

# مادختساب يودي ال Umbrella SIG ق فن عاشن ا Cisco Edge ةزهج

## تايوتحمل

[ةمدقملا](#)

[ةيساسالاب لطلتملا](#)

[تاب لطلتملا](#)

[ةمدختسملا تانوكملا](#)

[ةماع قرظن](#)

[يودي ال ق فنلا عاشن ا](#)

## ةمدقملا

رادصلال لغشي Cisco Edge هجوم مادختساب CDFW ق فن عاشن ا ةيفيك دنتسمل اذه حضوي Umbrella SIG في 16.12.

## ةيساسالاب لطلتملا

### تاب لطلتملا

ةيلاتال عيضاوملاب ةفرعم كي دل نوكت ناب Cisco ي صوت:

- ةهجاو ىل ا ةدنتسمل بالاولقلا مادختساب لماكلاب ال غشموانوكم زاهجل نوكتي نابجي  
هذه في اقحال ةروكذمل Umbrella SIG ب ةلصلال تاذ اناجال نيوكت لبقي (CLI) رماوالا رطس  
انه ق فنل نيوكتل طقف ةلصلال تاذ رصانعل طاقتل متي. ةلاقمل
- Transport VPN تاهجاو نم رثكا وا ةدحاو ةهجاو في NAT نيوكت بجي
- يلبقتسم رادصل في "Allow-Service IPsec" ةفاضل متت ىتح ليدب لح وه جردمل جهنل

