

# هنا ققحتل او Nexus ىل NAT نيوكت

## تاوت حمل

### مدم حمل

nat نيترمو (NAT) مخرت ناونع كيش تقودو لكشي نا فيك قيثو اذه فصوي

### سياس الابلط حمل

#### تابلط حمل

سيالاتل عيضاوم لابل مفرعم كيدل نوكت ناب Cisco ي صوت

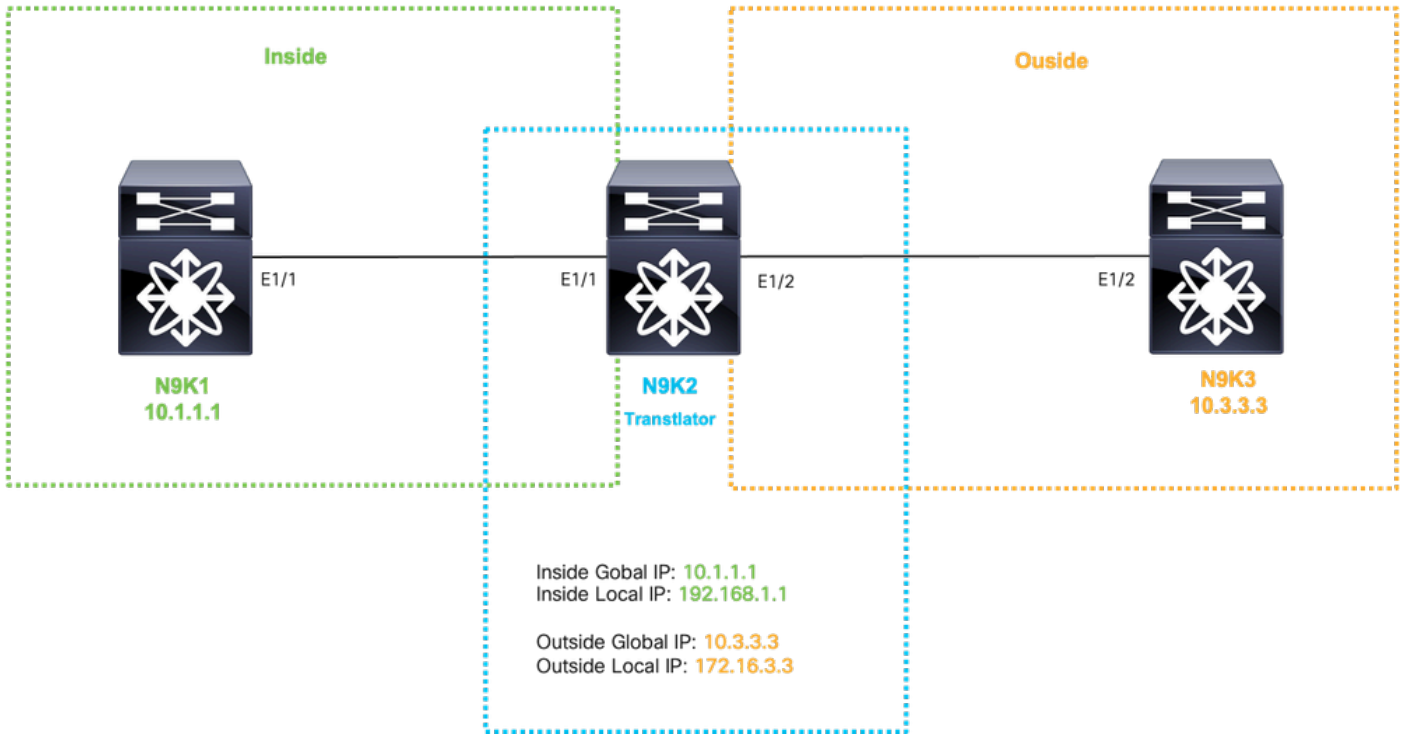
- nat
- NXOS ياساس الماظنل
- رزيلاناثي ال م ه ف

#### مدمخ تسمل تانوك حمل

| مس ال | مروف تابل       | رادص ال |
|-------|-----------------|---------|
| N9K1  | N9K-C93108TC-EX | 9.3(10) |
| N9K2  | N9K-C93108TC-EX | 9.3(10) |
| N9K3  | N9K-C93108TC-EX | 9.3(10) |

صاخ قيلمعم قئيب في دوجومل ازه ال نم دنتسمل اذه في دراوول تامولعمل عاشن ا مت  
ت ناك اذ. (يضا رتفا) حوسمم نيوكت ب دنتسمل اذه في مدمخ تسمل ازه ال عيمج ت ادب  
رم ا ل حمل ريثا تلل كم ه ف نم دك ات ف ، ليغش تل دي ق ك تك ب ش

