

# (DIA) تنرتنإلإىلإرشابملا لوصولا قىببطات SD-WAN ل

## تايوتحمل

[عمدقمل](#)

[ةيساسألا تابلطتمل](#)

[تابلطتمل](#)

[عمدختسمل تانوكمل](#)

[ةكبش لىل طي طختلا مسرلا](#)

[نىوكتلا](#)

[لقنلا ةهجاو لىل NAT نىكمت](#)

[عمدخالاب ةصاخلا VPN ةكبش نم ةرشابم رورم ةكرح](#)

[ققحتلا](#)

[DIA نودب](#)

[DIA عم](#)

## عمدقمل

دنع نىوكتلا لىل ريشي وهو Cisco نم SD-WAN DIA ذيفنت ةيفيك دنتسمل اذه حضوي عرفال هجوم نم ةرشابم تنرتنإل لىل تانايب رورم ةكرح ثودح.

## ةيساسألا تابلطتمل

### تابلطتمل

ةيلاتل عيضاوملاب ةفرعم كيدل نوكت ناب Cisco ي صوت:

- Cisco (SD-WAN) جم انرب نم ةفرعملا ةعساوولا ةقطنملا ةكبش
- (NAT) ةكبشلا ناووع ةمچرت

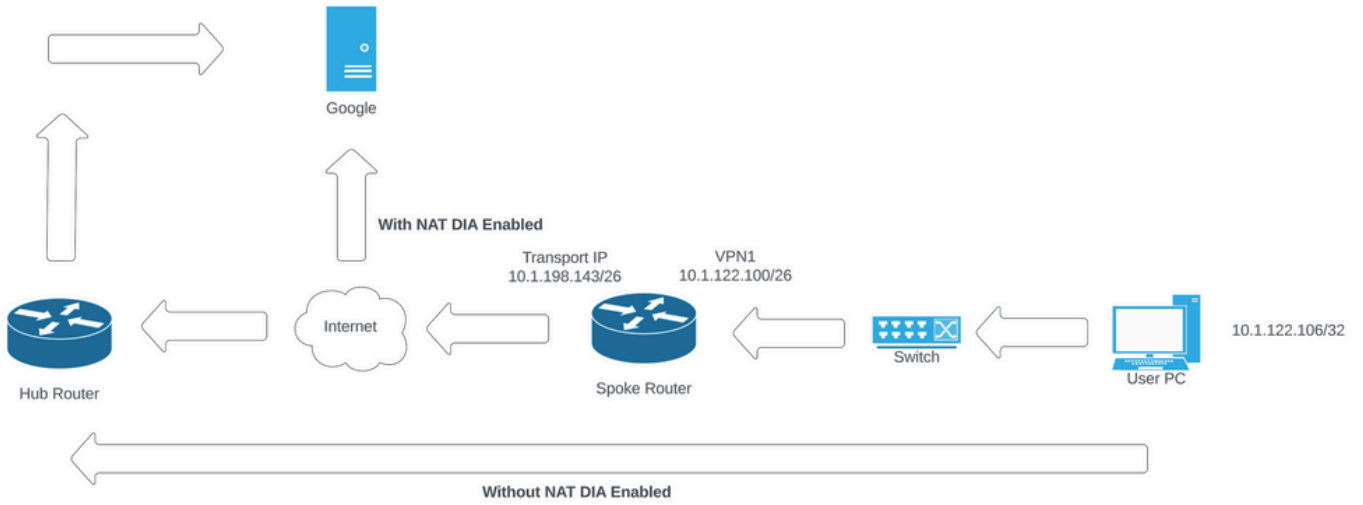
### عمدختسمل تانوكمل

ةيلاتل ةيدامل تانوكمل او جم اربال تارادصل لىل دنتسمل اذه يف ةدراول تامولعمل دنتست:

- Cisco vManage، رادصلال 20.6.3
- Cisco WAN Edge Router 17.4.2

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجال نم دنتسمل اذه يف ةدراول تامولعمل عاشنإ مت تناك اذا. (يضا رتفا) حوسمم نىوكتب دنتسمل اذه يف عمدختسمل ةزهجال عيمج تادب رما يال لم تحملل ريثا تلل كمهف نم دكأتف، ليغشتلا دي قكتك بش.

