

ذيفنتلا تاي ل مع لس لس و EAP-FAST مه ف ISE و AnyConnect NAM لى ل

تاي و تحملا

[عم دم قملا](#)

[عم س اس ال ا تاب ل ط ت م لا](#)

[تاب ل ط ت م لا](#)

[عم د خ ت س م لا ت ا ن و ك م لا](#)

[عم ر ظ ن](#)

[ل ح ا ر م](#)

[ي م ح م لا ل و ص و ل ا ت ا غ و س م](#)

[\(PAC\) ذ ف ن م ل ا ب عم ا خ ل ا ل و ص و ل ا ي ف م ك ح ت ل ا م ئ ا و ق ا ش ن ا د ن ع](#)

[ISE و ACS 5x ل ب ا ق م ACS 4.x م د ا خ ل ل ي س ي ئ ر ح ا ت ف م EAP-FAST](#)

[ل م ع ل ا عم س ل ج ف ا ن ئ ت س ا](#)

[م د ا خ ل ا عم ل ا ح](#)

[\(ي م ح م لا ل و ص و ل ا غ و س م ي ل ا د ن ت س م\) عم ل ا ح ل ا م ي د ع](#)

[AnyConnect NAM ذ ي ف ن ت](#)

[\(0 عم ل ح ر م ل ا\) ي م ح م لا ل و ص و ل ا ت ا غ و س م د ا د م ا](#)

[ل و ه ج م TLS ق ف ن](#)

[ق د ص م ل ا TLS ق ف ن](#)

[EAP-Chaing](#)

[PAC ت ا ف ل م ن ي ز خ ت م ت ي ث ي ح](#)

[AnyConnect NAM 3.1 ل ب ا ق م 4.0](#)

[عم ل ث م ال ا](#)

[عم ك ب ش ل ل ي ط ي ط خ ت ل ا م س ر ل ا](#)

[عم ل ال ا و م د خ ت س م ل ل ي م ح م لا ل و ص و ل ا غ و س م عم ل ص ا و ت ل ا ب EAP ن و د ب EAP-FAST](#)

[PAC ل ي ص و ت عم ا ع ا ب ع ي ر س ل ا EAP ل ي ص و ت عم EAP-FAST](#)

[PAC ن و د ب EAP ل ي ص و ت عم EAP-FAST](#)

[EAP لس لس ت ل ا ض ي و ف ت ل PAC عم ا ح ل ص ا ه ت ن ا عم EAP-FAST](#)

[ه ت ي ح ل ص ت ه ت ن ا PAC ي ل س لس ت ق ف ن EAP عم EAP-FAST](#)

[ل و ه ج م TLS ق ف ن PAC ر ي ف و ت و EAP لس لس ت عم EAP-FAST](#)

[ط ق ف م د خ ت س م ل ا عم د ا ص م ل ص و ي EAP عم EAP-FAST](#)

[عم ن م ا ز ت م ل ا ر ي غ TLS ق ف ن ت ا د ا د ع ا و EAP لس لس عم EAP-FAST](#)

[ا ح ل ص ا و ا ط خ ال ا ف ا ش ك ت س ا](#)

[\(ISE\) عم ي و ه ل ا ف ش ك ت ا م د خ ك ر ح م](#)

[AnyConnect NAM](#)

[ع ج ا ر م ل ا](#)

عم دم قملا

Cisco ن م (NAM) عم ك ب ش ل ل ا ل و ص و ل ا ر ي د م لى ل EAP-FAST ق ي ب ط ت ب عم ل ع ت م ل ا ل ي ص ا ف ت ل ا ل ا ق م ل ا ا ذ ه ح ر ش ي عم ي ح ذ و م ن عم ل ث م ا و ت ا ل ا ح م د ق ي و ا ع م عم د ح م ل ا ت ا ز ي م ل ا ل م ع عم ي ف ي ك ح ر ش ي ا م ك (ISE) عم ي و ه ل ا ت ا م د خ ك ر ح م و AnyConnect م ا د خ ت س ل ل .

