

# مادختساب يوديلا قفن عاشنإ Umbrella SIG ڏزهنجا Cisco Edge

## تاي وتحمل

[قمدقملا](#)

[قيسس اس الـا تابلطتملا](#)

[تابلطتملا](#)

[قمدختسملا تانوكملا](#)

[قمانع ڦرظن](#)

[يوديلـا قـفنـلـا عـاشـنـا](#)

## قمدقملا

رادصـا لـغـشـي CDFW ـجـومـ مـادـخـتـسـابـ قـفـنـ عـاشـنـاـ ـيـفـيـكـ دـنـتـسـمـلـاـ اـذـهـ حـضـوـيـ 16.12 يـفـ Umbrella SIG.

## قيسس الـا تابلطتملا

### تابلطتملا

ـيـلـاتـلـاـ عـيـضـاـوـمـلـاـ ـفـرـعـمـ كـيـدـلـ نـوـكـتـ نـأـبـ Ciscoـ يـصـوـتـ:

- ـهـجـاـوـىـلـاـ ـدـنـتـسـمـلـاـ بـلـاـوـقـلـاـ مـادـخـتـسـابـ لـمـاـكـلـاـبـ الـغـشـمـ وـاـنـوـكـمـ زـاهـجـلـاـ نـوـكـيـ نـأـبـ جـيـ  
ـهـذـهـ يـفـ اـقـحـاـلـ ـرـوـكـذـمـلـاـ Umbrella SIGـ بـ ـقـلـصـلـاـ تـاـذـ ـعـاـزـجـأـلـاـ نـيـوـكـتـ لـبـقـ (CLI)ـ رـمـاـوـأـلـاـ رـطـسـ  
ـاـنـهـ قـفـنـلـاـ نـيـوـكـتـلـ طـقـفـ ـقـلـصـلـاـ تـاـذـ رـصـانـعـلـاـ طـاـقـتـلـاـ مـتـيـ ـلـاـقـمـلـاـ  
ـتـاـهـجـاـوـ نـمـ رـثـكـأـ ـوـ ـدـحـاـوـ ـهـجـاـوـ ـيـفـ NATـ نـيـوـكـتـ بـ جـيـ Transport VPNـ.  
ـيـلـبـقـتـسـمـ رـادـصـاـ يـفـ "Allow-Service IPsec"ـ يـفـ.

