

# هجوم ىلع ةمدخل ب ن ا ج ن م ت با ث ل ا NAT ن ي و ك ت Cisco IOS XE SD-WAN

## تايوت حمل ا

---

[ةمدقم ل ا](#)

[ةيساس ال ا تابل ط ت م ل ا](#)

[تابل ط ت م ل ا](#)

[ةمدخت س م ل ا تان و ك م ل ا](#)

[ةيساس ا تام و ل ع م](#)

[ةك ب ش ل ل ل ي ط ي ط خ ت ل ا م س ر ل ا](#)

[ن ي و ك ت ل ا](#)

[cEdge ةسيهت](#)

[Via CLI](#)

[vManage ةزيم ب ل ا ق ل ل ا ل خ ن م](#)

[ةيزك ر م ل ا تان ا ي ب ل ا ةس ا يس](#)

[ةحص ل ا ن م ق ق و ح ت ل ا](#)

[ا و ح ا ل ص ا و ا ط خ ال ا ف ا ش ك ت س ا](#)

[ةل ص ت ا ذ ت ا م و ل ع م](#)

---

## ةمدقم ل ا

ىلع VRF ب ن ا ج ةمدخ ن م و ى ل ا NAT ي ك ي ت ا ت س ا ن ك ا س ز ج ن ي ن ا ل ي ك ش ت ل ا ةق ي ث و ا ذ ه ف ص ي  
cisco IOS-XE® SD-WAN م ا د ي د خ ت ج ا ح س م .

## ةيساس ال ا تابل ط ت م ل ا

ث د ح ا ر ا د ص ا و ا 17.3.1a ر ا د ص ا ل ا ى ل ع Cisco IOS-XE SD-WAN ة ز ه ج ا م ا د خ ت س ا ب ج ي .

## تابل ط ت م ل ا

ةي ل ا ت ل ا ع ي ض ا و م ل ا ب ة ف ر ع م ك ي د ل ن و ك ت ن ا ب Cisco ي ص و ت :

- Cisco (SD-WAN) ن م ج م ا ر ب ل ا ب ة ف ر ع م ة ع س ا و ة ق ط ن م ة ك ب ش
- (NAT) ة ك ب ش ل ا ن ا و ن ع ة م ح ر ت

## ةمدخت س م ل ا تان و ك م ل ا

ةي ل ا ت ل ا ة ي د ا م ل ا تان و ك م ل ا و ج م ا ر ب ل ا ت ا ر ا د ص ا ى ل ا د ن ت س م ل ا ا ذ ه ي ف ة د ر ا و ل ا ت ا م و ل ع م ل ا د ن ت س ت

- 17.6.2 ر ا د ص ا ل ا ISR4451-X/K9

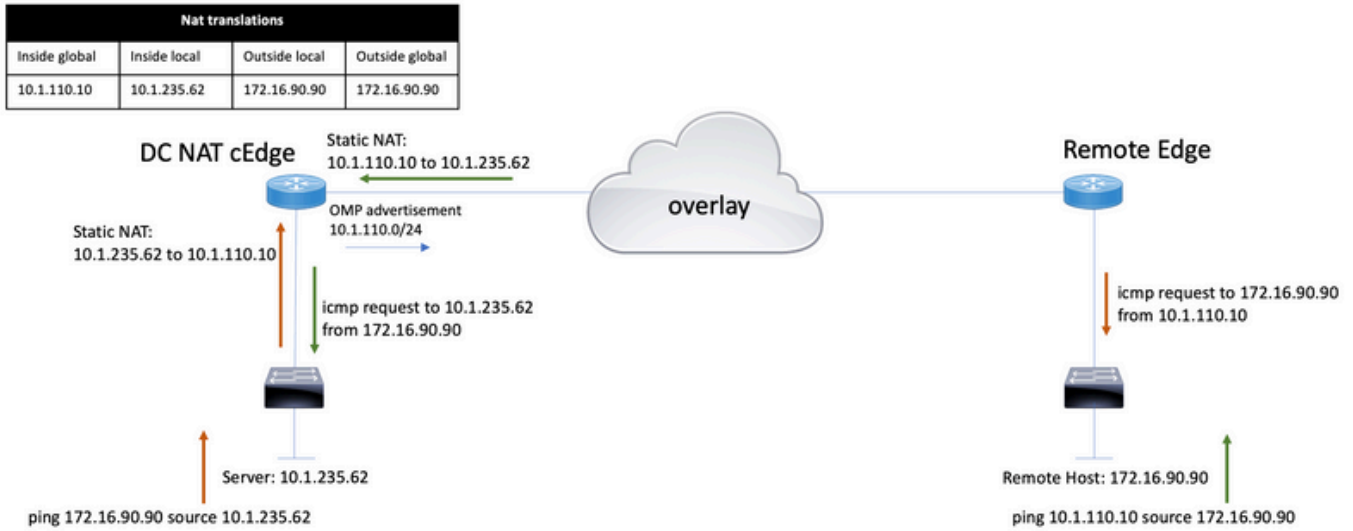
ة ص ا خ ة ي ل م ع م ة ئ ي ب ي ف ة د و ج و م ل ا ة ز ه ج ال ا ن م د ن ت س م ل ا ا ذ ه ي ف ة د ر ا و ل ا ت ا م و ل ع م ل ا ع ا ش ن ا م ت