# ةكبش ل ل يطي طخت ل ا مسر ل ا



ةكبش ل ا ايج ول و ب و ط

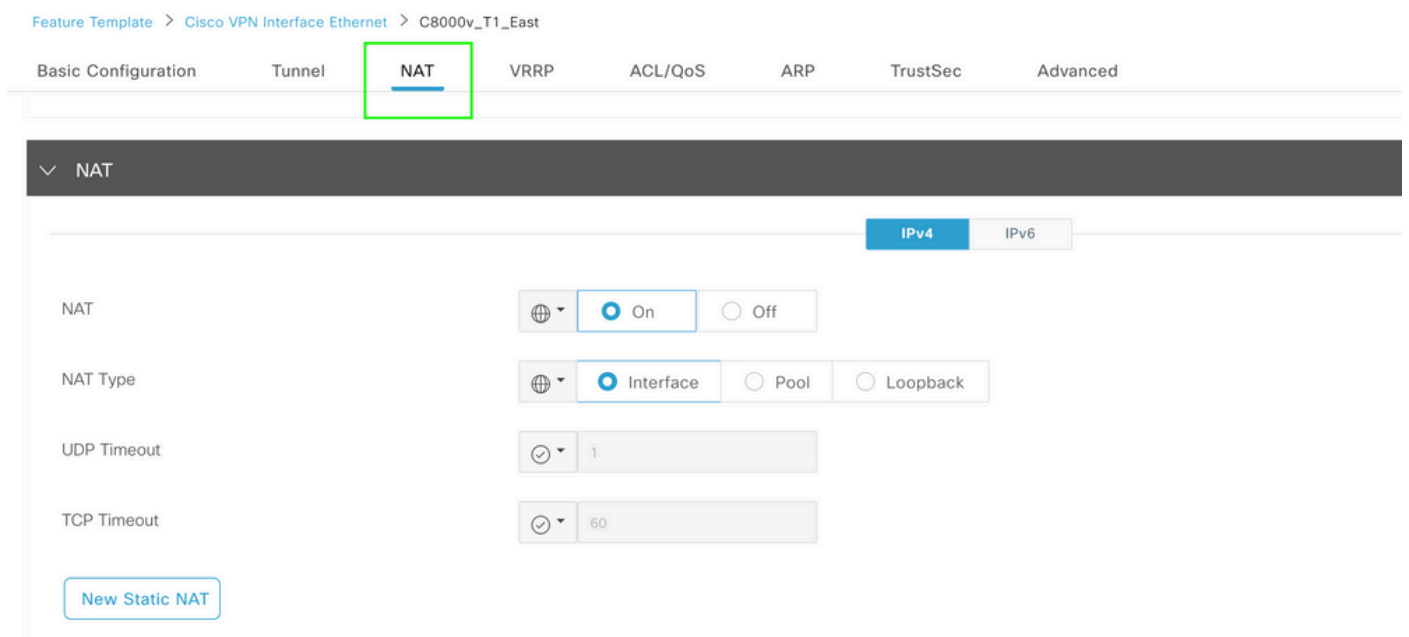
## ن ي و ك ت ل ا

ن ي و ط خ ي ف Cisco SD-WAN ت ا ه ج و م ي ل ع DIA ن ي ك م ت م ت ي :

1. ل ق ن ل ا ة ه ج ا و ي ل ع NAT ن ي ك م ت ب م ق .

2. ة س ا ي س و ا ت ب ا ث ر ا س م م ا د خ ت س ا ب ة م د خ ل ا ب ة ص ا خ ل ا VPN ة ك ب ش ن م ة ر ش ا ب م ر و ر م ة ك ر ح .  
ة ي ز ك ر م ت ا ن ا ي ب .