#### كيش لل يطيختل مسرل



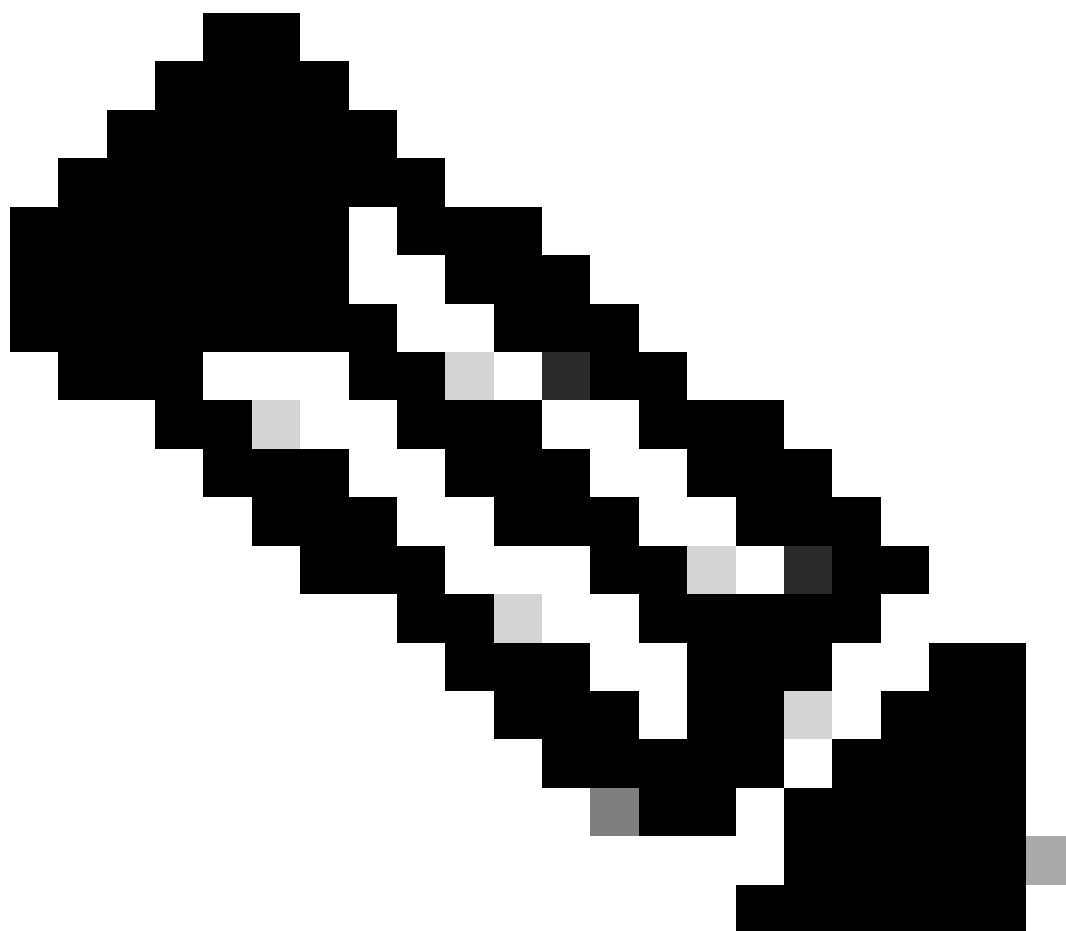
## IP لخاد ةمومع الةم جرت ال ني وكت

خاد Global IP:10.1.1.1

خاد IP لةم ال:192.168.1.1

| N9K1   | N9K2   |
|--|--|
| <pre>interface Ethernet1/1 ip address 10.10.10.10/24 no shut  interface loopback 0 ip address 10.1.1.1/32  ip route 0.0.0.0/0 10.10.10.1</pre> | <pre>feature nat  ip access-list tac-nat-inside permit ip host 10.1.1.1 any  ip nat pool tac-nat-inside-pool 192.168.1.1 192.168.1.1 prefix-length 32 ip nat inside source list tac-nat-inside pool tac-nat-inside-pool dynamic  interface Ethernet1/1 ip nat inside ip address 10.10.10.11/24 no shut  interface Ethernet1/2 ip nat outside ip address 10.20.20.21/24 no shut  ip route 10.3.3.3/32 10.20.20.20  ip route 10.1.1.1/32 10.10.10.10</pre> |

|  |  |
|--|--|
|  |  |
|--|--|



Nexus ل نوكي نأ بجي ،زاهج يألعلع ايلع ف دوجوم ريغ 192.168.1.1 IP نأ امب :ةظحالم  
راسم ل اخدا نيوكت نكمي . IP اذه ل اناي بل رورم ةكره هجوت ةداعل حل اص راسم  
راسم عاشن اب ايئاق لت Nexus موقوي . nat ةمئاق ةياهن يف "راسم ةفاضل" يودي تباث  
مجرتم ل ريغ IP نم ةيلات ل ةوطخل ل اريشي يذل مجرتم ل IP وحن

