

# وضع ل ضوفرم ل ليجستل اءاطخ ا فاشكتس ا SA قفاوت مدعب ةصاخ ل GETVPN ةومجم اهحالص او ليوطل

## تايوتحمل

[ءمدقم ل](#)

[ءيساس ال اءبلطتم ل](#)

[ءابلطتم ل](#)

[ءمدختس ل اءنوكل ل](#)

[ءلكش ل](#)

[لحل ل](#)

## ءمدقم ل

مدعب قلعتي اميف اءحالص او ليجستل ضوفر اءاطخ ا فاشكتس ا ةيفيك دننتم ل اءه فصبي ةصاخ ل ةكبش ل اءاتفم مءاخ ني (SA) ليوطل اءام ال اءرتقال يضا رتفال اءومجم ل قفاوت اءحالص او (GM) ةومجم ل وضع و (GETVPN) ةومجم ل رفش ل ل قنل ةيره اءل.

نم ةينف ل ةءعاس ل زكرم سءنهم ،زيكزاف يءري ف زيرب ل اءناء لبق نم ةمهاس ل تمء Cisco.

## ءيساس ال اءبلطتم ل

### ءابلطتم ل

ءيلال اءيضاوم ل اء ةفرعم لكيءل نوكت نأب Cisco يءصوء:

- Getvpn
- (ISAKMP) ءنءن ال اءام اءبلطءرا وءي ءافم ل ةراء لوكوءورب

### ءمدختس ل اءنوكل ل

ءيلال ةيءام ل اءنوكل ل او جم اءبل ل اءاراءص ل ل دننتم ل اءه يف ةءراول اءمولءم ل دننءسء:

- (IOS) ةينب ل ةكبش ل ل لءيغشء مءظن نم مءق اءراءص ل لءيغشءء موءءء يءل ال GMS لءيوطل يضا رتفال اءومجم ل ةءءء ال يءل ال 15.3(2)T.
- رمءل ةءيم مءءء ال يءل ال IOS XE 15.3(2)S نم مءق اءراءص ل لءيغشءء موءءء يءل ال GMS لءيوطل يضا رتفال.

ءصاخ ةيءمعم ةئيء يف ةءوءوم ل ةزهءال نم دننتم ل اءه يف ةءراول اءمولءم ل اءشءن اءمءءن اءا (يضا رتفال) ءوسمم نيوكءء دننتم ل اءه يف ةمدختس ل ةزهءال اءيجمءء اءب رما يءل لمءءم ل رءءاءل ل كمءهف نم ءكأءف ،لءيغشءءل ءيقل كءكءبش.

## ءلكش ل

نموذج 15.3(2)T رادصإلإ نم ةيساسألإ IOS ةمظنأ يف "SA ل لويوطال رمعلال" ةزيم نيمضت متي رورملا ةكرح ريفشت حاتفم ل رمعلال دمب حمسي وهو. IOS XE. ةزهجأ يف (15.3(2)S) XE3.9 زارطلال رمعلال ةزيم مادختسا دنع. اموي 30 لىلإ ةعاس 24 نم (KEK) حيتافم ل ريفشت حاتفمو (TEK) يف يضارتفالال رمعلال ريفيغت متي ام دنع اذهو، يسئيرال مادخالال يف SA ل لويوطالال يضارتفالال عيمجل جم انربال رادصإل نم GETVPN KS ققحتي، دحاو موي نم رثكأ لىلإ GDOI ةعومجم نيوكت ةزيمال معددي ال نمل ليجستال رطحي و GMS.

دوجو (SA) نمأل فالغل لوكوتوربل يضارتفالال رمعلال لوط مادختسا بلطتي: **ةظحال** ريفشتال راي عم عضو وأ (AES-CBC) مدقتم ل ريفشتل ل يساي ق ةلتك لس لست يوقا وأ تب 128 رادقمب AES حاتفمب (AES-GCM) دادعل/Galois-م دقتم ل.

مداخبة صاخال (GDOI) ريسفتال لاجمة وعومجم يف SA ل لويوطالال ةاقبلال ةدم ةزيم نيوكت مت حاتفم ل.

حاجنبل ضعبلال اهضعب عم ةقداصم لالو ISAKMP قفن لالامكإ ةزهجالل نكمي.

```
208752: Jun 10 22:19:14.380: ISAKMP-PAK: (82124):sending packet to 10.40.10.10 my_port 848
peer_port 848 (R) MM_KEY_EXCH
208753: Jun 10 22:19:14.380: ISAKMP: (82124):Sending an IKE IPv4 Packet.
208754: Jun 10 22:19:14.380: ISAKMP: (82124):Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE
208755: Jun 10 22:19:14.380: ISAKMP: (82124):Old State = IKE_R_MM5 New State = IKE_P1_COMPLETE

208756: Jun 10 22:19:14.380: ISAKMP: (82124):Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE
208757: Jun 10 22:19:14.380: ISAKMP: (82124):Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE
```

يف IOS رادصإل أن KS فشتكي، ريفشتال حيتافم لىل لوصحال GM لواحي ام دنع، ك لذ عمو لالصالال عطق ل أطخ ةلسر دلويو و"ةلويوطالال ةاقبلال ةدم" ةزيم معد نمضتال ال GM.

```
208758: Jun 10 22:19:14.433: ISAKMP-PAK: (82124):received packet from 10.40.10.10 dport 848
sport 848 Global (R) GDOI_IDLE
208759: Jun 10 22:19:14.433: ISAKMP: (82124):set new node 1548686329 to GDOI_IDLE
208760: Jun 10 22:19:14.433: ISAKMP: (82124):processing HASH payload. message ID = 1548686329
208761: Jun 10 22:19:14.433: ISAKMP: (82124):processing NONCE payload. message ID = 1548686329
208762: Jun 10 22:19:14.433: ISAKMP: (82124):GDOI Container Payloads:
208763: Jun 10 22:19:14.433: ID
208764: Jun 10 22:19:14.433: ISAKMP: (82124):Node 1548686329, Input = IKE_MSG_FROM_PEER,
IKE_GDOI_EXCH
208765: Jun 10 22:19:14.434: ISAKMP: (82124):Old State = IKE_KS_LISTEN New State =
IKE_KS_GET_SA_POLICY_AWAIT
208766: Jun 10 22:19:14.434: ISAKMP: (82124):GDOI Container Payloads:
208767: Jun 10 22:19:14.434: SA
208768: Jun 10 22:19:14.434: ISAKMP-ERROR: (82124):GDOI processing Failed: Deleting node
208769: Jun 10 22:19:14.434: ISAKMP-ERROR: (82124):deleting node 1548686329 error TRUE reason
"GDOI QM rejected - failed to process QM"
208770: Jun 10 22:19:21.280: %GDOI-4-REJECT_GM_VERSION_REGISTER: Reject registration of GM
10.40.10.10(ver 0x1000001) in group MYGETVPN as it cannot support these GETVPN features enabled:
Long-SA
```

هذه دنع. ل ليجستالال ةي لمع ءاهنإ اهنكمي ال نكلو ديديج ISAKMP قفن ءاشنإ GM لواحت ضوافتالال س فنل ةددعتم تالليثم ةظحالال كنكمي ةطقنلال.

```
Router# sh crypto isakmp sa | i 10.80.127.20
10.80.127.20 10.40.10.10 MM_NO_STATE 2104 ACTIVE (deleted)
```

```
Router#show crypto gdoi
GROUP INFORMATION
```

```
Group Name           : MYGETVPN
Group Identity       : 1
Rekeys received      : 0
IPSec SA Direction  : Inbound Only

Group Server list    : 10.80.127.20

Group member         : 10.40.10.10      vrf: None
  Registration status : Registering
  Registering to      : 10.80.127.20
  Re-registers in     : 44 sec
  Succeeded registration: 0
  Attempted registration: 3
  Last rekey from     : 0.0.0.0
  Last rekey seq num  : 0
  Multicast rekey rcvd : 0
  allowable rekey cipher: any
  allowable rekey hash : any
  allowable transformtag: any ESP

Rekeys cumulative
  Total received      : 0
  After latest register : 0
  Rekey Received     : never
```

```
ACL Downloaded From KS UNKNOWN:
```

إجراء `show crypto gdoi feature long-sa-life` لإظهار إعدادات `long-sa-life` في IOS. إذا لم تظهر الإعدادات، فإجراء `show crypto gdoi feature long-sa-life` لإظهار الإعدادات. إذا لم تظهر الإعدادات، فإجراء `show crypto gdoi feature long-sa-life` لإظهار الإعدادات.

```
Router# sh cry gdoi feature long-sa-lifetime
```

```
Group Name: GETVPN_GROUP
```

Key Server ID	Version	Feature Supported
10.80.127.20	1.0.18	Yes

```
Group Member ID Version Feature Supported 10.40.10.9 1.0.17 Yes
```

```
10.40.10.10
```

```
1.0.4
```

```
No
```

## الحل

- روثعلا نكمي. ثدحأ رادصإ وأ IOS 15.3(2) إلى GM ةيقرت مادختساب ةلكشملا حالصإ نكمي [GETVPN ميمصت ليلد](#) في IOS/IOS-XE تارادصإو GDOI تارادصإ نيب طيطخت ىلع.
- 86400 نم لوقأ إلى GDOI ةومجم في فيقيقحلل رملل ريغت نوكي نأ نكمي يثلاثلل حلل ال هأل لمعلل ةومجم ءاضأل ليطعت في إذل نيوكتلل ريغت ببستي ال. ةيثلل حلل. حاتفم في ليلغشت ىللي دي.

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 ةللخت. فرتمة مچرت مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او  
ىل إلمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةلصلأل ةزىل ءنل اءل دن تسمل