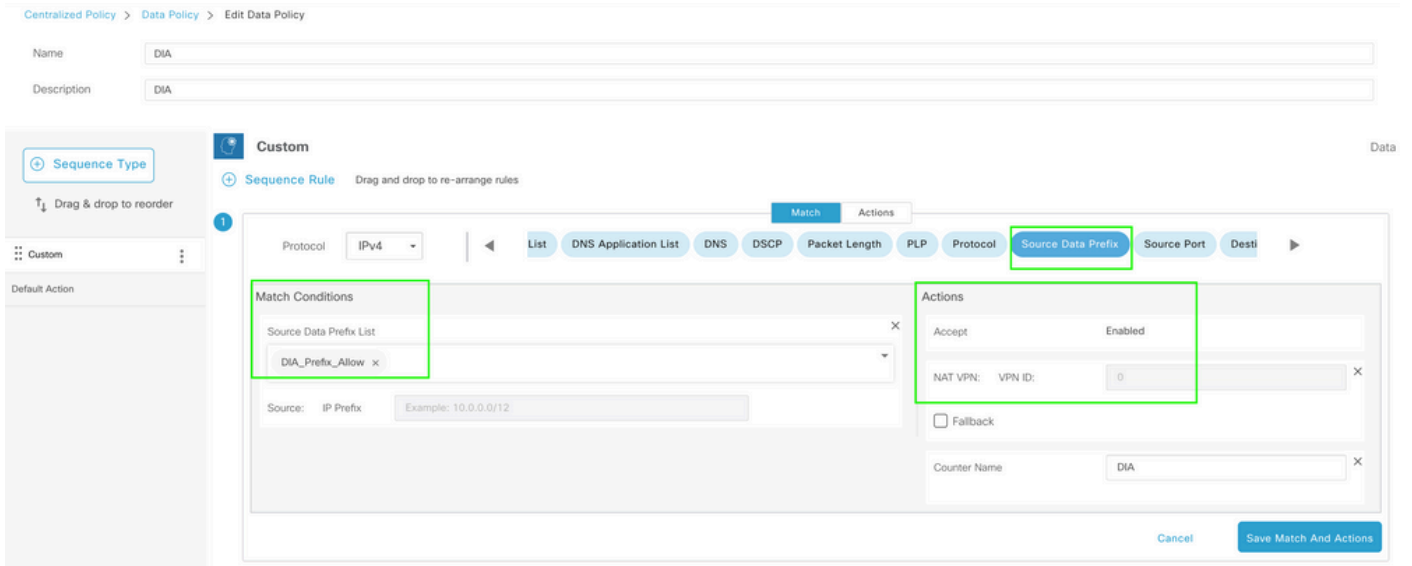
VPN

New Site List

Name	Entries	Reference Count	Updated By	Last Updated	Action
DIA_Site_list	100004	1	admin	18 Jul 2023 10:03:59 AM CDT	Edit Delete

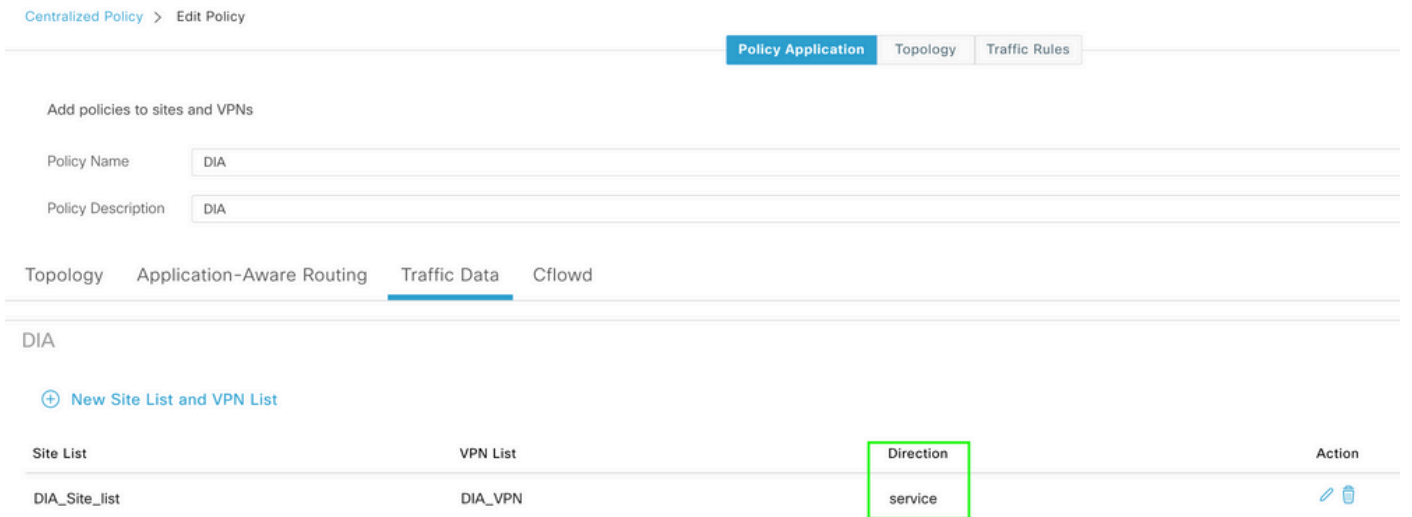
集中策略自定義站點清單

建立自定義資料策略以匹配源資料字首，並將操作設定為使用NAT VPN 0，以便它可以遍歷DIA。



集中資料策略

此策略的方向必須來自服務端。



流量資料規則

這是集中資料策略的預覽。

```
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
!
!

```

驗證

不使用DIA

在服務端未啟用NAT DIA時，下一個輸出將捕獲。

```
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#
```

預設情況下，VPN 1上的使用者不能訪問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>
```

使用DIA

1.靜態NAT路由：下一個輸出捕獲在服務端啟用的NAT DIA。

```
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#
```

VPN 1中的使用者現在可以訪問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>

後續輸出捕獲NAT轉換。

```
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
```

下一個命令會擷取封包必須採用的路徑。

```
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.集中資料策略：

將集中式資料策略推送到vSmart後，`show sdwan policy from-vsmart data-policy` 命令可用於WAN邊緣裝置，以驗證該裝置已接收哪些策略。

```
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#
```

VPN 1中的使用者現在可以訪問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>
```

下一個命令會擷取封包必須採用的路徑。

```
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
```

後續輸出捕獲NAT轉換。

```
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
```

此輸出捕獲計數器的增量。

```
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#
```

此輸出會擷取因為來源IP不屬於資料首碼清單而被封鎖的流量。

```
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#

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。