

# امدنع اهحالص او IP ردصم عاطخأ فاشكتسأ لقنلا ةكرش يه Verizon نوكت

## تايوتحمل

[عمدقمل](#)

[قيساس الابلطتمل](#)

[تابلطتمل](#)

[عمدختسمل تانوكمل](#)

[قيساس تامولعم](#)

[قلكشم](#)

[مجمولاب قلصتمل اقيطم نلا P-5GS6-GL ةدحو يف قلكشم مل افاشكتا](#)

[مجمولاب قلصتم P-5GS6-GL ةدحو ل](#)

[مجمولاب رورمل اكرحل \(ACL\) لوصول يف مكحتل اقيم: اق 1: رايخل](#)

[مجمولاب رورمل اكرحل nat: اق 2: رايخل](#)

[مجمولاب رورمل اكرحل IPsec نيوكت ذي فن: اق 3: رايخل](#)

[مجمولاب رورمل اكرحل ذي فن: اق 4: رايخل](#)

[مجمولاب رورمل اكرحل IP ردصم كاهتنا CG522-E](#)

## عمدقمل

نوكت Verizon امدنع رركتم رادصل نوكتي ا كاهتنا ردصم ip رحتي نا فيك ةقيثو اذه فص ي لقنلا.

## قيساس الابلطتمل

### تابلطتمل

ةيلاتل اقيضاوملاب قيساس ا ةفرعم كيدل نوكت ناب Cisco ي صوت

- 5G ةيولخل اكبشلا تايساس ا
- Cisco نم 522-E يولخل ا فتاهل ا ةرابع
- Cisco P-5GS6-GL ةدحو
- Cisco نم IOS-XE
- Cisco نم IOS-CG

### عمدختسمل تانوكمل

ةيلاتل اقيداملا تانوكمل او جماربال ا رادصل ا دننتسمل اذه يف ةدراول تامولعمل دننتس

- 17.9.5a رادصل ا IOS-CG عم 522-E ل اوخل ا ةرابع
- P-5GS6-GL ةدحو لي صوت عم 17.9.5 رادصل ا IOS-XE عم IR1101

ةصاخ ةي لمعم ةئي ب ي ف ةدوجوم ل ةزهجال نم دنتسمل اذ ف ةدراول تامولعمل اءشن ا م تناك اذا .(يضا رتفا) حوسم نيوك تب دنتسمل اذ ف ةمدختسمل ةزهجال عيمج ت ادب رما يال لمحتحمل ري ثاتلل كمهف نم دكأتف ، ليغشتل دي ق ك تكبش

