

ةكبش ىلإ راسم ىلإ دننسملا IKEv1 عقوم IPv6 مادختساب عقوملل VPN

تايوتحمل

[ةمدقملا](#)

[ةيساسالاب لطلتلا](#)

[تابلطلتلا](#)

[ةمدختسملا تانوكملا](#)

[نئوكتلا](#)

[ةكبش لىطىطختلا مسرلا](#)

[تانئوكتلا](#)

[يلحمل او حوملا](#)

[يلحمل او حومل لىئاه نئوكتلا](#)

[دعب نع حومل لىئاه نئوكتلا](#)

[اهجالص او اعاطخال فاشكتسا](#)

ةمدقملا

نئب عقوم ىلإ عقوم نم، راسملا ىلإ دننسملا، IPv6 قفن دادعإل نئوكت دننسملا اذه فصى (IKEv1/ISAKMP) 1 رادصلال تنرتنلال حاتفم لدابت لوكتورب مادختساب Cisco تاهجوم.

ةيساسالاب لطلتلا

تابلطلتلا

ةيللال عيضاوملاب ةفرعم كئيدل نوكت نأب Cisco ىصوت:

- Cisco IOS®/Cisco IOS® XE رم اوأل رطس ةهجاو نئوكتب ةيساسا ةفرعم
- (ISAKMP) تنرتنلال نامأ طابتر او حىتافملا ةرادل لوكتوربب ةيساسا ةفرعم
IPsec تالوكتوربو
- هيجوتلال او IPv6 ةنونع مهف

ةمدختسملا تانوكملا

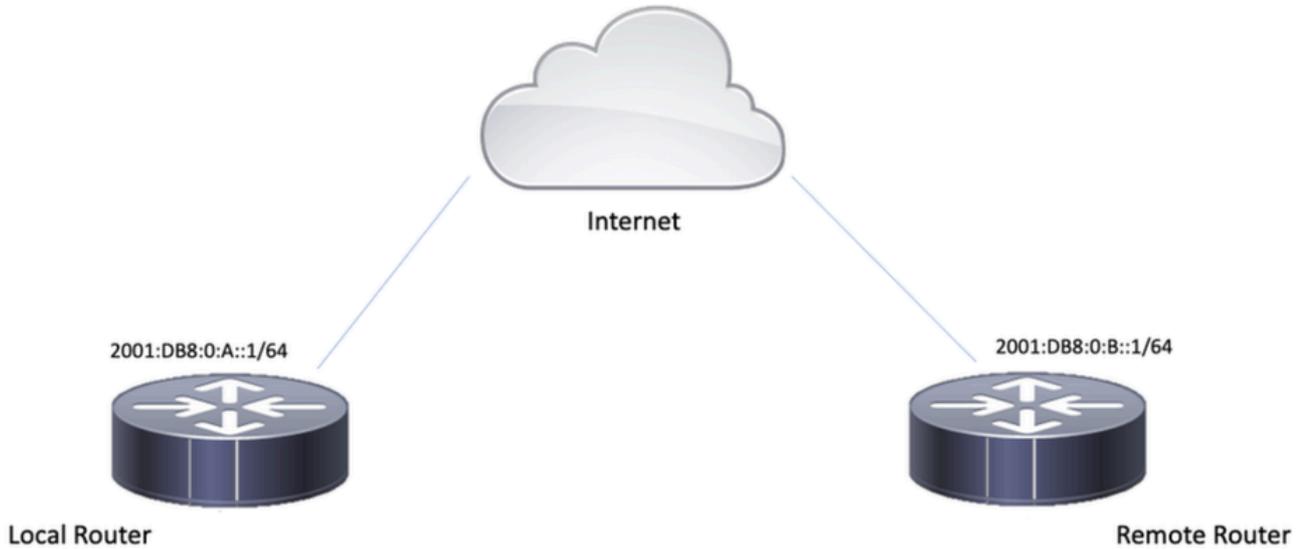
ةيللال جماربلل تارادصلال ىلإ دننسملا اذه ىف ةدراول تامولعمل دننست:

- IOS XE نم Cisco لىغشى 17.03.04a لىحم هجومك
- Cisco نم دعب نع هجومك 17.03.04a لىغشى ىذل IOS جمانرب

ةصاخ ةيلمعم ةئيب ىف ةدوجوملا ةزهجال نم دننسملا اذه ىف ةدراول تامولعمل عاشنإ مت تناك اذإ. (ىضارتفا) حوسمم نئوكتب دننسملا اذه ىف ةمدختسملا ةزهجال عيمج تادب رما ىل لم تحملا رىثأتلل كمهف نم دكأتف، لىغشنتلا دىق كتكبش.

