

ةكرتشملا ريفشتلا حيتافم نيوكت هجوم يف اقبس م

تايوت حمللا

[ةمدقملا](#)

[ةيساس الابلطت ملا](#)

[تابلطت ملا](#)

[ةمدختس ملا تانوك ملا](#)

[تاجالطص الابل](#)

[ةيساس ا تامولعم](#)

[نيوكت ملا](#)

[تانوكت ملا](#)

[ةحصلا نم ققحت ملا](#)

[اهجالص او اعاطخ الابل فاشكتسا](#)

[ةلص تاذا تامولعم](#)

ةمدقملا

ةيلاحلا اقبس مةكرتشملا حيتافملا نم لكل ريفشت دادعإ ةيفيك دنتسملا اذه حضوي
هجوم يف ةديجل او.

ةيساس الابلطت ملا

تابلطت ملا

دنتسملا اذهل ةصاخ تابلطت ملا دجوت ال.

ةمدختس ملا تانوك ملا

ةغصي ةيجمرب اذه ىلع ةقيثو اذه يف ةمولعملا تسسأ:

- 16.9 رادصل ال Cisco IOS XE® جم انرب

ةصاخ ةيولعم ةئيبي يف ةدوجوملا ةزهجال نم دنتسملا اذه يف ةدراولا تامولعملا عاشنإ مت
تناك اذا. (يضا رتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختس ملا ةزهجال اعمج تادب
رمأ يال لم تحملا ريثا تلل كم هف نم دكأتف، ليغشتلا دي قكتك بش.

تاجالطص الابل

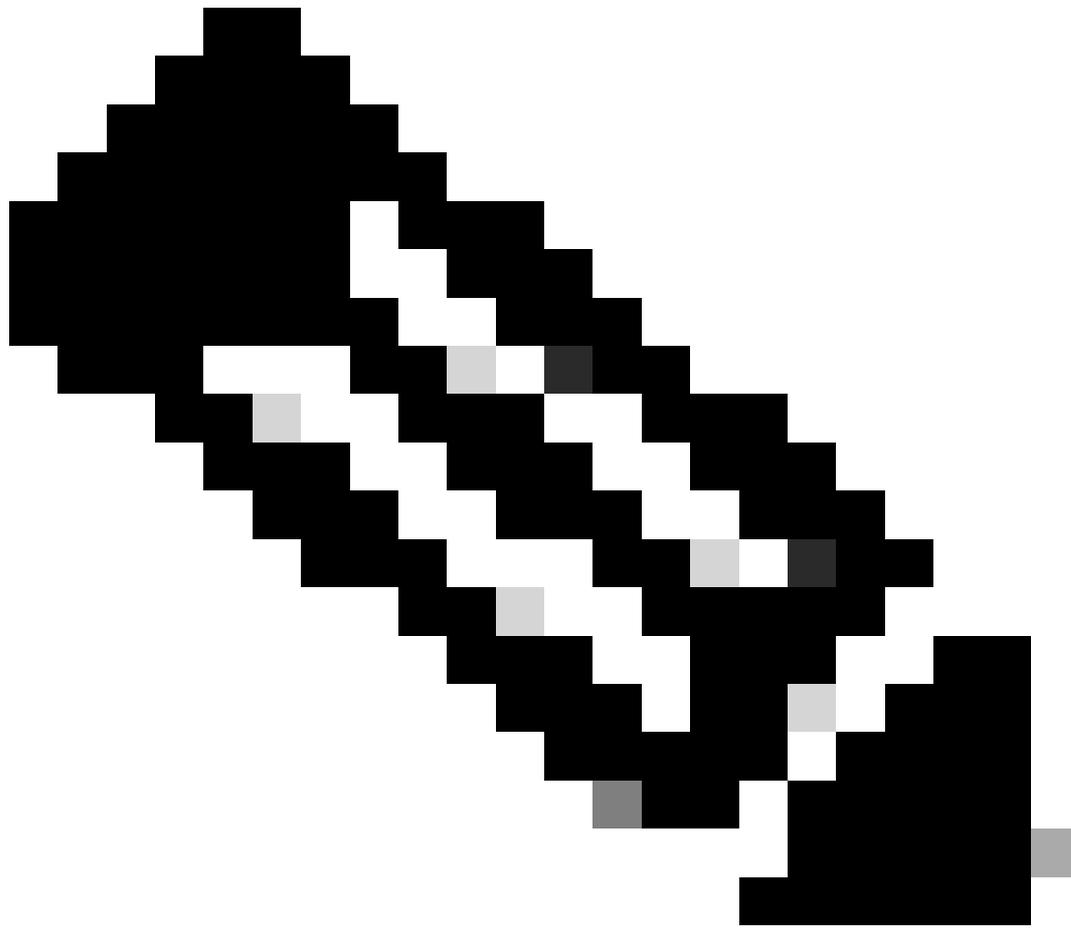
تاجالطصا لوح تامولعملا نم ديزم ىلع لوصحلل ةينقتلا Cisco تاجيملت تاجالطصا عجار
تادنتسملا.

ةيساسأ تامولعم

ريفشتب هجوملل حمست يتل ةفيظولا 12.3(2)T code رادصلال Cisco IOS جم انرب مدقي في اقبس م كرتشملا (ISAKMP) حيتافملا ةرادل لوكوتورب حاتفم و تنرتنال نامأ نارتقا لوصول ةركاذ، ةرپاطتملا ريغ يئوشعلا لوصول ةركاذ في نمآلا 6 عونلا قيسنت دارملا اقبس م كرتشملا حاتفملا نيوكت نكمي. (NVRAM) ةرپاطتملا ريغ يئوشعلا رورم ةملكك وأ، زيمتملا عضولا في، ISAKMP حيتافم ةقلح تحت وأ، رايعمك اما هريفشت ليمع دادعأ وأ لهس (EzVPN) مداخ تحت ةعومجم.

نيوكتلا

اذه اهفصي يتلا تازيملا نيوكتل اهمادختسا كنكمي يتلا تامولعملا مسقلا اذه كل مدقي دننتملا.



رمأوالا لوح تامولعملا نم ديزم يلع لوصول رمأوالا ثحب ةادأ مدختسا: ةظحالم مسقلا اذه في ةمدختسملا.

تامول عمو Cisco ةادأ ىلإ لوصولو نىلجسمل Cisco ىم دختسمل طقف نكمى :ةظحالم ةىلخاد

اقبس م كرتشمال حىتافملا رىفش ت نىكمتل نىرمأل نىذه لالخاد مت

- [ىساسأل حاتفملا] config-key password-encryption حاتفم
- رورملا ةم لك رىفش ت AES

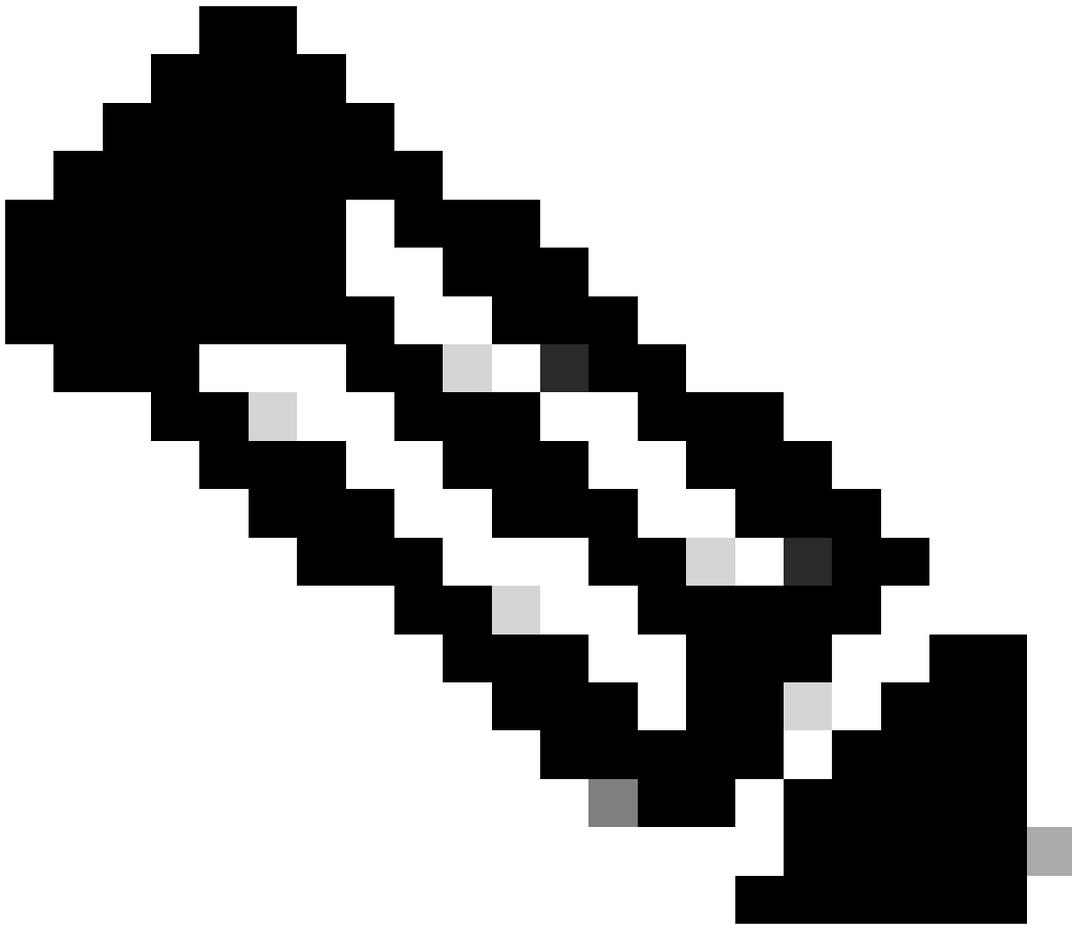
ىرخأل حىتافملا عىمى رىفش ت م دختسمل حاتفملا/رورملا ةم لك وه [ىساسأل حاتفملا] متى ال (AES) م دقتملا رىفش ت ل راعم ل لثام ت م رىفش ت مادختساب هوملا نىوكت ىف ةقيرط ىب هىل لوصولو وأ هتور نكمى الو هوملا نىوكت ىف ىساسأل حاتفملا نىخت هوملاب هلاصتإ ءانثأ

ىف ةدىج وأ ةىلح حىتافم ى رىفش ت ل ىساسأل حاتفملا مادختسإ متى ،اه نىوكت درجمبو نم بلطى هوملا نىف ،رم أوأل رطس ىف [ىسىئرلا حاتفملا] دىحت متى مل اذا . هوملا نىوكت ةبللاطم متت ،لعللاب حاتفم دوجو ةلح ىف . ققحتلل هلاخدا ةداعإ وحاتفملا لالخاد م دختسمل رمأل رادصإب موقت ىتح حىتافملا رىفش ت متى ال . الو م دقتل حاتفملا لالخاد م دختسمل

رورملا ةم لك ريفشت

حاتفملا قارتخأ متي مل ام ايرورض سيل هنأ نم مغرلا يلغ) يساسألا حاتفملا ريفيغت نكمي
ديدل [يساسألا حاتفملا] عم ىرخأ ةرم رمألا config-key... حاتفملا مادختساب (ام ةقيرطب
ديدل حاتفملا مادختساب هجوملا نيوكت يفة للاح ةرفشم حيتافم ية ريفشت ةداعإ مت

ىلا اذه يةوي، كلذ عمو no key config-key... رمألا رادصإ دنع يساسألا حاتفملا فذح كنكمي
ةلاسر ضرعت) ةديفم ريف هجوملا نيوكت يفة للاح اهن نيوكت مت يةلا حيتافملا عيمج لعلج
دعي مل يساسألا حاتفملا نأل ارظن. (يساسألا حاتفملا فذح دكويو رمألا اذه حضوي ريدحت
هجوملا ةطساوب اهمادختساو 6 عونلا نم رورملا تاملك ريفشت كف نكمي ال، ادجوم



ةم لك ريفشت رمأ aes ةلازا و يساسألا حاتفملا ةلازا موقت ال، ةينمأ بابسأل: ةظحالم
ال. اهريفشت كف متي ال، رورملا تاملك ريفشت درجمبو. هجوملا نيوكت يفة رورملا تاملك ريفشت كف رورملا
يساسألا حاتفملا ةلازا مدع ةطيرش نيوكتلا يفة للاح ةرفشملا حيتافملا ريفشت كف نكمملا نم لازي

عضو يف password logging رمأل مدختسأ ،رورملا ةملك ريفشت فئاظول debug عونلا لئاسر ةدهاشم لو ،كلذىل ةفاضل ابونىوكتلا

تانىوكتلا

ديدخت جاحسملال علكش اذى ةقوئو اذى لمعتسى

•

[يلاحلا اقبس مكرتشملا حاتملا ريفشت](#)

•

[يلعافت لكش بديج يساسأ حاتم ةفاضلا](#)

•

[يلعافت لكش بيلاحلا يساسأ حاتملا ليدعت](#)

•

[يساسأ حاتملا فذح](#)

```
<#root>
```

```
Router#
```

```
show running-config
```

```
Building configuration...
```

```
.  
.crypto isakmp policy 10  
  authentication pre-share  
crypto isakmp key cisco123 address 10.1.1.1  
.  
.  
endRouter#
```

```
configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.  
Router(config)#
```

```
key config-key password-encrypt testkey123
```

```
Router(config)#
```

```
password encryption aes
```

```
Router(config)#
```

```
^Z
```

```
Router#
```

```
Router#
```

```
show running-config
```

```
Building configuration...
```

```
.  
.   
password encryption aes  
.   
.   
crypto isakmp policy 10  
 authentication pre-share  
crypto isakmp key
```

```
6 FLgBaJHXdYY_AcHZZMgQ_RhTDJXHUBAAB
```

```
 address 10.1.1.1
```

```
.  
.   
end
```

يلعافت لكشپ ديدج يس اس احتفم قفاض!

```
<#root>
```

```
Router(config)#
```

```
key config-key password-encrypt
```

New key:

<enter key>

Confirm key:

<confirm key>

Router(config)#

يُلعافف لكش ب يلاحل يساس ألاحافملا لي دعت

<#root>

Router(config)#

key config-key password-encrypt

Old key:

<enter current key>

New key:

<enter new key>

Confirm key:

<confirm new key>

Router(config)#

*Jan 7 01:42:12.299: TYPE6_PASS: Master key change heralded,
re-encrypting the keys with the new primary key

يساس ألاتفملا فذح

<#root>

Router(config)#

no key config-key password-encrypt

WARNING: All type 6 encrypted keys will become unusable
Continue with primary key deletion ? [yes/no]:

yes

Router(config)#

ةحصلا نم ققحتلا

نويكتلا اذه ةحص نم ققحتلل ءارجا ايلاح دجوي ال

اهحالص او ءاطخألا فاشكتسا

ليكشت اذه ل رفوتي ةمولعم احوالص او ءاطخألا فاشكتسا صاخ نم ام ايلاح كانه

ةلص تاذا تاملعم

- [IPsec معده ةحفص](#)
- [Cisco نم تاليزنتلا او ينفلا معدلا](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت
م ل ا ل اء ان ا ع مچ ي ف ن م دخت س م ل ل م عد و ت ح م م دقت ل ة يرش ب ل و
امك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ال 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 م د ق ي ي ت ل ا ة ي ف ا ر ت ح ال ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ل ا ا م اء ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه 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