

ةلأحلا نع ةربعملا ISE ةسلج فانئتسا مهف TLS ل EAP-PEAP

تايوتحملا

[ةمدقملا](#)

[ةيساسالا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسا تامولعم](#)

[نيوكتلا](#)

[ةحصللا نم ققحتلا](#)

[ةيلوالا ةقداصملا](#)

[ةقداصملا ةداعلا عانثا](#)

[قيركتملا ةلئسالا](#)

ةمدقملا

كرحم ةمدخ ةيوه Cisco في فانئتسا ةسلج (TLS) نم ةقبط transport لا ةقيثو اذه فصي (ISE).

ةيساسالا تابلطتملا

تابلطتملا

- (TLS) لقنلا ةقبط نامأ ةحفاصم ةيلمع ةفرعم
- يمحرملا (PEAP) عسوتملا ةقداصملا لوكوتورب قفدت ةفرعم
- Cisco نم ةيوهلا تامدخ كرحم ةفرعم

ةمدختسملا تانوكملا

ةيلاتلا ةيداملا تانوكملا اوجماربلا تارادصا ىلا دنتسملا اذه في ةدراولا تامولعملا دنتست

- Cisco Identity Services Engine، رادصا 3.2
- ISE (VM) يرهاظلا زاھجلا
- Windows 10 رتويېمك

ةصاخ ةيلمعم ةئيې في ةدوجوملا ةزهجالا نم دنتسملا اذه في ةدراولا تامولعملا عاشنإ مت تناك اذا. (يضا رتفا) حوسمم نيوكتب دنتسملا اذه في ةمدختسملا ةزهجالا عيمج تأدب رما يال لم تحملا ريثأتلا ل كمهف نم دكأتف، ليغشتلا ديقتك كبش

ةيساسا تامولعم

حفاصم ل ةيفاضإل افاقفنل ىلع ءاضقلل مدختست ةينقت وه TLS ةسلج فانئتسإ نإ ةسلج فانئتساب اقباس TLS ةسلج أشنأ يذل مدخالل لمعمل حمست يهو. ةيلولأل TLS ةريثك دراوم بلطتت يتل حفاصم ل ةيلمع راركت نودب لمعل

ايازل

- بلطتت يتل ةيلولأل حفاصم ل تاوطخ بنجت لالځ نم لوصول نمز نم للقي وه ف .ك.لذب مايقلل مزالل تقولل ةريثك دراوم
- لدابتل تايلمع يطخت لالځ نم مدخال ىلع ةيباسحل لامحال ليقلت ىلع لمعي امك .تاداهشل ءحص نم ققحتل اوحي تافم لل فثكم ل

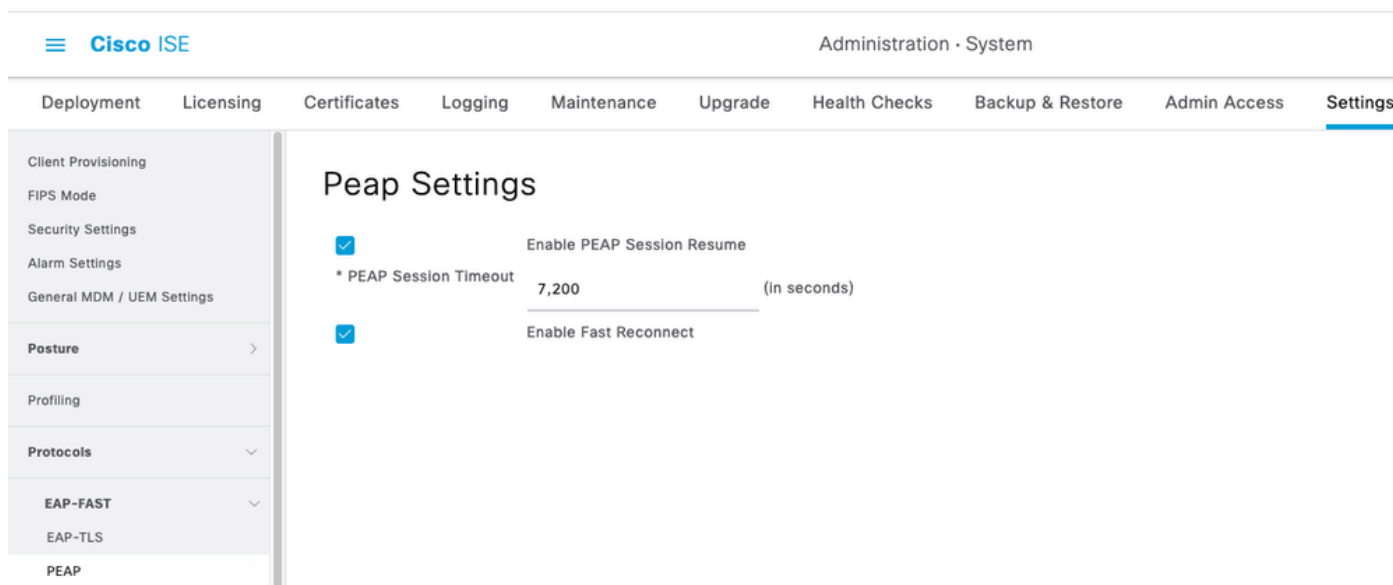
نيوكتل

PEAP ل فانئتسا ، TLS ةسلج نيكم تل ، ISE ىلع

PEAP ةسلج فانئتسإ نيكم ت عجار > PEAP > تالوكتورب > تاداعإ > ماظن > ةرادإ

يناث 7200 ل ةسلجل ISE لمحي ، يضارتفا لكشب

بولسأل يلاوتل ىلع يطختي يذلو ، عيرسل ل لصوتل ةداعإ نيكم ت كنكمي ، اي راي تخإ تاقيبطت ي ف هيف بوغرم وهو . عرسأ لكشب ءقداصم ل ةداعإ ب ىتح حمسيو PEAP ل يلخادلا يكلسلال لاوتل لثم



ISE PEAP لمع ةسلج فانئتساب صاځل نيوكتل

بللاطم ل ي ف عيرسل ل لاصتال ةداعإ نيكم ت اضيأ بجي

عيرسل ل لاصتال ةداعإ نيكم تل يلصلأل Windows بللاطم ب صاځ نيوكتل اذه

Protected EAP Properties



When connecting:

☐ Verify the server's identity by validating the certificate

☐ Connect to these servers (examples: srv1;srv2;.*\srv3\,com):

Trusted Root Certification Authorities:

- ☐ Baltimore CyberTrust Root
- ☐ Class 3 Public Primary Certification Authority
- ☐ DigiCert Assured ID Root CA
- ☐ DigiCert Global Root CA
- ☐ DigiCert Global Root G2
- ☐ DigiCert Global Root G3
- ☐ DigiCert High Assurance EV Root CA



Notifications before connecting:

Tell user if the server's identity can't be verified

Select Authentication Method:

Secured password (EAP-MSCHAP v2)



Configure...

☒ Enable Fast Reconnect

☐ Disconnect if server does not present cryptobinding TLV

☐ Enable Identity Privacy

OK

Cancel

ةركاذي ف اهب ظافتحال مت دق هنأو،ةسلجلال فرعم عم ءحفاصملا لئاسر ةيؤر كنكمي
تقؤملا نينختلا

```
Crypto,2024-02-12 19:13:20,542,DEBUG,0x7f8f923fc700,NIL-CONTEXT,Crypto::Result=0, Crypto.SSLConnection.
Crypto,2024-02-12 19:13:20,542,DEBUG,0x7f8f923fc700,NIL-CONTEXT,Crypto::Result=0, Crypto.SSLConnection
Crypto,2024-02-12 19:13:20,542,DEBUG,0x7f8f923fc700,NIL-CONTEXT,Crypto::Result=0, Call TLS Notify Callb
Eap,2024-02-12 19:13:20,542,DEBUG,0x7f8f923fc700,cntx=0000452308,sesn=labpan01/494696177/7940,CPMSessio
Eap,2024-02-12 19:13:20,542,DEBUG,0x7f8f923fc700,cntx=0000452308,sesn=labpan01/494696177/7940,CPMSessio
0000: 86 91 75 26 6f af 4e ec 5f b4 33 4f 81 9e 25 22 ..u&o.N._.30..%"
0010: 1f a0 cf 3c bf 0e 45 88 06 36 90 63 db a5 92 07 ...<..E..6.c.... ,EapTlsProtocol.cpp:1473
Crypto,2024-02-12 19:13:20,542,DEBUG,0x7f8f923fc700,NIL-CONTEXT,Crypto::Result=0, Crypto.SSLConnection.
Crypto,2024-02-12 19:13:20,542,DEBUG,0x7f8f923fc700,NIL-CONTEXT,Crypto::Result=0, Crypto.SSLConnection.
Crypto,2024-02-12 19:13:20,542,DEBUG,0x7f8f923fc700,NIL-CONTEXT,Crypto::Result=0, Call TLS Notify Callb
Crypto,2024-02-12 19:13:20,543,DEBUG,0x7f8f923fc700,NIL-CONTEXT,Crypto::Result=0, Crypto.SSLConnection.
Crypto,2024-02-12 19:13:20,543,DEBUG,0x7f8f923fc700,NIL-CONTEXT,Crypto::Result=0, Crypto.SSLConnection.
Crypto,2024-02-12 19:13:20,543,DEBUG,0x7f8f923fc700,NIL-CONTEXT,Crypto::Result=0, Call TLS Notify Callb
Crypto,2024-02-12 19:13:20,581,DEBUG,0x7f8f923fc700,NIL-CONTEXT,Crypto::Result=0, Crypto.SSLConnection.
Crypto,2024-02-12 19:13:20,581,DEBUG,0x7f8f923fc700,NIL-CONTEXT,Crypto::Result=0, Crypto.SSLConnection.
Crypto,2024-02-12 19:13:20,581,DEBUG,0x7f8f923fc700,NIL-CONTEXT,Crypto::Result=0, Call TLS Notify Callb
Crypto,2024-02-12 19:13:20,581,DEBUG,0x7f8f923fc700,NIL-CONTEXT,Crypto::Result=0, Crypto.SSLConnection.
Crypto,2024-02-12 19:13:20,581,DEBUG,0x7f8f923fc700,NIL-CONTEXT,Crypto::Result=0, Crypto.SSLConnection.

Crypto,2024-02-12 19:13:20,737,DEBUG,0x7f8f91df9700,NIL-CONTEXT,shutting session id
0000: 86 91 75 26 6f af 4e ec 5f b4 33 4f 81 9e 25 22 ..u&o.N._.30..%"
0010: 1f a0 cf 3c bf 0e 45 88 06 36 90 63 db a5 92 07 ...<..E..6.c.... ,SSLConnection.cpp:337
Crypto,2024-02-12 19:13:20,737,DEBUG,0x7f8f91df9700,NIL-CONTEXT,Crypto::Result=0, Crypto.SSLConnection.
```

رييغت ريياعمو Client Key Exchange جم انرب مادختساب لي لمعلا بيحتسي ،كلذ دعب
ريفشلا

```

  Attribute Value Pairs
  > AVP: t=User-Name(1) l=26 val=host/LABPCSK.vmlab.local
  > AVP: t=Service-Type(6) l=6 val=Framed(2)
  > AVP: t=Vendor-Specific(26) l=27 vnd=ciscoSystems(9)
  > AVP: t=Framed-MTU(12) l=6 val=1500
  > AVP: t=Called-Station-Id(30) l=19 val=70-81-05-C6-82-C7
  > AVP: t=Calling-Station-Id(31) l=19 val=B4-96-91-26-DE-2E
  > AVP: t=EAP-Message(79) l=170 Last Segment[1]
    Type: 79
    Length: 170
    EAP fragment: 02d200a8198000000009e1603030066100000626104ffebcf6f6dc1691906e89d323be55d...
  Extensible Authentication Protocol
    Code: Response (2)
    Id: 210
    Length: 168
    Type: Protected EAP (EAP-PEAP) (25)
  > EAP-TLS Flags: 0x80
    EAP-TLS Length: 158
  Transport Layer Security
    > TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
    > TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
    > TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message

```

يرى تامس وولي عمال حات فم لدابت

TLS. ةحفاص موري غتال ريفشت تافصاوم لامتك اعم اضي امدخال بيحتسي، اريخ او

```

  Attribute Value Pairs
  > AVP: t=State(24) l=78 val=333743504d53657373696f6e49443d304136413235443030303030303031303030333045...
  > AVP: t=EAP-Message(79) l=59 Last Segment[1]
    Type: 79
    Length: 59
    EAP fragment: 01d300391900140303000101160303002886fb6f8346c90902674f55d75068aebda907a7...
  Extensible Authentication Protocol
    Code: Request (1)
    Id: 211
    Length: 57
    Type: Protected EAP (EAP-PEAP) (25)
  > EAP-TLS Flags: 0x00
  Transport Layer Security
    > TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
    > TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message

```

مدخال بناج نم ريفشتال تافصاوم ريغت

ءانثا ثدت ةلمالك ال TLS ةحفاص م نأ ىرت نأ كنكمي، رشابم ال RADIUS لچس تاوطخ في
ىلوال ةقداصم ال

12800 Extracted first TLS record; TLS handshake started
12805 Extracted TLS ClientHello message
12806 Prepared TLS ServerHello message
12807 Prepared TLS Certificate message
12808 Prepared TLS ServerKeyExchange message
12810 Prepared TLS ServerDone message

12812 Extracted TLS ClientKeyExchange message
12803 Extracted TLS ChangeCipherSpec message
12804 Extracted TLS Finished message
12801 Prepared TLS ChangeCipherSpec message
12802 Prepared TLS Finished message
12816 TLS handshake succeeded
12310 PEAP full handshake finished successfully

RADIUS Live TLS لاصرتا ديكأت تاووطخ

Microsoft Challenge Handshake Authentication Protocol (MSCHAPv2) لوكوتورب ةقداصم ذيفنتب يلخادل بولسأل موقي امك لمالكالب

- 12313 PEAP inner method started
- 11521 Prepared EAP-Request/Identity for inner EAP method
- 12305 Prepared EAP-Request with another PEAP challenge
- 11006 Returned RADIUS Access-Challenge
- 11001 Received RADIUS Access-Request
- 11018 RADIUS is re-using an existing session
- 12304 Extracted EAP-Response containing PEAP challenge-response
- 11522 Extracted EAP-Response/Identity for inner EAP method
- 11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge

RADIUS Live لجسمل يلخادال بولسأل تاوطخ

ةقداصملا ةداعإ ءانثأ

اهسفن ةسلجلال فرعم ليمعلا لسري ،ةقداصملا ةداعإ ءانثأ
يذل Client Hello في 869175266faf4eec5fb4334f819e25221fa0cf3cbf0e45806369063dba59207
ةيلوالا ةقداصملا نم ملعت

13	10	10.106.37.208	10.127.197.164	RADIUS	582 Access-Request id=86
14	10	10.106.37.208	10.127.197.164	RADIUS	583 Access-Request id=86


```

Code: Access-Request (1)
Packet identifier: 0x56 (86)
Length: 540
Authenticator: f02d6c9bc16d1ec04bbf9a76f2fd77b
[The response to this request is in frame 14]
Attribute Value Pairs
  > AVP: t=User-Name(1) l=26 val=host/LABPCSK.vmlab.local
  > AVP: t=Service-Type(6) l=6 val=Framed(2)
  > AVP: t=Vendor-Specific(26) l=27 vnd=ciscoSystems(9)
  > AVP: t=Framed-MTU(12) l=6 val=1500
  > AVP: t=Called-Station-Id(30) l=19 val=70-81-05-C6-82-C7
  > AVP: t=Calling-Station-Id(31) l=19 val=B4-96-91-26-DE-2E
  > AVP: t=EAP-Message(79) l=206 Last Segment[1]
    Type: 79
    Length: 206
    EAP fragment: 023900cc1980000000c216030300bd010000b9030365ca25445d1bc5d267140a0569c193...
  > Extensible Authentication Protocol
    Code: Response (2)
    Id: 57
    Length: 204
    Type: Protected EAP (EAP-PEAP) (25)
    > EAP-TLS Flags: 0x80
    EAP-TLS Length: 194
    > Transport Layer Security
      > TLSv1.2 Record Layer: Handshake Protocol: Client Hello
        Content Type: Handshake (22)
        Version: TLS 1.2 (0x0303)
        Length: 189
        > Handshake Protocol: Client Hello
          Handshake Type: Client Hello (1)
          Length: 185
          Version: TLS 1.2 (0x0303)
          > Random: 65ca25445d1bc5d267140a0569c193446ace0334e68b64509f5220928b0e65c6
          Session ID Length: 32
          Session ID: 869175266faf4eec5fb4334f819e25221fa0cf3cbf0e458806369063dba59207
          Cipher Suites Length: 42
          > Cipher Suites (21 suites)

```

لمعمل قس لچ فانئستس ءانثا ليملعل ببي حرت

قبط قس لچل تقؤم لانيختللا ةركاذي ف دوجوم اذه لمعمل قس لچ فرعم نأ ISE دكؤي ،كلذ دعب
ال .رصتخم ل TLS لاصتا ديكأت مساب فرعي امب رمي امهالكو (SSL) ةنمآل ليصوتل ذخأم
مادختس ءداعإ متي و ةرصتخم ل TLS ءحفاصم ءانثا ءاتفم تامولعم وأ ءداهش يآ لدابت متي
اقبس م اهيلع ضوافتل م تي ل ءياتفم ل

Crypto,2024-02-12 19:33:48,821,DEBUG,0x7f8f925fd700,NIL-CONTEXT,Crypto::Result=0, Call TLS Notify Callb
Crypto,2024-02-12 19:33:48,821,DEBUG,0x7f8f925fd700,NIL-CONTEXT,Crypto::Result=0, Crypto.SSLConnection.
Crypto,2024-02-12 19:33:48,821,DEBUG,0x7f8f925fd700,NIL-CONTEXT,Crypto::Result=0, Crypto.SSLConnection.
Crypto,2024-02-12 19:33:48,821,DEBUG,0x7f8f925fd700,NIL-CONTEXT,Crypto::Result=0, Call TLS Notify Callb
Crypto,2024-02-12 19:33:48,821,DEBUG,0x7f8f925fd700,NIL-CONTEXT,Crypto::Result=0, Crypto.SSLConnection.
Crypto,2024-02-12 19:33:48,821,DEBUG,0x7f8f925fd700,NIL-CONTEXT,Crypto::Result=0, Crypto.SSLConnection.

TLS. ةحفاصم ةزيم لامكإو ريشفشتلا تافصاوم رييغت عم اضيأ لي م عمل بي جتسي ،اريخأو

15	10	10.106.37.208	10.127.197.164	RADIUS	439 Access-Request id=87
16	10	10.127.197.164	10.106.37.208	RADIUS	206 Access-Challenge id=87

Frame 15: 439 bytes on wire (3512 bits), 439 bytes captured (3512 bits)
Ethernet II, Src: Cisco_fd:ad:f9 (4c:e1:76:fd:ad:f9), Dst: VMware_8b:e7:12 (00:50:56:8b:e7:12)
Internet Protocol Version 4, Src: 10.106.37.208, Dst: 10.127.197.164
User Datagram Protocol, Src Port: 1645, Dst Port: 1645
RADIUS Protocol
Code: Access-Request (1)
Packet identifier: 0x57 (87)
Length: 397
Authenticator: 1eed5f9362cc3c9c9c7c60bb5c06a50b
[\[The response to this request is in frame 16\]](#)
Attribute Value Pairs
AVP: t=User-Name(1) l=26 val=host/LABPCSK.vmlab.local
AVP: t=Service-Type(6) l=6 val=Framed(2)
AVP: t=Vendor-Specific(26) l=27 vnd=ciscoSystems(9)
AVP: t=Framed-MTU(12) l=6 val=1500
AVP: t=Called-Station-Id(30) l=19 val=70-81-05-C6-82-C7
AVP: t=Calling-Station-Id(31) l=19 val=B4-96-91-26-DE-2E
AVP: t=EAP-Message(79) l=63 Last Segment[1]
Type: 79
Length: 63
EAP fragment: 023a003d19800000003314030300010116030300280000000000000faee969b85aa09...
Extensible Authentication Protocol
Code: Response (2)
Id: 58
Length: 61
Type: Protected EAP (EAP-PEAP) (25)
EAP-TLS Flags: 0x80
EAP-TLS Length: 51
Transport Layer Security
TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message

لي م عمل رييغت ريشفشت تافصاوم لم عمل قس ل ج فان ئتسإ

ةقداصلملا ةداعإ ءانثأ ثدحت ةرصتخملا TLS ةحفاصم نأ ىرت نأ كنكمي ،رشابملا RADIUS ل ج س تاوطخ يف

12800 Extracted first TLS record; TLS handshake started
12805 Extracted TLS ClientHello message
12806 Prepared TLS ServerHello message
12801 Prepared TLS ChangeCipherSpec message
12802 Prepared TLS Finished message
12803 Extracted TLS ChangeCipherSpec message
12804 Extracted TLS Finished message
12816 TLS handshake succeeded
12311 PEAP session resumed successfully

RADIUS Live Log TLS لمع قس ل ج فانئئس إ تاو ط خ

.ه ي ط خ ت م ت ي ل خ ا د ل ا ب و ل س أ ل ا ن أ ى ر ت ن أ ك ن ك م ي ، ع ق د ا ص ل ا ع د ا ع إ ي ف

12312 PEAP fast-reconnect - skipping inner method

RADIUS Live ل ج ل PEAP ب ع ي ر س ل ل ا ص ت ا ل ا ع د ا ع إ

ة ر ك ت م ل ا ة لئ س أ ل ا

اهض ع ب ن ع ل ق ت س م ل ك ش ب ة ع ر س ب ل ا ص ت ا ل ا ع د ا ع إ و ل م ع ل ا ة س ل ج ف ا ن ئ ت س إ م ت ي ل ه 1)
ض ع ب ل ل

.ة ق د ا ص ل ل ل ة ل خ ا د ل ا ة ق ي ر ط ل ا ز و ا ج ت ا ه ي ف م ت ي ة ي ر ا ي ت خ ا ة ز ي م ع ي ر س ل ل ا ل ا ص ت ا ل ا ع د ا ع إ ، م ع ن
ل م ع ل ا ة س ل ج ف ا ن ئ ت س إ " ن ي ك م ت د ن ع ع ي ر س ل ل ا ل ا ص ت ا ل ا ع د ا ع إ ن ي ك م ت ا ي م ا ز ل ا س ي ل

2) ة ي ن م أ ر ط ا خ م ي أ ل ا ة ف ن أ ت س م ل ا ة س ل ج ل ا ن ي ك م ت ي د و ي ل ه

ض ر ع ت س م ل ا ع م ة ي ل و أ ل ا ة ح ف ا ص م ل ا ء ا ن ث أ ي ئ ا و ش ع ل م ع ة س ل ج ف ر ع م ن ي ي ع ت ب م د ا خ ل ا م و ق ي
ح ي ت ا ف م ل ا ة ف ا ض ل ا ب ه ذ ه ل م ع ل ا ة س ل ج ف ر ع م ن ي ز خ ت ب م د ا خ ل ا و ل ي م ع ل ا م و ق ي . (ل ي م ع ل ا)
ل م ع ل ا ة س ل ج ف ر ع م ل ي م ع ل ا ل س ر ي ، ل م ع ة س ل ج ف ا ن ئ ت س ل . ل ا ص ت ا ل ا ت ا ل ا ح و ل م ع ل ا ة س ل ج
ل ا ص ت ا ل ا ل ع م د ا خ ل ا ف ر ع ت ا ذ ا . م د ا خ ل ا ل ا (ClientHello) ل و أ ل ا ل و ك و ت و ر ب ل ا ة ل ا س ر ع م ة ن ز خ م ل ا
ة س ل ج ل ا ء ا ش ن إ ع د ا ع ل ا ة س ل ج ل ا ف ر ع م س ف ن ب د ر ي ه ن إ ف ، ة س ل ج ل ا ف ا ن ئ ت س ل ا ا د ع ت س م ن ا ك و

ةداعإب موقت كنأل ارظن نامألل دقف نودو ةعرسب نم آلاصتا عاشنإب حمسي اذهو. ةلباقملا اقبسماهي لع ضوافتلا مت يتلا لمعلا ةسلج تانايب مادختسا

3) ىرخأ دقع ىلإ TLS لمع تاسلج تافرعم خسنت له

ةداعإ ةلاح يف. ىرخأ PSNs ىلإ رركي الو. هسفن PSN ل ىلع ننخم IDs ةسلج TLS ل، نم ام ةركاذ نم لمعلا تاسلج تافرعم عيجم دقف نكمي، PSN ل ةمدخل ل يغشت ةداعإ وأ ليغشتلا ةيلاتلا ةرملال يف ةلماكل TLS ةحفاصم ثدحي نأ بجي وتقوملا ننزختلا

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م ج ر ت
م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م ج ر ت ل ض ف ا ن ا ة ط ح ا ل 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 م ج ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م ج ر ت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا ء ا د ع و ج ر ل ا ب ي ص و ت و ت ا م ج ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م 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 د ن ت س م ل ا