- حاتفملا ةطساوب كلذ لك ريفشت مت - مدختسمل اةوه (PAC حاتفم) PAC مت عم (EAP-FAST مداخل يسيرلرا)
- (TTL تاتقؤم، مداخل فرعم) PAC تامولعم

لوصول تاغوسم ةوه وحاتفم ريفشتب يمحملا لوصول تاغوسم رصبي يذلا مداخل موقبي يمحملا لوصول غوسم يف متعم وه) EAP-FAST مداخل يسيرلرا حاتفملا مادختساب يمحملا ىرخا تامولعم يا نزي / ظفحتي ال . ليمعلا الى لمالكلا يمحملا لوصول غوسم لسريو (PAC) (PACs عيمجل هسفن وه يذلا يسيرلرا حاتفملا ادعام) .

حاتفملا مادختساب اهريفشت كفتي ، (PAC) يمحملا لوصول غوسم متعم يقلت درجمبو لوصول تاغوسم حاتفم مادختسا متي . اهتخص نم ققحتل متي و EAP-FAST مداخل يسيرلرا TLS قفنل لمعلا تاسلج حياتفم و ةيسيرلرا TLS حياتفم صالختسال (PAC) يمحملا رصتخملا .

ق. باسلا يسيرلرا حاتفملا ةيخالص اءهتنا دنع ةديج EAP-FAST مداخل حياتفم اءشنا متي يسيرلرا حاتفم لاطبا نكمي ، تالاحل صعب يف .

ايلاح ةمدختسمل يمحملا لوصول تاغوسم نم عاونأ ةدع كانه

- مت . (مداخل و اليمع ةءاهش الى ةجال نوب) TLS قفن اءشنا مدمختسي : قفنل PAC TLS Client Hello يف لاسرالا
- يروفلا زاهلج حيرصتو TLS قفن اءشنا مدمختسي : يلالا (PAC) يمحملا لوصول غوسم TLS Client Hello يف لاسرالا مت
- مدمختسمل اةقداصل مدمختسي : مدمختسمل اضيوفتل (PAC) يمحملا لوصول غوسم لخال لاسرالا مت . مداخل لبق نم هب اءومسم ناك اذا (يخالل بولسألي طخت) ةيروفلا TLV مادختساب TLS قفن
- زاهلل ةيروفلا اةقداصل مدمختسي : زاهلج اضيوفتل (PAC) يمحملا لوصول غوسم TLS قفن لخال لاسرالا مت . مداخل لبق نم هب اءومسم ناك اذا (يخالل بولسألي طخت) TLV مادختساب
- جهن و ابيئب شيءحت اءلج دنع ليءوختلل مدمختسي : TrustSec ل PAC

ميسلست نكمي امك 0. ةلحرملا يف ابيئقلا لءه يمحملا لوصول تاغوسم عيمج ميسلست متي ايودي (Tunnel، Machine، TrustSec) يمحملا لوصول تاغوسم صعب

(PAC) ذفنملا بةصال لوصول يف مكحتل اءواق اءشنا دنع

- مل اذا (ةيخالل ةقيرط) ةءجان اةقداصل مدمختسي : قفنل ربع (PAC) يمحملا لوصول غوسم اءباس هءادختسا متي
- (ةيخالل ةقيرط) ةءجانل اةقداصل مدمختسي : لءوختلل (PAC) يمحملا لوصول غوسم اءباس هءادختسا متي مل اذا
- (ةيخالل ةقيرط) ةءجانل زاهلج اةقداصل مدمختسي : زاهلل (PAC) يمحملا لوصول غوسم لءوختلل (PAC) يمحملا لوصول غوسم مادختسا مدمختسي اءواس هءادختسا متي مل اذا نكلو ، قفنل ربع (PAC) يمحملا لوصول غوسم ةيخالص اءهتنا دنع اهءدقت مءسي مءي فوسو . اضيوفتل (PAC) يمحملا لوصول غوسم ةيخالص اءهتنا دنع سيل هءل طعت و EAP-Chaining نءمء دنع هريفوت

ةظالم:

ةلاح اءنثتساب ةءجان اةقداصل يمحملا لوصول غوسم يف ريفوت ةيلمع لك بلطت يمحملا لوصول غوسم الى لوصول غوسم مدمتعمل مدمختسمل بلطي : ةيئال مادختسال AD باسح هءل سيل يذلا زاهلل