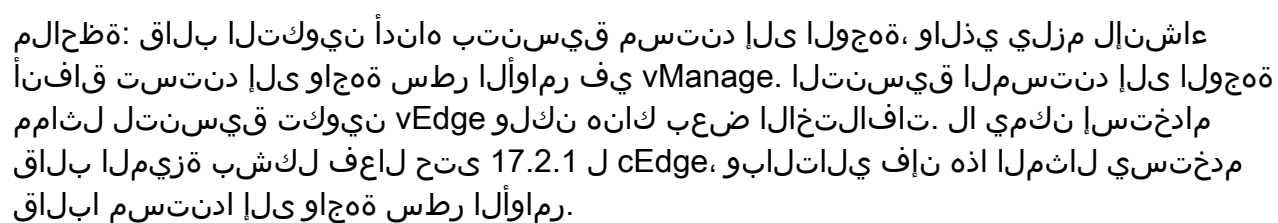
### ةمدختسملا تانوكملا

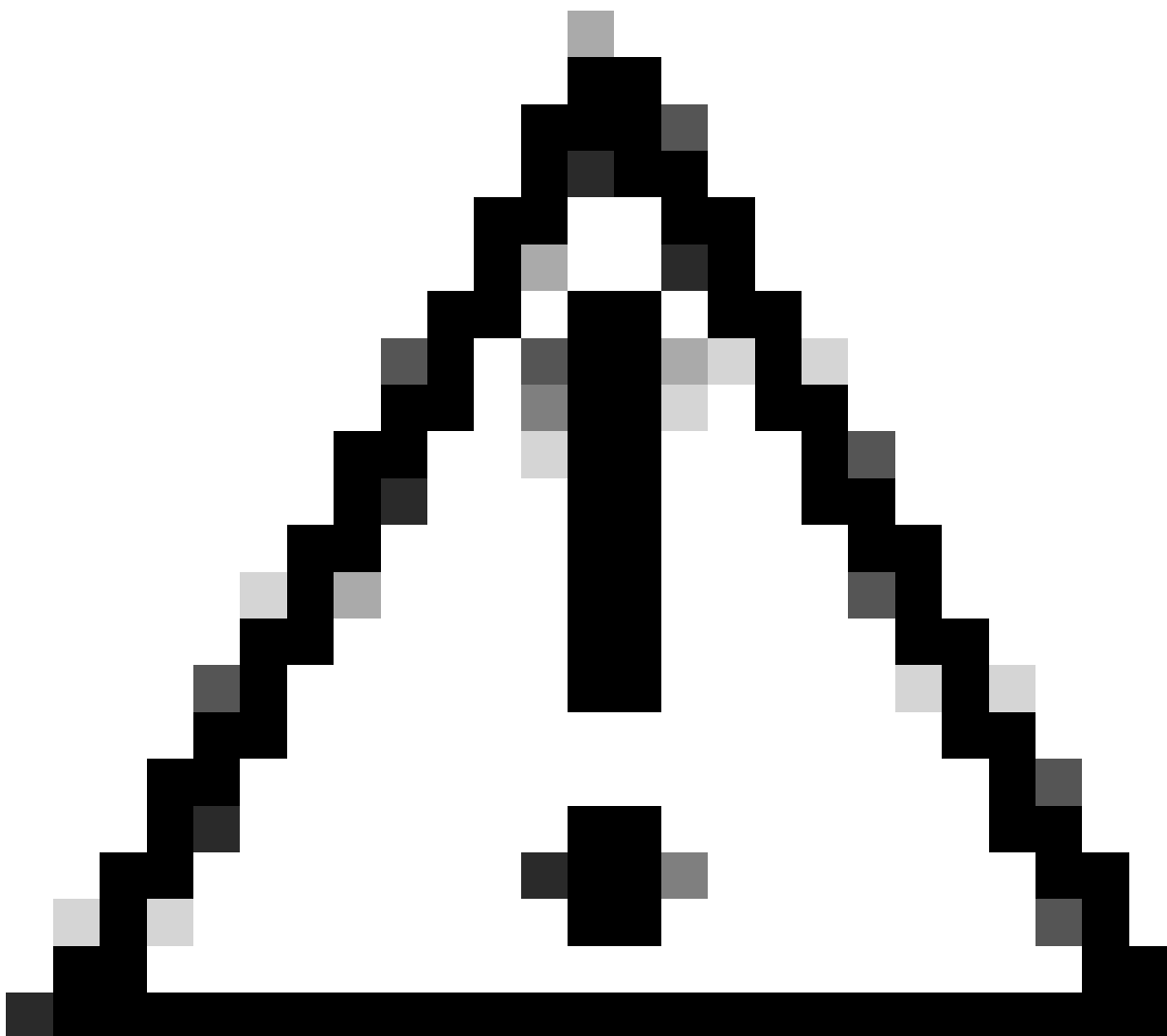
Cisco نم (SIG) ةنمالا تنرتنالا ةرابع ىل ا دنتسمل اذه في ةدراول تامولعمل دنتست Umbrella.

ةصاخ ةيلمعم ةئيبي في ةدوجوملا ةزهجالا نم دنتسمل اذه في ةدراول تامولعمل عاشن ا مت  
تناك اذ. (يضا رتفا) حوسمم نيوكتب دنتسمل اذه في ةمدختسملا ةزهجالا عيمج تادب  
رمأ يال لم تحمل ريثأتلل كمهف نم دكأتف، ليغشتل دي ق ك تكبش

## ةماع قرظن

اقباس فورعمل Cisco Edge هجوم مادختساب CDFW ق فن عاشن ا ةيفيك لاقمل اذه حرشي  
16.12 رادصلال لغشي يذل (Viptela cEdge م ساب





فېض رورم ةكرح لاسرال مادختسالال ةلاح ةجلالعمل ةلاقملال هذه عاشنإ م ت: ريذحت  
"مادختسالال ةيفيك" ةلاقملال هذه مدختست Cisco Umbrella SIG لال لال خ نم ةكرشلال  
ىلإ ةدنتسملال بلالوقلال دح زواجتل (CLI) رمالوالا رطس ةهجالو ىلإ ةدنتسملال بلالوقلال  
vManage في تازيملال.

## يوديال قفنال عاشنإ

1. ةلظملال تامولعم ةحول في CDFW قفن عاشنإ.
2. كئيبلا ةداع هنويوكتب موقتس امك Viptela زاهج بلالوق نويوكتب مق.
3. ج. لقنلال تاهجالو في 4500 و 500 UDP ذفانمب حامسلل SIG ةسايس نويوكتب مق.
  - ةكرحل حمسي يذلا (ACL) لوصولال في مكحتلال ةمئاق مسا وه CL\_for\_IKE\_IPSec\_tunnel رورم  
قفنلال ةهجالو لال لال خ نم IPSec رورم
  - تادحو ىلإ يفاضل لكشب (ACL) لوصولال في مكحتلال ةمئاق دييقت كنكمي: يرايخا  
Umbrella [قئاثو](#) في ديزملال ةءارق. Umbrella ةزيمب ةصاخلال SIG DC

```
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
!
```

4. اهم دخت ست يتال قفنال هه جاو ىل ع (ACL) لوصولا يف مكحتال عمئاق قيبطت .