IP ل خاد ةمجرتم ل ةيمومع نم ققحت ل

N9K1

```
ethalyzer local interface inband display-filter icmp limit-captured-frames 0
Capturing on inband
1 2023-09-09 00:34:03.617811110 10.3.3.3 → 10.1.1.1 ICMP 158 Echo (ping) request id=0xd923, seq=0/0, ttl=254
```

10.1.1.1 إلى هجوم الة مخرج الة مزل الة N9K1 ملت سي

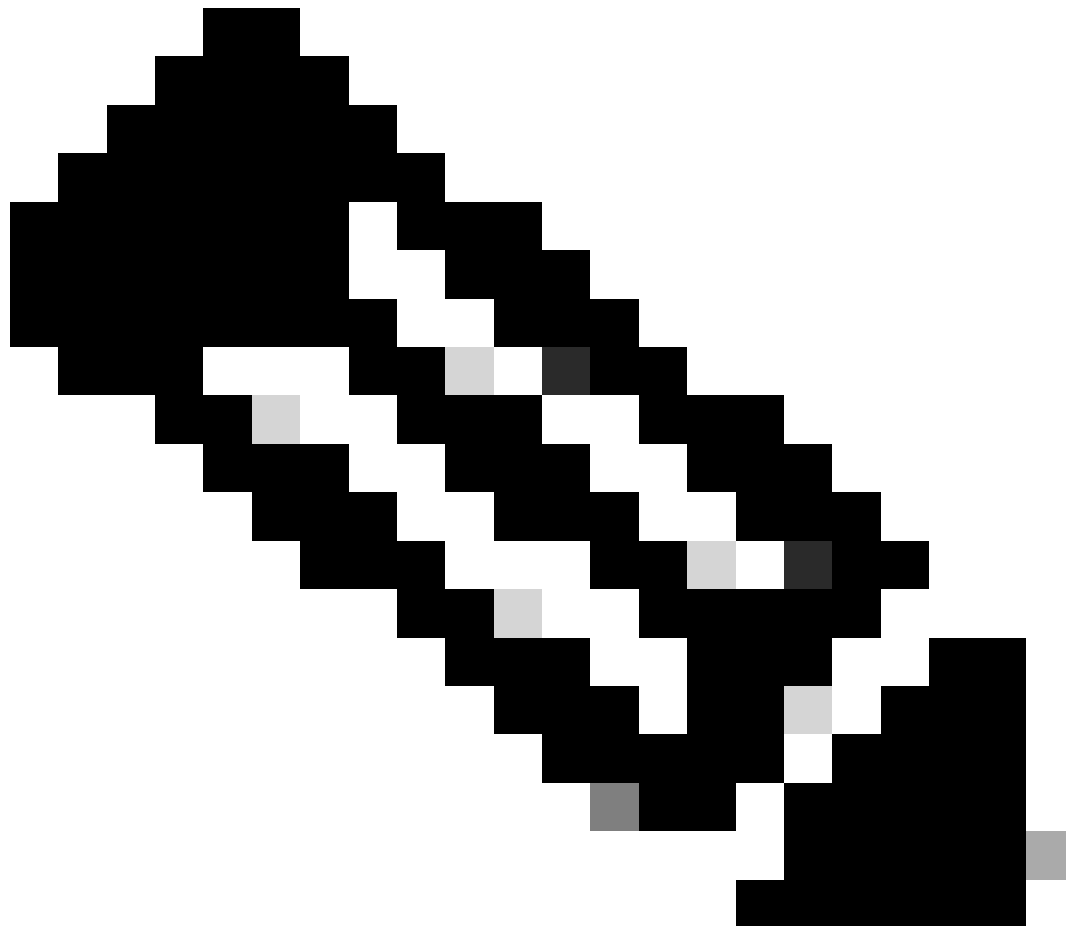
## جراخ ي مومع الة IP نم ة مخرج الة نيوكت