## ل ق ن ل ا ة ه ج ا و ي ل ع NAT ن ي ك م ت



VPN ة ك ب ش ة ه ج ا و (NAT) ة ك ب ش ب ل ا ق

NAT. رشنن ال ةدام و د ب ي ذل ا ني و ك ت ال ني ك م ت ا ه ب م ت ي ي ت ال ة ق ي ر ط ل ا ي ه ه ذه

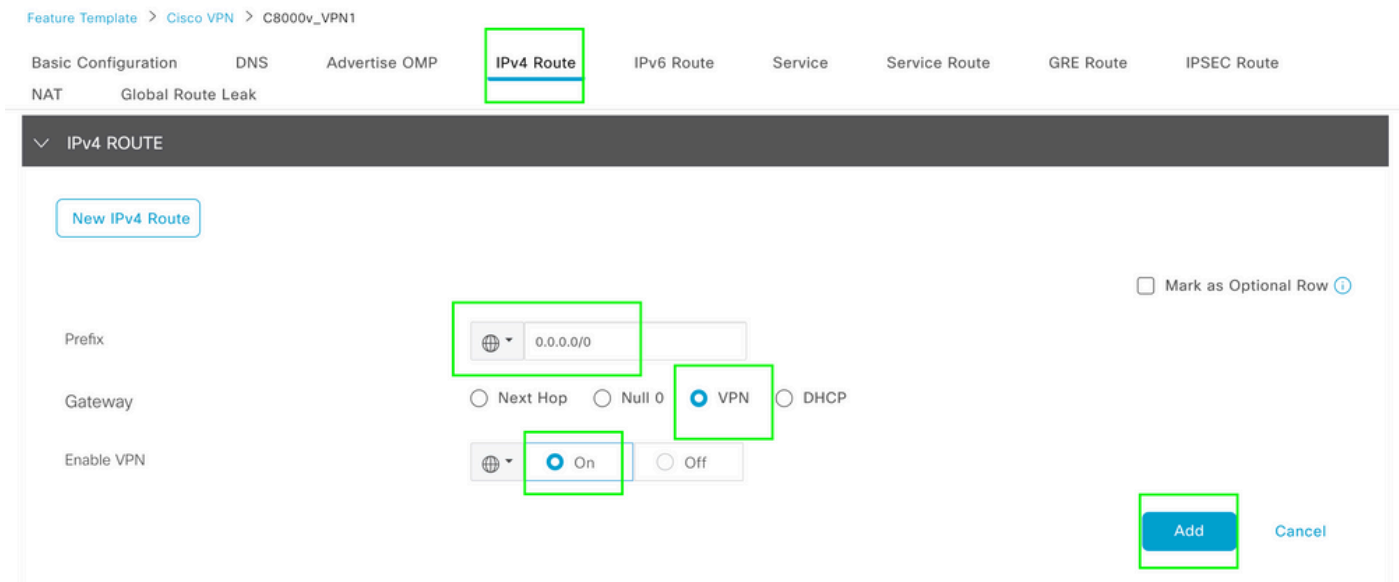
```
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet2 overload
ip nat translation tcp-timeout 3600
ip nat translation udp-timeout 60
```

```
interface GigabitEthernet2
ip nat outside
```

## ةمدخل اب ة ص ا خ ال VPN ة ك ب ش ن م ة ر ش اب م ر و ر م ة ك ر ح

ن ي ت ق ي ر ط ب ا ذ ه ق ق ح ت ي ن ا ن ك م م ل ا ن م و :

1. ةمدخل ال VPN 1 ة ز ي م ب ل ا ق ن م ض ت ب ا ث NAT ر ا س م ا ش ن ا م ز ل ي : ت ب ا ث ال NAT ر ا س م .



IPV4 VPN 1 ر ا س م ب ل ا ق

ن ي و ك ت ال ن م ع ز ج ك ر ط س ل ا ا ذ ه ع ف د م ت ي .