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

5. ةبولطملا تاراسملا كلذ في امب لقنلل VPN ةكبش في IPsec (تاهجاو) هجاو نيوكت.

**:مهم اقبال هذه دعوى رم او ال رطس هه جاو ني وكت بل اق ي ف تاري غتم ل هذه في رع ت م تي**

- {transport\_vpn\_1} IPsec قفنى ئىشلىتىش (WAN) ئەھۋال ئۆزگەرتىش (WAN) قىلىپ بەرگەن بولسا، ئۇنىڭ ئورنىدا {transport\_vpn\_ip\_addr\_prefix} بولغان VPN ئورنىدا بەرگەن بولسا، ئۇنىڭ ئورنىدا بەرگەن بولسا، ئۇنىڭ ئورنىدا بەرگەن بولسا.
- {ipSec\_\_int\_number} IPsec قفنى ئىشلىتىش (WAN) ئەھۋال ئۆزگەرتىش (WAN) قىلىپ بەرگەن بولسا، ئۇنىڭ ئورنىدا بەرگەن بولسا، ئۇنىڭ ئورنىدا بەرگەن بولسا، ئۇنىڭ ئورنىدا بەرگەن بولسا.
- {ipSec\_ip\_addr\_prefix} IPsec قفنى ئىشلىتىش (WAN) ئەھۋال ئۆزگەرتىش (WAN) قىلىپ بەرگەن بولسا، ئۇنىڭ ئورنىدا بەرگەن بولسا، ئۇنىڭ ئورنىدا بەرگەن بولسا، ئۇنىڭ ئورنىدا بەرگەن بولسا.
- {transport\_vpn\_interface\_1} IPsec قفنى ئىشلىتىش (WAN) ئەھۋال ئۆزگەرتىش (WAN) قىلىپ بەرگەن بولسا، ئۇنىڭ ئورنىدا بەرگەن بولسا، ئۇنىڭ ئورنىدا بەرگەن بولسا، ئۇنىڭ ئورنىدا بەرگەن بولسا.
- {psk} IPsec قفنى ئىشلىتىش (WAN) ئەھۋال ئۆزگەرتىش (WAN) قىلىپ بەرگەن بولسا، ئۇنىڭ ئورنىدا بەرگەن بولسا، ئۇنىڭ ئورنىدا بەرگەن بولسا، ئۇنىڭ ئورنىدا بەرگەن بولسا.
- {sig\_fqdn} IPsec قفنى ئىشلىتىش (WAN) ئەھۋال ئۆزگەرتىش (WAN) قىلىپ بەرگەن بولسا، ئۇنىڭ ئورنىدا بەرگەن بولسا، ئۇنىڭ ئورنىدا بەرگەن بولسا، ئۇنىڭ ئورنىدا بەرگەن بولسا.
- {sig\_tunnel\_dest\_ip} IPsec قفنى ئىشلىتىش (WAN) ئەھۋال ئۆزگەرتىش (WAN) قىلىپ بەرگەن بولسا، ئۇنىڭ ئورنىدا بەرگەن بولسا، ئۇنىڭ ئورنىدا بەرگەن بولسا، ئۇنىڭ ئورنىدا بەرگەن بولسا.

```
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}}
```

3-5: تاوطلخا لى ف روكذم نيوكت جذومن انه ،كعجرمل

```

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 VPN0
  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

```

ةمچرتل هذه لوح

ةيلآل تاي نقتل نم ةومجم مادختساب دنتسمل اذه Cisco تمچرت  
ملاعلا ءانأ عي مجي في ني مدختسمل معدى وتحم مي دقتل ةيرشبلا و  
امك ةقيقد نوكت نل ةيلآ ةمچرت لصفأ نأ ةظحال ميجري. ةصاغل مهتغلب  
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحا وه  
ىلإ أمئاد عوچرلاب يصوت و تامچرتل هذه ةقदन ع اهتيلوئسم Cisco  
Systems (رفوتم طبارلا) يلصأل يزيلجنلإا دنتسمل