نېوكتالا

ةكبش ل ل يطخ تالا مسرلا



تاناوكتالا

ي لحملا هجوملا

IPv6 ل يداحالا ثبلا هيجوت نېكمت 1. ةوطخلا

```
ipv6 unicast-routing
```

هجوملا تاهجاو نېوكتا ب مق 2. ةوطخلا

```
interface GigabitEthernet1
ipv6 address 2001:DB8:0:A::1/64
no shutdown
```

```
interface GigabitEthernet2
ipv6 address FC00::1/64
no shutdown
```

IPv6 ل يضارتفالا راسملا نېيغت 3. ةوطخلا

```
ipv6 route ::/0 GigabitEthernet1
```

1. ةلحرمل جهن نيوكت 4. ةوطخل

```
crypto isakmp policy 10
encryption aes
authentication pre-share
group 14
```

اقبس م كرتشم حاتفم مادختساب حيتافملا ةقلح نيوكتب مق 5. ةوطخل

```
crypto keyring IPV6_KEY
pre-shared-key address ipv6 2001:DB8:0:B::1/128 key cisco123
```

ISAKMP فيرعت فلم نيوكتب مق 6. ةوطخل

```
crypto isakmp profile ISAKMP_PROFILE_LAB
keyring IPV6_KEY
match identity address ipv6 2001:DB8:0:B::1/128
```

2. ةلحرمل جهن نيوكت 7. ةوطخل

```
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
mode tunnel
```

IPsec فيرعت فلم نيوكت 8. ةوطخل

```
crypto ipsec profile Prof1
set transform-set ESP-AES-SHA
```

قفلنلا ةهجاو نيوكتب مق 9. ةوطخل

```
interface Tunnel0
no ip address
ipv6 address 2012::1/64
```

```
ipv6 enable
tunnel source GigabitEthernet1
tunnel mode ipsec ipv6
tunnel destination 2001:DB8:0:B::1
tunnel protection ipsec profile Prof1
end
```

ةديفملا رورملا ةكرحل تاراسملا نيوكتب مق 10 ةوطخل

```
ipv6 route FC00::/64 2012::1
```

ي لحملا هجوملل يئاهنلا نيوكتلل

```
ipv6 unicast-routing
!
interface GigabitEthernet1
ipv6 address 2001:DB8:0:A::1/64
no shutdown

!

interface GigabitEthernet2
ipv6 address FC00::1/64
no shutdown

!

ipv6 route ::/0 GigabitEthernet1

!

crypto isakmp policy 10
encryption aes
authentication pre-share
group 14

!

crypto keyring IPV6_KEY
pre-shared-key address ipv6 2001:DB8:0:B::1/128 key cisco123

!

crypto isakmp profile ISAKMP_PROFILE_LAB
keyring IPV6_KEY
match identity address ipv6 2001:DB8:0:B::1/128

!

crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
mode tunnel
```

```
!  
crypto ipsec profile Prof1  
  set transform-set ESP-AES-SHA  
  
!  
interface Tunnel0  
  no ip address  
  ipv6 address 2012::1/64  
  ipv6 enable  
  tunnel source GigabitEthernet1  
  tunnel mode ipsec ipv6  
  tunnel destination 2001:DB8:0:B::1  
  tunnel protection ipsec profile Prof1  
end  
  
!  
ipv6 route FC00::/64 2012::1
```

دعب نع هجوم لئ يئاهن لاني وكتلا

```
ipv6 unicast-routing  
!  
interface GigabitEthernet1  
  ipv6 address 2001:DB8:0:B::1/64  
  no shutdown  
  
!  
interface GigabitEthernet2  
  ipv6 address FC01::1/64  
  no shutdown  
  
!  
ipv6 route ::/0 GigabitEthernet1  
  
!  
crypto isakmp policy 10  
  encryption aes  
  authentication pre-share  
  group 14  
  
!  
crypto keyring IPV6_KEY  
  pre-shared-key address ipv6 2001:DB8:0:A::1/128 key cisco123  
  
!  
crypto isakmp profile ISAKMP_PROFILE_LAB  
  keyring IPV6_KEY  
  match identity address ipv6 2001:DB8:0:A::1/128
```

```
!  
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac  
mode tunnel  
  
!  
crypto ipsec profile Prof1  
set transform-set ESP-AES-SHA  
  
!  
interface Tunnel0  
no ip address  
ipv6 address 2012::2/64  
ipv6 enable  
tunnel source GigabitEthernet1  
tunnel mode ipsec ipv6  
tunnel destination 2001:DB8:0:A::1  
tunnel protection ipsec profile Prof1  
end  
  
!  
ipv6 route FC00::/64 2012::1
```

اهحال صإو ءاطخأل فاشك تسأ

رمأ debug لآ، قف نلآ تي رحت in order to تلم عتسأ

- debug crypto isakmp
- debug crypto isakmp أطخ
- debug crypto ipSec
- IPsec لوكوتورب يف ريفش تالآ ءاطخأ ححصت أطخ

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نء مء دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءء. ةصاأل مء تءل ب
Cisco ةللأل. فرتمة مچرت مء دق ةل
ىل ةل
(رفوتم طبارل) ةل ةل