## ةيساس ا تامولعمل

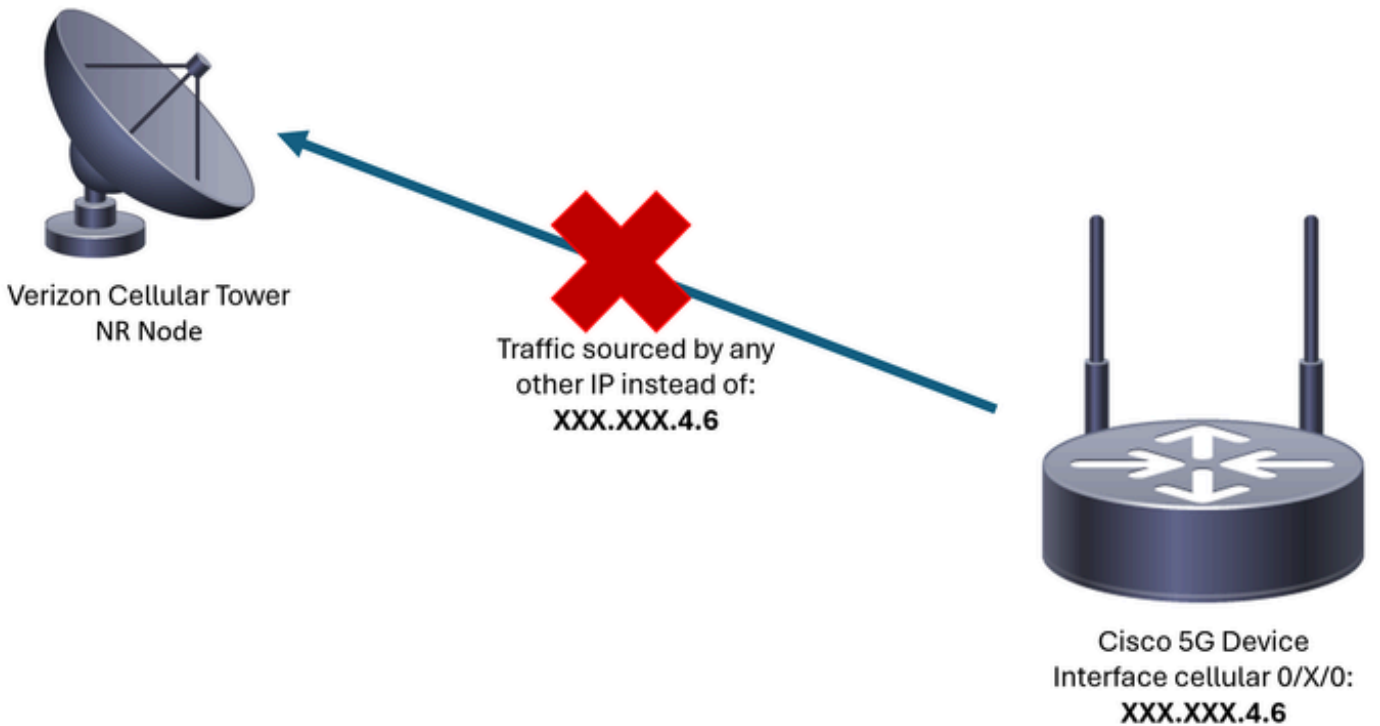
ا ، لقتسمل ا عضول ا ي ف هجومب ةلصتم P-5GS6-GL ةئفلا نم مكحت ةدحو ل ع اذ قبطني قبطني ال . SD-WAN ةطساوب رادم مكحت ةدحو عضو ا لقتسم عضو ي ف CG522-E مكحت ةدحو ةغايص نال ارطن SD-WAN ي ف هجومب ةلصتم P-5GS6-GL ةي طمن ةدحو ل ع دنتسمل ا اذ ةفلتخم رمال

## ةلكشملا

امئاد ع قوتتو ، SIM ةقاطب/ل ي مع ل كل صاخ لكشب IP ناو نع ني يعتب Verizon موقت طقف IP نم اه ل ع لوصحل ا متي يتل ا تانا يبال رورم ةكرح ل ا بقتسا

ip اهرصم نو كي نو بزل ا نم لسري رورم ل ةكرح ا Verizon فشتك ي ام دن ع كاهتنا رصم عقي اقباس ني عي وه نم فلتخم

ناو نع نم رورم ةكرح Verizon ملتستو ، IP xxx.xxx.4.6 ناو نع ني يعت مت اذا ، ل ا ثمل ا ل ي بس ل ع ةدوجوم ةلكشملا ن ا ف ، IP xxx.xxx.8.9



ةكبشلا ل ا ل ي صول ل ا ، فلتخم ناو نع عم ةادال ا نم طبر 10 نم رثك ا Verizon ملتسي ةرم ل منكم ي و ، يولخل ا زاوجل ا نم دي دج ل اصتا ادب متي ، ك لذل ةجيتنو . ف قوت ي و فر فري ةيولخل ا ةمدخل ا ل ع دمتعي وهف . دي دج ناو نع ا قباسلا نم رثك ا هسفن IP ناو نع ل ع لوصحل ا ةبستكمل ا

## هجوم لاب ةلصتم لال ةيظمن لال P-5GS6-GL ةدحو ي ف ةلكشمل ل فاشتك

ي ف رصم لال كاهتنا نوكي، رمأل ا جارخا ي ف ادوجوم رهاظلا لاصتال عطق ببس نوكي ام دنع  
هعضوم:

```
<#root>
```

```
isr#
```

```
show cellular 0/X/0 call-history
```

```
*  
*
```

```
[Wed May 8 18:46:26 2024] Session disconnect reason = Regular deactivation (36)
```

```
*  
*
```