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

2. ة ي ز ك ر م ل ا ت ا ن ا ي ب ل ا ة س ا ي س :

ل و ص و ل ا ب ن ي د د ح م ل ا ن ي م د خ ت س م ل ل ح ا م س ل ا ن ك م ي ش ي ح ب ، ت ا ن ا ي ب ل ا ت ا ئ ا ب ة م ئ ا ق ا ش ن ا ب م ق DIA. ل ل ا ل خ ن م ت ن ر ت ن ا ل ا ل

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

Application		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	<a href="#">Edit</a> <a href="#">Delete</a>	

ةيزك رمللا ةسايس ل ةصصخم ل تانايب ل تاءاب ةمئاق

رورم ةكرح تادب عي طتسي لم عتسم VPN صاخ كلذل ، ةمئاق VPN تقلخ

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

Application		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	<a href="#">Edit</a> <a href="#">Delete</a>	

ةيزك رمللا ةسايس ل ةصصخم ل VPN تاكبش ةمئاق

نعم عقوم ل ع جهن ل قيبطت نكمي شيحب ، عقاوم ةمئاق عاشنا

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

Application		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	<a href="#">Edit</a> <a href="#">Delete</a>	

ةيزك رمللا ةسايس ل ةصصخم عقاوم ةمئاق

عارج ل نبيعت و ردصم ل تانايب ل ةءاب ةقباطم ل صصخم تانايب جهن عاشنا ب مق  
DIA زاي تاج نكمي يتح ، NAT VPN 0 م ادختسال

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)

Actions:

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

Buttons: Cancel, Save Match And Actions

ۆي زك رمل تانا يابل ا ؤ سا يس

ؤ م د خ ل ا ب ن ا ج ن م ج ه ن ل ا ا ذ ه ا ج ت ا ن و ك ي ن ا ب ج ي

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	

ر و ر م ل ا ؤ ك ر ح ت ا ن ا ي ب ؤ د ع ا ق

ۆي زك رمل تانا يابل ا ؤ سا يس ل ؤ ن ي ا ع م ي ه ه ذ ه

```
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>
```

## مع DIA

1. مَدْخَلُ بِنَاجِ يَلْعَقُ نَكْمَمَ الـ NAT DIA يَلْتَلِجُ إِخْرَاجًا إِلَى طَقْتَلِي: تَبَاثُلُ NAT رَاسِم.

```
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#
```

تَنْزِلُ إِلَى لَوْصُولِ 1 مَقْرَرِ (VPN) فِيهِ رَهْاطُ الصَّخْلِ كَبَشَلِي فِي نِيْمَدْخَلِ سَمَلِ نَأَلِ نَكْمِي.

```
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>

NAT تامجرت قحلالا جارخال طقتلي

```
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

ةمزالا هكلس ت نأ بجي يذلا راسملا يلاتلا رمألا طقتلي

```
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. ةيزكرملا تانايبلا ةسايس:

زاهجال ملتسا يذلا جهنلا نم قححتلل WAN Edge زاهج يلع رمألا مادختسا نكمي policy show sdwan policy from-vsmart data-

```
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#

تنترنإلا يلا لوصولا 1 مقرر (VPN) ةيرهاظلا ةصاخلا ةكبشلا يف ني مدختسملل نألا نكمي

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>
```

ةمزلح لك لس ت نأ ب جي يذل راسم ال يلالت ال رمأل طقت لي

```
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
```

NAT تامجرت قحلالا جارخال طقت لي

```
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
```

دادعلا تاداي ز جارخال اذه طقت لي

```
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#
```

ردصم ال نأل ارظن ةادوس ةمئاق ي ف اهعضو مت ي تلل تانا يبل رورم ةكرح جارخال اذه ضبق يلع  
تانا يبل تاءاب ةمئاق يلل يمتني ال IP

```
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#

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت  
ملاعلاء انء مء مء ف ن مء دختسمل معد و تمة مء دقتل ةر شبل او  
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب  
Cisco ةلخت. فرتمة مچرت مء دقء ةل ةل ةفارتحال ةمچرتل عم لاعل او  
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةلصلأل ةزءل ءن إل دن تسمل