جراخ الة IP: 10.3.3.3

جراخ الة IP: 172.16.3.3

| N9K1  | N9K2   |
|---|--|
| <pre>interface Ethernet1/1   ip address 10.10.10.11/24   no shut  interface loopback 0   ip address 10.1.1.1/32  ip route 0.0.0.0/0 10.10.10.11</pre> | <pre>feature nat  ip access-list tac-nat-outside permit ip host 10.3.3.3 any  ip nat pool tac-nat-outside-pool 172.16.3.3 172.16.3.3 prefix-length 32 ip nat outside source list tac-nat-outside pool tac-nat-outside-pool dyna  interface Ethernet1/1   ip nat inside   ip address 10.10.10.11/24   no shut  interface Ethernet1/2   ip nat outside   ip address 10.20.20.21/24   no shut  ip route 10.3.3.3/32 10.20.20.20  ip route 10.1.1.1/32 10.10.10.10</pre> |

|  |  |
|--|--|
|  |  |
|--|--|



Nexus ل نوكي نأ بجي ، زاهج إي لعل اي لعف دوجوم ريغ 172.16.3.3 IP نأ أمب :ةظحالم راسم لاخذإ نيوكت نكمي . اذه IP لىل اتانايلال رورم ةكرح هي جوت ةداعإل حل اص راسم IP وحن راسم عاشنإب Nexus موقوي . nat ةمئاق ةياهن يف "راسم ةفاضإ" يودي تباث مجرتملا ريغ IP نم ةيلاتلا ةوطخلال لىل ريشي يذلا مجرتملا

## جراخ ي مومعلا IP نم ةمجرتلا نم ققحتلا

| N9K1                            | N9K2                   |
|---------------------------------|------------------------|
| ping 172.16.3.3 source 10.1.1.1 | sh ip nat translations |

|   |   |
|---|---|
| <pre>PING 172.16.3.3 (172.16.3.3) from 10.1.1.1: 56 data bytes 64 bytes from 172.16.3.3: icmp_seq=0 ttl=253 time=1.103 ms</pre> | <pre>Pro Inside global      Inside local      Out any ---                ---                172  show ip route 172.16.3.3 172.16.3.3/32, ubest/mbest: 1/0 via 10.20.20.20 [1/0], 00:48:06, NAT</pre>  |
| <p>يچراخ IP لى لاصتا رابتخا ئىيەتەب N9K1 موقت 172.16.3.3.</p>   | <p>(192.168.3.3) يچراخ IP لى لاصتا رابتخا ئىيەتەب N9K2 موقت (10.3.3.3).</p> <p>ءاشنا مەتەي "راسمە فاضىل" رمال مادختساب ايئاقلىت</p> <p>نەخس، طوقف يچراخ نىوكتەب Nexus نال ارظن طوقف يچراخ لى لاصتا رابتخا ئىيەتەب N9K1 موقت 172.16.3.3.</p> |