ةمزح طاقتلال نكمي، (تقؤم لال نزخم لال ةي لمع ببسب) تامولعم قباسل لال جارخال رفوي مل اذا  
ةي لال رمأل لال مادختساب NetFlow:

```
isr#conf t  
isr(config)#flow record NETFLOW_MONITOR  
isr(config-flow-record)#match ipv4 protocol  
isr(config-flow-record)#match ipv4 source address  
isr(config-flow-record)#match ipv4 destination address  
isr(config-flow-record)#match transport source-port  
isr(config-flow-record)#match transport destination-port  
isr(config-flow-record)#collect ipv4 source prefix  
isr(config-flow-record)#collect ipv4 source mask  
isr(config-flow-record)#collect ipv4 destination prefix  
isr(config-flow-record)#collect ipv4 destination mask  
isr(config-flow-record)#collect interface output  
isr(config-flow-record)#exit
```

```
isr(config)#flow monitor NETFLOW_MONITOR  
isr(config-flow-monitor)#cache timeout active 60  
isr(config-flow-monitor)#record NETFLOW_MONITOR  
isr(config-flow-monitor)#exit
```

```
isr(config)#interface cellular 0/X/0  
isr(config-if)#ip flow monitor NETFLOW_MONITOR output  
isr(config-if)#exit
```

طاقتلال نم جاتنال لال يري نأ:

```
<#root>
```

```
isr#
```

```
show flow monitor NETFLOW_MONITOR cache format table
```

رمال مادختساب زاهجلا لىل Verizon نم ني عم ل IP ناو نع ةيؤر نكمي

```
<#root>
```

```
isr#
```

```
show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0/0	unassigned	YES	NVRAM	administratively down	down
FastEthernet0/0/1	unassigned	YES	unset	down	down
FastEthernet0/0/2	unassigned	YES	unset	down	down
FastEthernet0/0/3	unassigned	YES	unset	down	down
FastEthernet0/0/4	unassigned	YES	unset	down	down
Cellular0/1/0	IP_address	YES	IPCP	up	up
Cellular0/1/1	unassigned	YES	NVRAM	administratively down	down
Async0/2/0	unassigned	YES	unset	up	down
Vlan1	unassigned	YES	unset	up	down

دحاولا نم فل تخم ناو نع عم sourced نا نع غلبأ وه، رورم ةكرح يلىل NetFlow نم log لىل في نإ رضاح كاهتنا ردصملا. نراق ةيولخلال في تبتثي

## هجوم بةلصتم P-5GS6-GL ةدحول ل

متي يذلا IP ةطساوب طقف ردصملا نم اهلاسرإ متي رورملا ةكرح لك نا نم دكأتلا وه فدهلا لىل اهذيفنت دمتعيو. فدهلا اذقحت ةفل تخم بيلاسأ كانهو. Verizon لبق نم هنييت لىل ةكشلاورشنلا تابلطتم:

- ةرداصلال رورملا ةكرحل (ACL) لوصولال في مكرحتلال ةمئاق: 1 رايخلال
- متي يلىل رورملا ةكرح نا نم دكأتلال كنكمي، لوصولال في مكرحتلال ةمئاق مادختساب Verizon ب صاخلا IP ناو نع نم طقف اهلىل لوصولال متي زاهجال نم اهلاسرإ

```
isr#conf t
isr(config)#ip access-list extended 196
isr(config-ext-nacl)#permit ip host <IP_Assigned_by_Verizon> any
isr(config-ext-nacl)#deny ip any any
isr(config-ext-nacl)#exit

isr(config)#interface cellular 0/X/0
isr(config-if)#ip access-group 196 out
isr(config-if)#end
```

## • ةي لخدال رورم لة كرح ل nat: 2 راي خال

### • تابل طتم ل هذ ب افول ا ب جي:

1. "ip nat outside" انا لى لة ولخال ة هاولا نيوك ت مت .
2. "ip nat inside" انا لى لة هاولا نيوك ت مت .
3. تم جرت اضي انا يم لك لذل (برض) دياز لمح nat تقب ط .
4. متيس يتل رورم لة كرح دي دحت ل (ACL) لوصول ا يف مكحت لة ة مئاق مادخت سا . NATed ا هدي دحت .

ن نيوك ت ل لاثم:

```
<#root>
```

```
isr#conf t
```

```
isr(config)#interface cellular 0/X/0
isr(config-if)#ip nat outside
isr(config-if)#exit
```

```
isr(config)#interface vlan 6
isr(config-if)#ip nat inside
isr(config-if)#exit
```

```
isr(config)#access-list 20 permit <IPv4_subnet_to_be_NATed> <wildcard>
isr(config)#ip nat inside source list 20 interface cellular 0/1/0 overload
```

## • رخا ق فن نيوك ت ي ا و IPsec نيوك ت ذي فن ت: 3 راي خال

- رورم ة كرح لك نا ام ب Verizon. نم ني عم ل IP نا ونع مادخت ساب ق فن ل ا ذه لمع متي ادب ا ري غ تي ال ا ج را خال IP نا ونع ن ا ف، ا ه ل خاد ل ق ت ن ت

## • ق ي رط ة ط ي رخ ذي فن ت: 4 راي خال

- متي ثي ح ب راسم لة ط ي رخ ذي فن ت ن ك مي، ه ج و م ل ل ا ه و ا ش ن ا مت رورم ة كرح ك ا ن ه ت ن ا ك ا ذ ا ب ل ا ص ت ا ل ا ر ا ب ت خ ا ر م ت س ي، ل ا ث م ل ا ل ي ب س ي ل ع . ج ي ح ص ل ك ش ب رورم لة كرح ر ي ف و ت ل و ص ح ل ا م ت ي ي ت ح ر ا س م ة ط ي ر خ ذي فن ت ن ك م ي و، "ت ن ر ت ن ا ل ا ل ا ص ت ا" د و ج و ن ا م ص ل DNS، ج ي ح ص ل ك ش ب رورم لة كرح ي ل ع .

ج ا ح س م ي ل ل ا ط ب ر ي ة ي ط م ن ة د و ح o c i s c o P - 5 G S 6 - G L ي ف ك ا ه ت ن ا ر د ص م ي ر ح ت ي ن ا ع ا ر ج ا ل ا ي ه ن ي ا ذه د ي د خ ت .

## CG522-E ي ف IP ر د ص م ك ا ه ت ن ا

ت ا م ي ل ع ت ل ا ي ف ة ل ك ش م ل ا ه ذ ه ي ل ع ا ض ق ل ل ة ز ي م ط ي ش ن ت م ت ي، ي ض ا ر ت ف ا ل ك ش ب ة ز ه ا ل ا ه ذ ه ل ة ي ج م ر ب ل ا .

جارخإلا اذه ضرعي زاوجلأ نأ ديكتأت

```
<#root>
```

```
CellularGateway#
```

```
show cellular 1 drop-stats
```

```
Ip Source Violation details:
```

```
Ipv4 Action = Drop
```

```
Ipv4 Packets Drop = 0
```

```
Ipv4 Bytes Drop   = 0
```

```
Ipv6 Action = Drop
```

```
Ipv6 Packets Drop = 0
```

```
Ipv6 Bytes Drop   = 0
```

تنكم ةمسلأ نأ ينعي وه. drop. ه IPv4/IPv6 ءارخإلا ةلاح نوكت نأ بجي.

---

ةزيملا ليطعت متي ،نذا لوقي جارخال ناك اذإ :ةطحالم

---

ةزيملا طيشنت ةداعإ نكمي ،رم اوألا هذه عم

```
CellularGateway#conf t
CellularGateway(config)# controller cellular 1
CellularGateway(config-cellular-1)# no ip-source-violation-action ipv4-permit
CellularGateway(config-cellular-1)# no ip-source-violation-action ipv6-permit
CellularGateway(config-cellular-1)# commit
Commit complete.
CellularGateway(config-cellular-1)# end
```

ةزيملا ليطعت متي ،نذا لوقي جارخال ناك اذإ :ةطحالم

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت  
م ل ا ل ا اء ن ا ع مچ ي ف ن ي م دخت س م ل ل م عد ي و ت ح م م ي دقت ل ة ي ر ش ب ل و  
ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب  
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه  
ي ل ا م اء ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco  
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا