

Implémenter un accès direct à Internet (DIA) pour SD-WAN

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Diagramme du réseau](#)

[Configuration](#)

[Activer NAT sur l'interface de transport](#)

[Trafic direct du VPN de service](#)

[Vérification](#)

[Sans DIA](#)

[Avec DIA](#)

Introduction

Ce document décrit comment mettre en oeuvre Cisco SD-WAN DIA. Il fait référence à la configuration lorsque le trafic Internet est interrompu directement à partir du routeur de la filiale.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Réseau étendu défini par logiciel (SD-WAN) de Cisco
- Traduction d'adresses réseau (NAT)

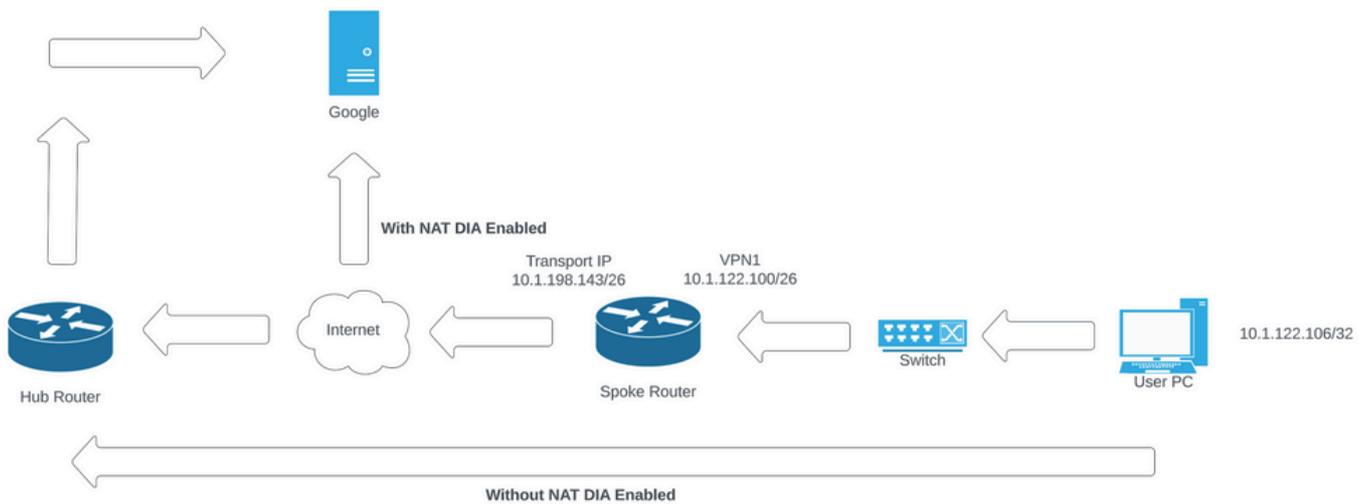
Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco vManage version 20.6.3
- Routeur de périphérie WAN Cisco 17.4.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Diagramme du réseau



Topologie du réseau

Configuration

L'activation de la fonction DIA sur les routeurs Cisco SD-WAN s'effectue en deux étapes :

1. Activez NAT sur l'interface de transport.
2. Dirigez le trafic à partir du VPN de service avec une route statique ou une politique de données centralisée.

Activer NAT sur l'interface de transport

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](#)

Modèle NAT d'interface VPN

Voici à quoi ressemble la configuration après l'activation de la fonction NAT.

```
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
```

Trafic direct du VPN de service

Pour ce faire, deux méthodes sont possibles :

1. Route NAT statique : une route NAT statique doit être créée sous le modèle de fonctionnalité VPN 1 de service.

The screenshot shows the configuration page for an IPv4 Route. The breadcrumb trail is 'Feature Template > Cisco VPN > C8000v_VPN1'. The 'IPv4 Route' tab is active. The configuration includes a 'Prefix' field with '0.0.0.0/0', a 'Gateway' section with radio buttons for 'Next Hop', 'Null 0', 'VPN' (selected), and 'DHCP', and an 'Enable VPN' section with radio buttons for 'On' (selected) and 'Off'. There is a 'Mark as Optional Row' checkbox and an 'Add' button.

Modèle de route IPV4 VPN 1

Cette ligne est diffusée dans le cadre de la configuration.

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

2. Politique de centralisation des données :

Créez une liste de préfixes de données afin que des utilisateurs spécifiques puissent accéder à Internet via DIA.

Centralized Policy > Define Lists Custom Options

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	✎ 🗑

Liste de préfixes de données personnalisées de stratégie centralisée

Créez une liste VPN, de sorte que des utilisateurs VPN spécifiques puissent initier le trafic.

Centralized Policy > Define Lists Custom Options

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	✎ 🗑

Liste VPN personnalisée de stratégie centralisée

Créez une liste de sites afin que la stratégie puisse être appliquée à un site spécifique.

Centralized Policy > Define Lists Custom Options

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	✎ 🗑

Liste des sites personnalisés de stratégie centralisée

Créez une stratégie de données personnalisée afin de correspondre au préfixe de données source et définissez l'action pour utiliser NAT VPN 0, afin qu'il puisse traverser DIA.

Centralized Policy > Data Policy > Edit Data Policy

Name: DIA
Description: DIA

Sequence Type: Custom

Match Conditions:

- Source Data Prefix List: DIA_Prefix_Allow
- Source: IP Prefix (Example: 10.0.0.0/12)

Match: Protocol (IPv4), List, DNS Application List, DNS, DSCP, Packet Length, PLP, Protocol, Source Data Prefix, Source Port, Desti

Actions:

- Accept: Enabled
- NAT VPN: VPN ID: 0
- Fallback:
- Counter Name: DIA

Buttons: Cancel, Save Match And Actions

Politique de données centralisée

La direction de cette politique doit être du côté du service.

Centralized Policy > Edit Policy

Policy Application | Topology | Traffic Rules

Add policies to sites and VPNs

Policy Name: DIA
Policy Description: DIA

Topology | Application-Aware Routing | Traffic Data | Cflowd

DIA

+ New Site List and VPN List

Site List	VPN List	Direction	Action
DIA_Site_list	DIA_VPN	service	

règle relative aux données de trafic

Il s'agit de l'aperçu de la politique de données centralisée.

```
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
!
!
```



```
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>
```

Avec DIA

1. Route NAT statique : le résultat suivant capture NAT DIA activé côté service.

```
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#
```

Les utilisateurs du VPN 1 peuvent désormais accéder à 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>

Le résultat suivant capture les traductions 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
```

La commande suivante capture le chemin que le paquet doit emprunter.

```
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. Politique de centralisation des données :

Une fois que la politique de données centralisées est poussée vers vSmart, le `show sdwan policy from-vsmart data-policy` peut être utilisée sur le périphérique de périphérie WAN afin de vérifier quelle stratégie le périphérique a reçue.

```
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#

Les utilisateurs du VPN 1 peuvent désormais accéder à 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>
```

La commande suivante capture le chemin que le paquet doit emprunter.

```
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
```

Le résultat suivant capture les traductions 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
```

Cette sortie capture les incréments du compteur.

```
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#
```

Cette sortie capture le trafic qui est mis en trou noir puisque l'IP source n'appartient pas à la liste de préfixes de données.

```
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#
```

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.