تنالك اذا (يضا رتفا) حوسمم نيوكتب دنن سمل اذ في م دختس مل ازه جال ا عي مج ت ادب رما يال لم حمل ري ثا تلل كم هف نم دك اتف ، لي غش تل دي ق كت كبش

## ةيساس ا تامول عم

ةكبش لل يطي طختل مسرلا

in order to ايجول و بوط اذ ، ةقي ث و اذ في فص ي nat يكي تات سا نكاس ةمدخل تل لكش . تل م عت سا



ةكبش ل ا هذ نع نال عال متي ال DC ع قو مل ةي لحم و ةصاخ 10.1.235.0/24 ةي عرفل ا ةكبش ل ا متي ، لاصتال ا نم مداوخل ا نكمتت يكل (OMP) تاكبش ل ا ةراد لوكوتورب ي ةي عرفل ا ةي عرفل ا ةكبش ل ا ي ل تباث لكش ب تاكبش ل ا هذ لي صوت

- NAT لى ل cEdge جاتحي ، 172.16.90.90 ب لاصتال ا ادب 10.1.235.62 مداخل ا موق ي ام دن ع لى ل 10.1.110.10
- لى ل بل طلاب موق ي ه ن ا ف ، مداخل ا ب لاصتال ا لى ل 172.16.90.90 في ضمل ا جاتحي ام دن ع لى ل 10.1.235.62 لى ل ةه جولا IP ةم جرت لى ل cEdge جاتحي و ، 10.1.110.10

## نيوكتل

cEdge ةي ةهت

ةزي م بلاق لال خ نم و ا ه جوم ل رما و ال رطس ةه جاو لال خ نم نيوكتل ا اذ ذي فن نكمي vManage.

Via CLI

ةكبش nat ل تل لكش:

```
ip nat pool natpool10 10.1.110.1 10.1.110.253 prefix-length 24
```

ةكرب لماش nat يكي تاتاسا نكاس ي ل خاد تل كش:

```
ip nat inside source list global-list pool natpool10 vrf 10 match-in-vrf
```

ل خ دم nat يكي تاتاسا نكاس لا تل كش:

```
ip nat inside source static 10.1.235.62 10.1.110.10 vrf 10 match-in-vrf pool natpool10
```

vManage ةزيم بلاق لال خ نم

.دي دج NAT عمجت روناو، nat عمجت > NAT مسق ىل لقتنا، ةمدخلل VPN ةزيم بلاق يف

اهاتنا درجمب ةفاضل روناو تاري غتملا ةئبعتب مق:

Basic Configuration	DNS	Advertise OMP	IPv4 Route	IPv6 Route
<b>NAT POOL</b>	PORT FORWARD	STATIC NAT	NAT64 v4 POOL	
<a href="#">New NAT Pool</a>				
NAT Pool Name			<input type="text" value="10"/>	
NAT Pool Prefix Length			<input type="text" value="24"/>	
NAT Pool Range Start			<input type="text" value="10.1.110.1"/>	
NAT Pool Range End			<input type="text" value="10.1.110.253"/>	
NAT Overload			<input type="radio"/> On	<input checked="" type="radio"/> Off
NAT Direction			<input type="text" value="Inside"/>	