## nat (نىتەرم) چراخ/لخاد مەچرتلىل يملال IP ناوئە نىوكتە

چراخ IP لى لاصتا رابتخا ئىيەتەب N9K1 موقت 10.3.3.3

چراخ IP لى لاصتا رابتخا ئىيەتەب N9K2 موقت 172.16.3.3

لخاد Global IP: 10.1.1.1

لخاد IP لى لاصتا رابتخا ئىيەتەب N9K2 موقت 192.168.1.1

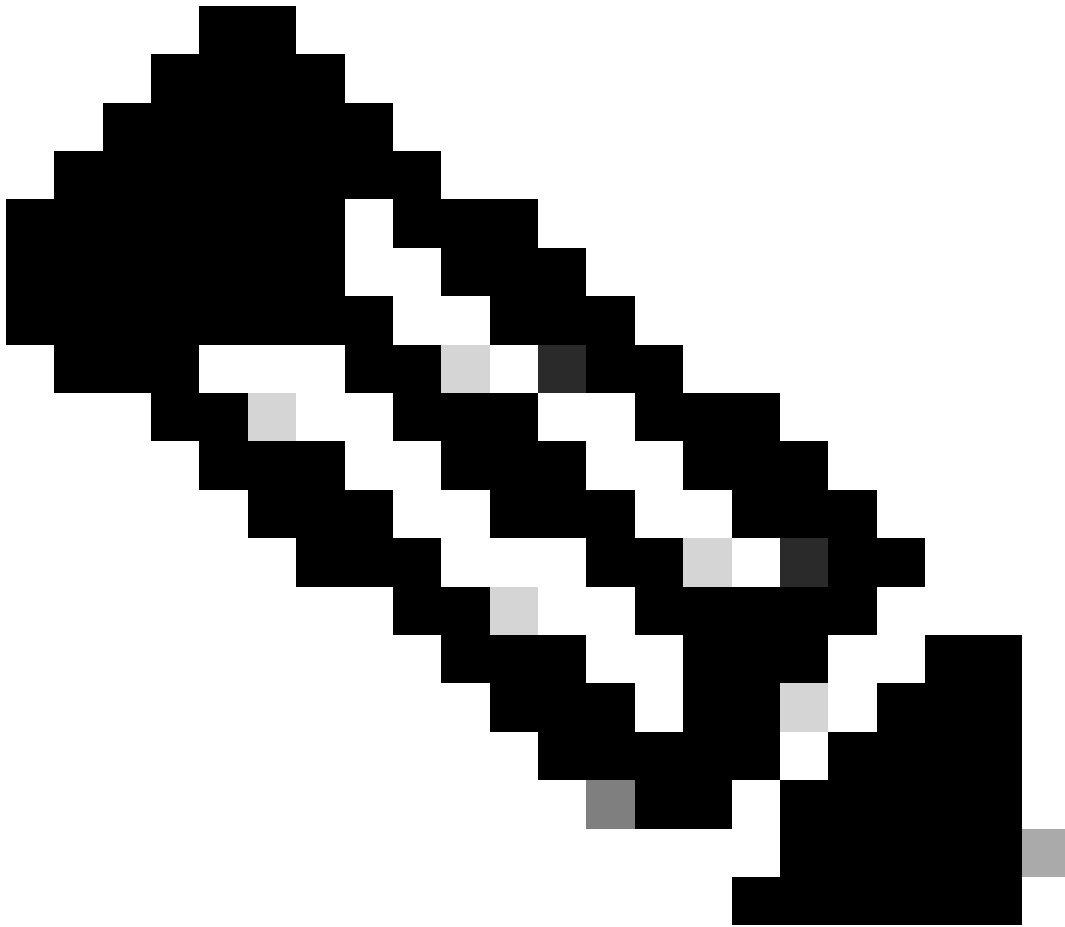
| N9K1  | N9K2  |
|---|---|
| <pre>interface Ethernet1/1   ip address 10.10.10.11/24   no shut  interface loopback 0   ip address 10.1.1.1/32  ip route 0.0.0.0/0 10.10.10.11</pre> | <pre>feature nat  ip access-list tac-nat-outside permit ip host 10.3.3.3 any  ip access-list tac-nat-inside permit ip host 10.1.1.1 any  For Outside Twice translation nexus need 2 source list, one static Inside Both of them needs to match the same group.  ip nat pool tac-nat-outside-pool 172.16.3.3 172.16.3.3 prefix-length 32 ip nat outside source list tac-nat-outside pool tac-nat-outside-pool group 2 ip nat inside source static 10.1.1.1 192.168.1.1 group 2 dynamic add-route  For Inside Twice translation nexus need 2 source list, one static Outside Both of them needs to match the same group.  ip nat pool tac-nat-inside-pool 192.168.1.1 192.168.1.1 prefix-length 32 ip nat inside source list tac-nat-inside pool tac-nat-inside-pool group 1 ip nat outside source static 10.3.3.3 172.16.3.3 group 1 dynamic add-route</pre> |

```
interface Ethernet1/1
  ip nat inside
  ip address 10.10.10.11/24
  no shut

interface Ethernet1/2
  ip nat outside
  ip address 10.20.20.21/24
  no shut

ip route 10.3.3.3/32 10.20.20.20

ip route 10.1.1.1/32 10.10.10.10
```



نأ بجي، زاهج يأل ع ايل عف ني دوجوم ريغ 192.168.1.1 و 172.16.3.3 IP نأ أمب: ةظحالم نيوكت نكمي. IP اذه لئان ايل رورم ةكره هيجوت ةداعل حل اص راسم Nexus ل نوكتي ائاقولت Nexus موقوي. nat ةمئاق ةيانه في "راسم ةفاضل" يودي تباث راسم لاخذل. مچرتم ل ريغ IP نم ةيلال ةوطخل لئان ريشي يذل مچرتم ل IP وحن راسم ديحتب.

## nat (نېتروم) IP جراخ/لخاد لماش ةمچرت تقود

N9K1

```
ethalyzer local interface inband display-filter icmp limit-captured-frames 0
```

```
Capturing on inband
```

```
1 2023-09-09 00:34:03.617811110 172.16.3.3 → 10.1.1.1 ICMP 158 Echo (ping) request id=0xd923, seq=0/0, ttl=2
```

10.1.1.1 ىل ةهجوم ةمچرت مزمح ملتسي N9K1 .



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 تامةرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةلصلأل ةزءل ءنل دن تسمل