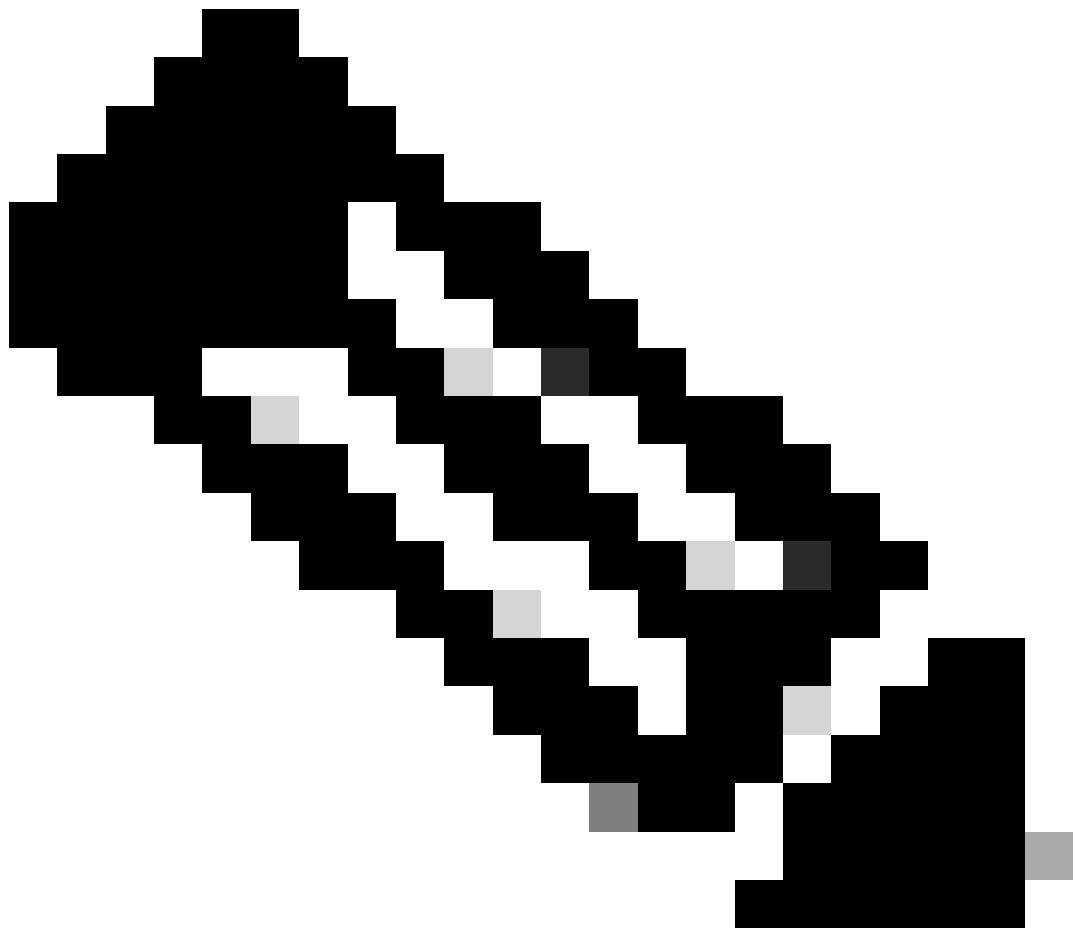
## قمدختسملا تانوكملا

Ciscoـ نـمـ (SIGـ)ـ ةـنـمـآـلـاـ تـنـرـتـنـإـلـاـ ـرـابـعـ ـلـاـ دـنـتـسـمـلـاـ اـذـهـ يـفـ ـدـرـاـوـلـاـ تـامـوـلـعـمـلـاـ دـنـتـسـتـ  
ـUmbrellaـ.

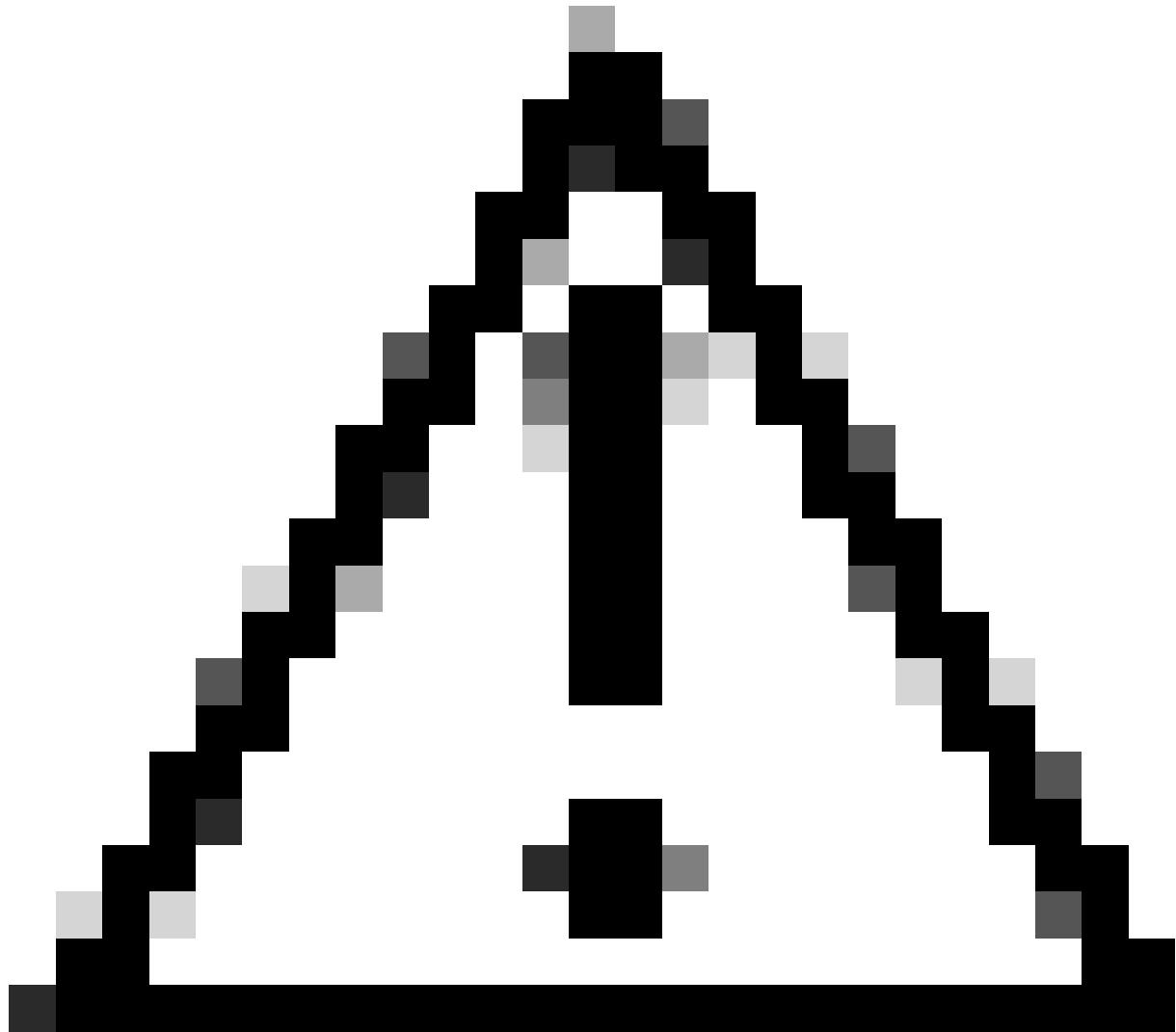
ـصـاخـ ـيـلـمـعـمـ ـئـيـبـ يـفـ ـدـوـجـوـمـلـاـ ـزـهـجـأـلـاـ نـمـ دـنـتـسـمـلـاـ اـذـهـ يـفـ ـدـرـاـوـلـاـ تـامـوـلـعـمـلـاـ عـاشـنـاـ مـتـ  
ـتـنـاـكـ اـذـاـ (ـيـضـارـتـفـاـ)ـ حـوـسـمـمـ نـيـوـكـتـبـ دـنـتـسـمـلـاـ اـذـهـ يـفـ ـقـمـدـخـتـسـمـلـاـ ـزـهـجـأـلـاـ عـيـمـجـ تـأـدـ  
ـرـمـأـ يـأـلـ لـمـتـحـمـلـاـ رـيـثـأـتـلـلـ كـمـهـفـ نـمـ دـكـأـتـفـ،ـلـيـغـشـتـلـاـ دـيـقـ كـتـكـبـشـ.