يالاتلا وحنلا ىلع عمجتلا عاشنإ نم ققحت

NAT							
NAT POOL	PORT FORWARD	STATIC NAT	NAT64 v4 POOL				
<a href="#">New NAT Pool</a>							
Optional	NAT Pool name	NAT Pool Prefix Length	NAT Pool Range Start	NAT Pool Range End	NAT Pool Overload	NAT Pool Direction	Action
<input type="checkbox"/>	<input type="text" value="10"/>	<input type="text" value="24"/>	<input type="text" value="10.1.110.1"/>	<input type="text" value="10.1.110.253"/>	<input type="radio"/> Off	<input type="text" value="Inside"/>	<a href="#">Edit</a> <a href="#">Delete</a>

نكاس ديدج رزلا ةقطقو nat يكي تاتسإ نكاس ىلإ حفصت ،نوكي ةكرب تقلخ نإ ام nat يكي تاتسإ

اهئاتنا درجم ةفاضل رقناو تاريختملا ةئبعتب مق

▼ NAT

NAT POOL
PORT FORWARD
STATIC NAT
NAT64 v4 POOL

New Static NAT

Mark as Optional Row i

NAT Pool Name	🌐	10	▼
Source IP Address	🌐	10.1.235.62	
Translated Source IP Address	🌐	10.1.110.10	i
Static NAT Direction	🌐	Inside	▼

Add
Cancel

## ةيزك رمل تانايب لة سايس

ىل ةبول طمل تائادابل عم تانايب ل رورم ةكرح هيجوتل ةيزك رمل تانايب ةسايس ل ةجاح كانه ةمدخل ب ناج نم NAT.

عقاوم لة ةمئاقو VPN ةكبش ديدحت:

```

policy
lists
vpn-list VPN-10
vpn 10
!
site-list CEDGE
site-id 30
!

```

جراخل لىل لخدال نم ةمجرتلل لسلست لوأ ديدحت ب مق:

```

<#root>

data-policy _VPN-10_Data_NAT_cEdge
vpn-list VPN-10
sequence 1
match

source-ip 10.1.235.62/32

```

```
!  
action accept  
  count nat_cedge_-1665659624  
  nat pool 10  
!  
!
```

رورم لة كرح ادب دنع هم ادختس ا متي . ةه جولا ناو نع ةم جرتل يلاتل لس لس تال مادختس ا متي  
لخادل الى جراخل نم:

<#root>

```
sequence 11  
match
```

```
destination-ip 10.1.110.10/32
```

```
!  
action accept  
  count nat_cedge_out2in_-1665659624  
  nat pool 10  
!  
!  
default-action accept  
!  
!
```

تاهاجتال لك في ةسايسال قيبطت:

```
apply-policy  
site-list CEDGE  
  data-policy _VPN-10_Data_NAT_cEdge all
```

## ةحصلال نم ققحتال

رماً قيقدتال عم ليكشت nat ل نم ةلودل تقود.

```
show sdwan policy from-vsmart  
show ip nat translations  
sdwan policy data-policy-filter
```

172.16.90.90 فيضمال الى 10.1.235.62 مداخلال نم لاصتال رابتخال:

```
cEdge#show ip nat translations
Pro  Inside global  Inside local  Outside local  Outside global
---  10.1.110.10    10.1.235.62  ---           ---
icmp 10.1.110.10:0  10.1.235.62:0 172.16.90.90:0 172.16.90.90:0
Total number of translations: 2
```

10.1.110.10 مداخل إلى 10.90.90.90 فيض من لاصت ال رابتخا

```
cEdge#show ip nat translations
Pro  Inside global  Inside local  Outside local  Outside global
---  10.1.110.10    10.1.235.62  ---           ---
icmp 10.1.110.10:8299 10.1.235.62:8299 172.16.90.90:8299 172.16.90.90:8299
Total number of translations: 2
```

## اهح ال صا وء اطخال ا فاشك ت سا

تانا ب ال جهن تادادع لىع مزحلا ةدايز نم ققحت ل

<#root>

```
cEdge#show sdwan policy data-policy-filter
data-policy-filter _VPN-10_Data_NAT_cEdge
data-policy-vpnlist VPN-10
data-policy-counter default_action_count
packets 1412
bytes 109382
```

```
data-policy-counter nat_cedge_-1665659624
```

```
packets 154
```

```
bytes 16852
```

```
data-policy-counter nat_cedge_out2in_-1665659624
```

```
packets 7
```

```
bytes 886
```

ةلص تاذا تامولعم

- [17.x رادصإلا، Cisco SD-WAN NAT، Cisco IOS XE نڤوكت لڤلد](#)



ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت  
ملاعلاء انء مء مء نمة 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 تامچرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةلصلأل ةزءل ءنل دن تسمل