ي: قبائتسال شيءحتلا و اءملا ةفيظو يئاللا لوءلل صللي

لوصول غوسم عون يحمل	v1/v1a/CTS قفنل	ةآ	دامتعالا دادعالا يلع طقف انه ناك اذوق قدصملا لوصول نزخمل بلط فنلل (PAC) يحملا اضي
لوصول تاغوسم ريفوت معن بلل طال دنع (PAC) يحملا دادمال دنع		ديوزتلا يلع طقف قداصملا	ادختسا مدع ةلاح يف ف ةقداصملا هذه يف
لوصول تاغوسم مديقت معن بلل طال دنع (PAC) يحملا ةقداصملا دنع		معن	ال
لوصول تاغوسم مديقت معن بلل طال دنع (PAC) يحملا يقا بتسا شي دحت ريفوت يلا عوچرلا دنع يحملا لوصول تاغوسم لش ف دعب (PAC)		ال	ال
ريفوت مدع و ضفر يلا ةدنتسملا ةقداصملا يديجل يحملا لوصول تاغوسم دنع، لاثملا ليلبس يلع) غوسم ةيخالص اهتنا (PAC) يحملا لوصول ACS 4.x PACs مدع	J Tunnel PAC v1/v1a	ريفوت مدع و ضفر يديجل	ريفوت مدع و ضفر يديجل
		معن	ال

ISE و ACS 5x لباقم ACS 4.x مداخلل يسيئرلحات ف EAP-FAST

ISE و ACS 4.x ةنراقم دنع يسيئرلحات فملا ةجالعام يف طيسب فالختخا كانه

ةزيملا	ACS 4.1.2	ACS 5.x / ISE
حات فملا يسيئرلا	حات فملا يوتحي ةدم يلع يسيئرلا ن انكمي و (TTL) اقبلا ادعاقاتم و اطشن نوكي ةيخالصلا يهتتم و	حات فملا عاشنلا متي نم ايئاقلت يسيئرلا ةرتف لك يف ةيادبلا نكمي. اهنوكت مت ةينمز يلا امئاد لوصول "يسيئرلحات فملا" يهتنت ال م، ددح ادبا هتيخالص
شي دحت تاغوسم لوصول يحملا	شي دحت لاسرا متي يحملا لوصول غوسم دنع مداخلل ةطساوب غوسم ةيخالص اهتنا (PAC) يحملا لوصول ةيخالص تهتنا اذا ال يسيئرلحات فملا ريفشتل مدختسملا يحملا لوصول غوسم	شي دحت لاسرا متي يحملا لوصول تاغوسم دعب مداخلل ةطساوب (PAC) متي ةحجان ةقداصم لو ةينمز ةرتف يف اهذيفنت نيوكتلل ةلباق ةدح ةيخالص اهتنا ةطحل لبق يحملا لوصول تاغوسم (PAC).

اديح اجات فم ئشنني و ةميدقلا ةيسيئرلحات فملا عي مجب ISE ظفتحتيس، رخا ينعمبو
متيس، يهتني نا نكمي ال يسيئرلحات فملا نا امب. عوبسالا يف ةرم يضا رتفا لكش ب
طقف PAC TTL ةحص نم ققحتلا

-> لوكوتوربلا -> تاداعال -> ةرادال نم ISE يسيئرلحات فملا عاشنلا ةرتف نيوكت متي
EAP-FAST تاداعال -> EAP-FAST.

لمعلا ةسلج فانئتسا

ةداعإب حمسي وهو. قف نلل (PAC) يحمملا لوصولا غوسم مادختساب حمسي مهم نوكم اذه تاداهشلا مادختسا نودب TLS قف ن ضوافت.

ةميدعو مداخل ةلاح ىل ةدنتسم EAP-FAST ل تاسلجل فانئتسا عاون نم ناعون كانه (PAC) ىل ةدنتسم) ةلاحلا.