## قمانع ڦرظن

ـاقـبـاـسـ فـوـرـعـمـلـاـ (Cisco Edgeـ)ـ ـجـومـ مـادـخـتـسـابـ CDFWـ قـفـنـ عـاشـنـاـ ـيـفـيـكـ لـاـقـمـلـاـ اـذـهـ حـرـشـيـ  
ـرـادـصـاـ لـغـشـيـ يـذـلـاـ Viptela cEdgeـ)ـ 16.12ـ مـسـابـ.



عاشنال مزلي يذل او، ۋەچولا ىلى دىتىسم قىسىنتب ھاندأ نىوكتىلا بىلاق: ۋەظحالىم  
ۋەچولا ىلى دىتىسەملا قىسىنتىلا vManage. يىف رماؤألا رطس ۋەچجاو ىلى دىتىست قافنأ  
مادختسى نكىمىي اىل . تافالىت خالا ضىعب كانه نكلى و vEdge نىوكت قىسىنىتل لىثامم  
مدىختسى لاثملا اذە نإف يىلاتلابو، cEdge ل 17.2.1 ىتىح لاعف لىكشىپ ۋەزىملا بىلاق  
رماؤألا رطس ۋەچجاو ىلى دىتىسم اپىلاق.



فیض رورم ڈکرچ لاسرال مادختسالا ڈلچاعمل ڈلائملا ہذہ عاشنامت :ریذحت "مادختسالا ڈیفیک" ڈلائملا ہذہ مادختسال Cisco Umbrella SIG. لح لالخ نم ڈکرشالا یلإ ڈدنتسملابلاوقلادح زواجتل (CLI) رماؤلا رطس ڈھجاویلإ ڈدنتسملابلاوقلایف تازیملا vManage.

## یودیل ا قفنل ا عاشناء

1. ڈلظملا تامولعم ڈھولیف CDFW قفن عاشناء.

2. کتئیبل ڈاع ہنیوکتب موقتس امک Viptela زاہج بلاق نیوکتب مق.

