

تنرتن إلإ رشابمل ا لوصولا قيبلت ل SD-WAN

تاي وتحمل

ةمدقملا

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكمل](#)

[ةكبشلل يطي طختلا مسرا](#)

[نيوكتلا](#)

[لقنلا ةهجاو لع NAT نيك مت](#)

[ةمدخلاب ةصالخا VPN ةكبش نم ةرشابم رورم ةكرح](#)

[ققحتلا](#)

[نودب DIA](#)

[مع DIA](#)

ةمدقملا

دنه نيوكتلا إلإ ريشي وهو Cisco ذيفنت ةيفيك دنتسملا اذه حضوي عرفلأ هجوم نم ةرشابم تنرتن إلإ لع تانايبل رورم ةكرح ثودح.

ةيساسألا تابلطتملا

تابلطتملا

ةيلاتلا عيضاوملاب ةفرعم كيدل نوكتنأب Cisco يصوت:

- جمانرب نم ةفرعلملا ةعساولا ةقطنملا ةكبش Cisco (SD-WAN)
- ةكبشلا ناونع ةمجرت (NAT)

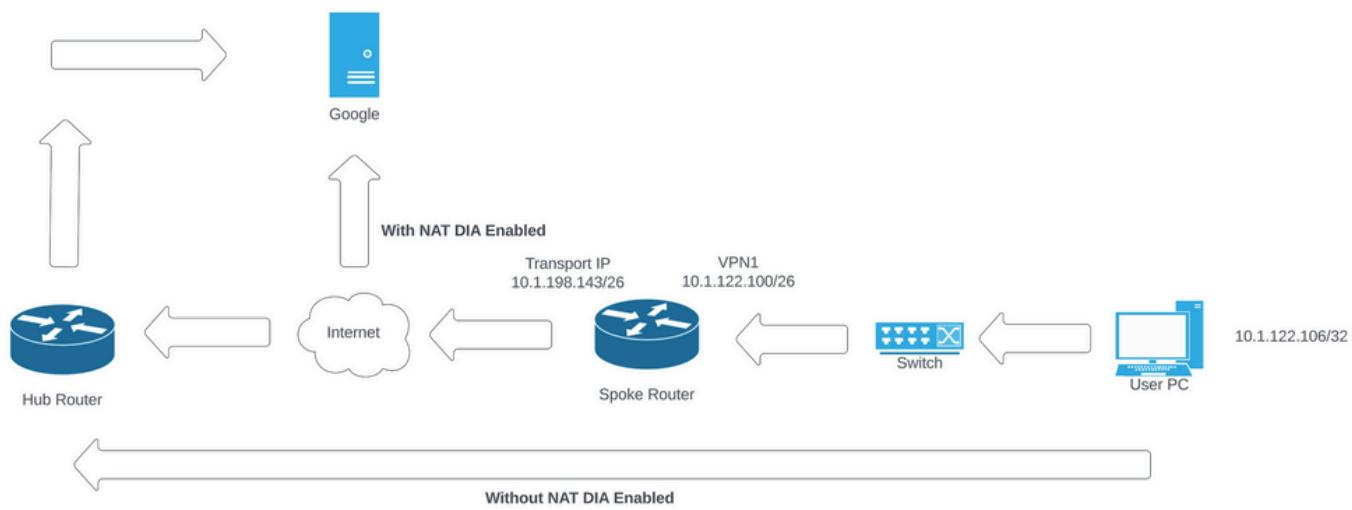
ةمدختسملا تانوكمل

ةيلاتلا ةيダメلا تانوكمل او جماربلا تارادصإ إلإ دنتسملا اذه يف ةدواولالا تامولعمل دنتسست:

- Cisco vManage 20.6.3
- Cisco WAN Edge Router 17.4.2

ةصالخ ةيلمعم ةئيب يف ةدوچوملا ةزهجلأا نم دنتسملا اذه يف ةدواولالا تامولعملاءاشنإ مت تناك اذا .(يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسملا ةزهجلأا عيمج تأدبل رمأ يأ لمحملاريايثأتلل كمهف نم دكأتف ،ليغشتلا ديق كتكبش.

ةكبشلل يطي طختلا مسرلا



ةكبشلا ايجولوبوط

نيوكتل

نیتوطخ یف Cisco SD-WAN تاهجوم ىلע DIA نیکمەت مەتى:

1. لقىللا ۋەجاو ىلع NAT نیکمەت مەق.

2. ئەسايىس و أ تباث راسىم مادختساب ۋەمدىخلىپ ۋەچىلىپ چىخىش نىم ۋەرشابم رورم ۋەرچ. ۋەيىزكىرم تانايىپ.

لقىللا ۋەجاو ىلع NAT نیکمەت

The screenshot shows the Cisco SD-WAN interface for configuring a Cisco VPN Interface Ethernet. The 'NAT' tab is selected. The 'IPv4' tab is active. The 'NAT' section is expanded, showing the following settings:

- NAT: On (radio button selected)
- NAT Type: Interface (radio button selected)
- UDP Timeout: 1
- TCP Timeout: 60

A 'New Static NAT' button is visible at the bottom left.

ةكبش ۋەجاو (NAT) ئەكىپش بىلاق VPN

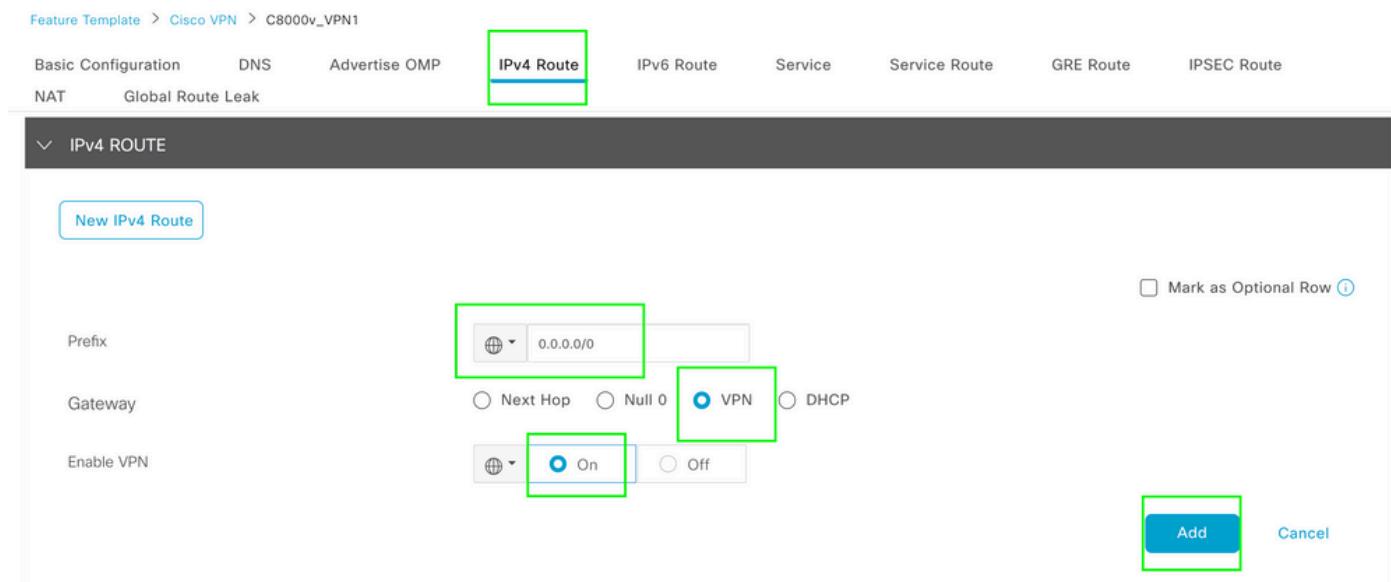
رشنلا ۆدام ودبی يذلا نیوکتلانی کمەت اھب مەتی یتلا ۆقیرطلایە.

```
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
```

ۆمدخلاب ۆصاخلا VPN ۆكبش نم ۆرشابم رورم ۆکرح

نیتقیرطب اذه ققحتی نأ نکمملا نم و:

1. ۆمدخلل 1 VPN ۆزیم بلاق نم ض تباث NAT راسم عاشنامزلي :تباثلاراسم.



راسم بلاق VPN 1 IPv4

نیوکتلانم عزجك رطسلانی اذه عفدا متی.

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

2: ۆيىزكرملاتانايبلانى سايس:

لوصولاب نىدەھملا نىم دختسەملىڭامسىلەن كەمەتىچىپ ، تانايىبلاتايىداب ۆمىئاڭ عاشناب مۇق لالخ نم تىنرتنىلى.

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

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

ةيـزـكـرـمـلـا ةـسـاـيـسـلـلـ ةـصـصـخـمـلـا تـانـاـيـبـلـا تـائـدـاـبـ ةـمـئـاـقـ

رورم ةـكـرـحـ تـأـدـبـ عـيـطـتـسـيـ لـمـعـتـسـمـ VPN صـاخـ كـلـذـلـ ،ـمـئـاـقـ

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

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

ةـيـزـكـرـمـلـا ةـسـاـيـسـلـلـ ةـصـصـخـمـلـا تـاكـبـشـ ةـمـئـاـقـ

نـيـعـمـ عـقـومـ يـلـعـ جـهـنـلـا قـيـبـطـتـ نـكـمـيـ ثـيـحـبـ ،ـعـقـاوـمـ ةـمـئـاـقـ عـاشـنـاـ

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

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

ةـيـزـكـرـمـلـا ةـسـاـيـسـلـلـ ةـصـصـخـمـ عـقـاوـمـ ةـمـئـاـقـ

ءـارـجـإـلـا نـيـيـعـتـوـ رـدـصـمـلـا تـانـاـيـبـلـا ةـئـدـابـ ةـقـبـاطـمـلـ صـصـخـمـ تـانـاـيـبـ جـهـنـ عـاشـنـاـبـ مـقـ

زـايـتـجـاـ نـكـمـيـ يـتـحـ DIAـ NATـ VPNـ 0ـ مـادـخـتـسـالـ

Centralized Policy > Data Policy > Edit Data Policy

Name	DIA
Description	DIA

Custom

Sequence Type: Custom

Sequence Rule: Drag and drop to re-arrange rules

Protocol: IPv4

Match Actions

Source Data Prefix (highlighted)

Actions

Accept Enabled

NAT VPN: VPN ID: 0

Counter Name: DIA

Save Match And Actions

ۆي زکرملە تانايىبلا ۆسايىس

ۆم دخلا بناج نم جەنلە ادھە حاجتى نوکى نا بجي.

Centralized Policy > Edit Policy

Policy Application (highlighted)

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	

رورملە ۆكىح تانايىب ۆدعاق

ۆي زکرملە تانايىبلا ۆسايىسلە ئەنۋاعم يە ھەذە.

```

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
!
!
```

ققحتلا

نودب DIA

مدخلـا بنـاجـىـلـعـ NAT DIAـ نـيـكـمـتـ مـتـيـ الـ اـمـدـنـعـ يـلـاتـلـاـ جـاخـإـلـاـ طـقـتـلـيـ.

```
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#
```

تنـرـتـنـاـ ذـفـنـمـ 1ـ VPNـ يـلـعـ لـمـعـتـسـمـ يـقـلـتـيـ الـ ايـضـارـتـفـاـ.

```
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.

Ping statistics for 8.8.8.8:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

```

C:\Users\Administrator>

مۇ DIA

1. دەخلىا بناجىلۇ ئەنکەممىلا جارخىلا طوقتلىي: تېباتلى NAT DIA راسىم.

```
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 - LISPs
      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#
```

تىنرتنىلا ئىلا لوصولى 1 مقر (VPN) ئىرها ئەظلىا ئەصاخلا ئەكبسلىا يىف نىمىمىلىلى ئەن كەممى.

```
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

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>
```

تامجرت قحاللا جارخإا طقتلي 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
```

ةمزحلا هكلست نأ بجي يذلا راسملاء يلاتلا رمأا 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: ةيذكرملاء تانايبلاء ةسايـس:

نإـف، vSmart، قـيـبـطـتـ إـلـيـ ةـيـذـكـرـمـلـاـ تـانـايـبـلـاـ ةـسـايـسـ عـفـدـ درـجـمـبـ show sdwan policy from-vsmart data-policy زـاهـجـ مـلـتـسـاـ يـذـلـاـ جـهـنـلـاـ نـمـ قـقـحـتـلـلـ WAN Edge نـكـمـيـ.

```
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#
```

تنـرـتـنـ إـلـاـ إـلـاـ لـوـصـولـاـ 1ـ مـقـرـ (VPN)ـ ةـيـرـهـاـظـلـاـ ةـصـاخـلـاـ ةـكـبـشـلـاـ يـفـ نـيـمـدـخـتـسـمـلـلـ نـآـلـاـ نـكـمـيـ.

```
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>

ةمزلجا هكلست نأبجي 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
```

تامجرت قحاللا جارخالا طقتلي 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
```

دادعلالا تادايزجاريلا اذه طقتلي.

```
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#

ردصلالا نأل ارظن ءادوس ةمياق يف اهعض و مت يتلا تانايبلالا رورم ةكرح جارخا اذه ضبق ىلع تانايبلالا تاءداب ةمياق ىلا يمتنى 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#

هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).