3. ج .لقnelا تاہجاویف 4500 و 500 UDP ذفانمب حامسلل SIG ڈسایس نیوکتب مق

- CL\_for\_IKE\_IPSec\_tunnel (ACL) لوصولا یف مکحتلا ڈمیاں مسا وہ قفنل ا ڈھجاو لالخ نم IPSec رورم تادحویلإ یف اصلکش (ACL) لوصولا یف مکحتلا ڈمیاں دییقت کنکمی :یرایتخا SIG DC ڈیزملا ڈعارق [Umbrella](#) ڈیزیمپ ڈصالخل ا [Umbrella](#) قیاثو.

```

access-list ACL_for_IKE_IPSec_tunnel
sequence 10
match
protocol 50
!
action accept
!
!
sequence 20
match
destination-port 4500 500
!
action accept
!
!
default-action drop
!
```

اهم دختسن ي يتلا قفنلا ةهجاو لىع (ACL) لوصولا يف مكحتملا ةمئاق قيبيطت.

```

sdwan
interface GigabitEthernet1
tunnel-interface
access-list ACL_for_IKE_IPSec_tunnel in
```

ةبولطملا تاراسملالا كلذ يف امب لقنلل VPN ةكبش يف IPsec (تاهجاو) ةهجاو نيوكت.

ةمئاقلا هذه دعب رماولا رطس ةهجاو نيوكت بلاق يف تاريغتملا هذه فيرعت متى:

- {transport\_vpn\_1} WAN ةهجاو نيوكت ام ةداع) ةكبشلا ةهجاويه
- {transport\_vpn\_ip\_addr\_prefix} لقنلل VPN ةكبش ووه 1.1.1.0/24، لاثملالا ليبس
- {ipSec\_int\_number} قفن ةهجاو مقر ووه "IPSec1"
- {ipSec\_ip\_addr\_prefix} ناونع ووه IP قفن ةفرعم ةيعرف ةكبش ووه IPSec.
- {transport\_vpn\_interface\_1} WAN (ةهجاو ةداع) ةكبشلا ةهجاويه قفن IPSec.
- قافنأ مسق يف هؤاشنا مت ي يتلا اقبسم كرتشملا قفنلا حاتفم ةميقيه transport\_vpn\_1.
- {psk} قافنأ مسق يف هؤاشنا مت ي ذلا قفنلاب صاخلا IKE فرعم ووه تامولعملاء Umbrella.
- {sig\_fqdn} قافنأ مسق يف هؤاشنا مت ي ذلا قفنلاب صاخلا IKE فرعم ووه تامولعملاء Umbrella.
- {sig\_tunnel\_dest\_ip} قفنلا هب لصتملا CDFW DC ب صاخلا IP ناونع ووه

```

vpn 0
interface {{transport_vpn_1}}
ip address {{transport_vpn_ip_addr_prefix}}
nat
```

```

refresh bi-directional
!
mtu      1360
no shutdown
!
interface ipsec{{ipsec__int_number}}
  ip address {{ipsec_ip_addr_prefix}}
  tunnel-source-interface {{transport_vpn_interface_1}}
  tunnel-destination    {{sig_tunnel_dest_ip}}
  ike
    version      2
    rekey        14400
    cipher-suite aes256-cbc-sha1
    group        14
    authentication-type
      pre-shared-key
        pre-shared-secret {{psk}}
        local-id       {{sig_fqdn}}
        remote-id     {{sig_tunnel_dest_ip}}
    !
  !
!
ipsec
  rekey          3600
  replay-window   512
  cipher-suite     aes256-gcm
  perfect-forward-secrecy none
!
no shutdown
!
ip ipsec-route 0.0.0.0/0 vpn 0 interface ipsec{{ipsec__int_number}}

```

### تاوطخلا يف روکذم نیوکت جذومن انه ،کعجمل 3-5:

```

access-list ACL_for_IKE_IPSec_tunnel
sequence 10
match
protocol 50
!
action accept
!
!
sequence 20
match
destination-port 4500 500
!
action accept
!
!
default-action drop
!
!
vpn 0
dns 208.67.222.222 primary

```

```
name VPNO
  interface GigabitEthernet4
    ip address 192.168.1.0/24
    nat
      refresh bi-directional
    !
    mtu      1360
    no shutdown
  !
  interface ipsec1
    ip address 10.10.10.1/30
    tunnel-source-interface GigabitEthernet4
    tunnel-destination      146.112.83.8
    ike
      version      2
      rekey        14400
      cipher-suite aes256-cbc-sha1
      group        14
      authentication-type
        pre-shared-key
          pre-shared-secret YourPreSharedKey
          local-id       YourTunnelID@umbrella.sig.cisco.com
          remote-id     146.112.83.8
      !
    !
  !
  ipsec
    rekey          3600
    replay-window   512
    cipher-suite    aes256-gcm
    perfect-forward-secrecy none
  !
  no shutdown
!
ip ipsec-route 0.0.0.0/0 vpn 0 interface ipsec1
```

## 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).