مدخال ةلاح

ىل ع اتقؤم نزخملا TLS لمع ةسلج فرعم ىل TLS ىل دننتسملا يسايقلا بولسأل دننتسي ةسلجل فانئتسال SessionID قافراق TLS Client Hello لسري يذلا ليمعلا موقى. مداخل TLS قف ن مادختسا دنن (PAC) يحمملا لوصولا غوسم ريفوتل طقف ةسلجل مادختسا متي لوهجم:

Source	Destination	Protocol	Length	Info	User-Name
10.62.148.109	10.48.17.14	RADIUS	378	Access-Request(1) (id=9, l= anonymous	
10.48.17.14	10.62.148.109	RADIUS	86	Access-Reject(3) (id=9, l=4	
10.62.148.109	10.48.17.14	RADIUS	301	Access-Request(1) (id=30, l anonymous	
10.48.17.14	10.62.148.109	RADIUS	193	Access-Challenge(11) (id=30	
10.62.148.109	10.48.17.14	RADIUS	510	Access-Request(1) (id=31, l anonymous	

Length: 138

Type: Flexible Authentication via Secure Tunneling EAP (EAP-FAST) (43)

▷ EAP-TLS Flags: 0x01

▽ Secure Sockets Layer

▽ TLSv1 Record Layer: Handshake Protocol: Client Hello

Content Type: Handshake (22)

Version: TLS 1.0 (0x0301)

Length: 127

▽ Handshake Protocol: Client Hello

Handshake Type: Client Hello (1)

Length: 123

Version: TLS 1.0 (0x0301)

▷ Random

Session ID Length: 32

Session ID: 9a344ae351082ec6dbafb8509cf99b4fa664574b6272f876...

Cipher Suites Length: 52

▷ Cipher Suites (26 suites)

Compression Methods Length: 1

▷ Compression Methods (1 method)

(يحمملا لوصولا غوسم ىل دننتسم) ةلاحلا ميدع

نيزختل زاهجلا/مدختسملا ضيوفتبا صاخلا (PAC) يحمملا لوصولا غوسم مادختسا متي رىظنلل ققبا سلا ضيوفتلاو ةقداصملا تالاح.

ةيأ نيزخت ىل مداخل جاتحي ال RFC 4507 ىل ليمعلا بناجل ةيتاذلا ةريسل دننتست TLS Client Hello قحلم ي PAC قافراق ليمعلا موقى كلذ نم الديو، اتقؤم تانايب ةطساوب (PAC) يحمملا لوصولا غوسم ةحص نم ققحتلا متي، ىلاتلابو. SessionTicket مداخل ىل هميلست مت يذلا قف نلل PAC ىل دننتسي لاثم. مداخل

	Source	Destination	Protocol	Length	Info	User-Name
23	10.62.148.109	10.48.17.14	RADIUS	301	Access-Request(1) (id=91, l=259)	anonymous
24	10.48.17.14	10.62.148.109	RADIUS	193	Access-Challenge(11) (id=91, l=151)	
25	10.62.148.109	10.48.17.14	RADIUS	666	Access-Request(1) (id=92, l=624)	anonymous
26	10.48.17.14	10.62.148.109	RADIUS	311	Access-Challenge(11) (id=92, l=269)	
27	10.62.148.109	10.48.17.14	RADIUS	437	Access-Request(1) (id=93, l=395)	anonymous
28	10.48.17.14	10.62.148.109	RADIUS	226	Access-Challenge(11) (id=93, l=184)	
29	10.62.148.109	10.48.17.14	RADIUS	468	Access-Request(1) (id=94, l=426)	anonymous
30	10.48.17.14	10.62.148.109	RADIUS	258	Access-Challenge(11) (id=94, l=216)	
31	10.62.148.109	10.48.17.14	RADIUS	516	Access-Request(1) (id=95, l=474)	anonymous
32	10.48.17.14	10.62.148.109	RADIUS	258	Access-Challenge(11) (id=95, l=216)	
33	10.62.148.109	10.48.17.14	RADIUS	452	Access-Request(1) (id=96, l=410)	anonymous

Secure Sockets Layer

- ▼ TLSv1 Record Layer: Handshake Protocol: Client Hello

- Content Type: Handshake (22)

- Version: TLS 1.0 (0x0301)

- Length: 281

- ▼ Handshake Protocol: Client Hello

- Handshake Type: Client Hello (1)

- Length: 277

- Version: TLS 1.0 (0x0301)

- ▶ Random

- Session ID Length: 0

- Cipher Suites Length: 52

- ▶ Cipher Suites (26 suites)

- Compression Methods Length: 1

- ▶ Compression Methods (1 method)

- Extensions Length: 184

- ▼ Extension: SessionTicket TLS

- Type: SessionTicket TLS (0x0023)

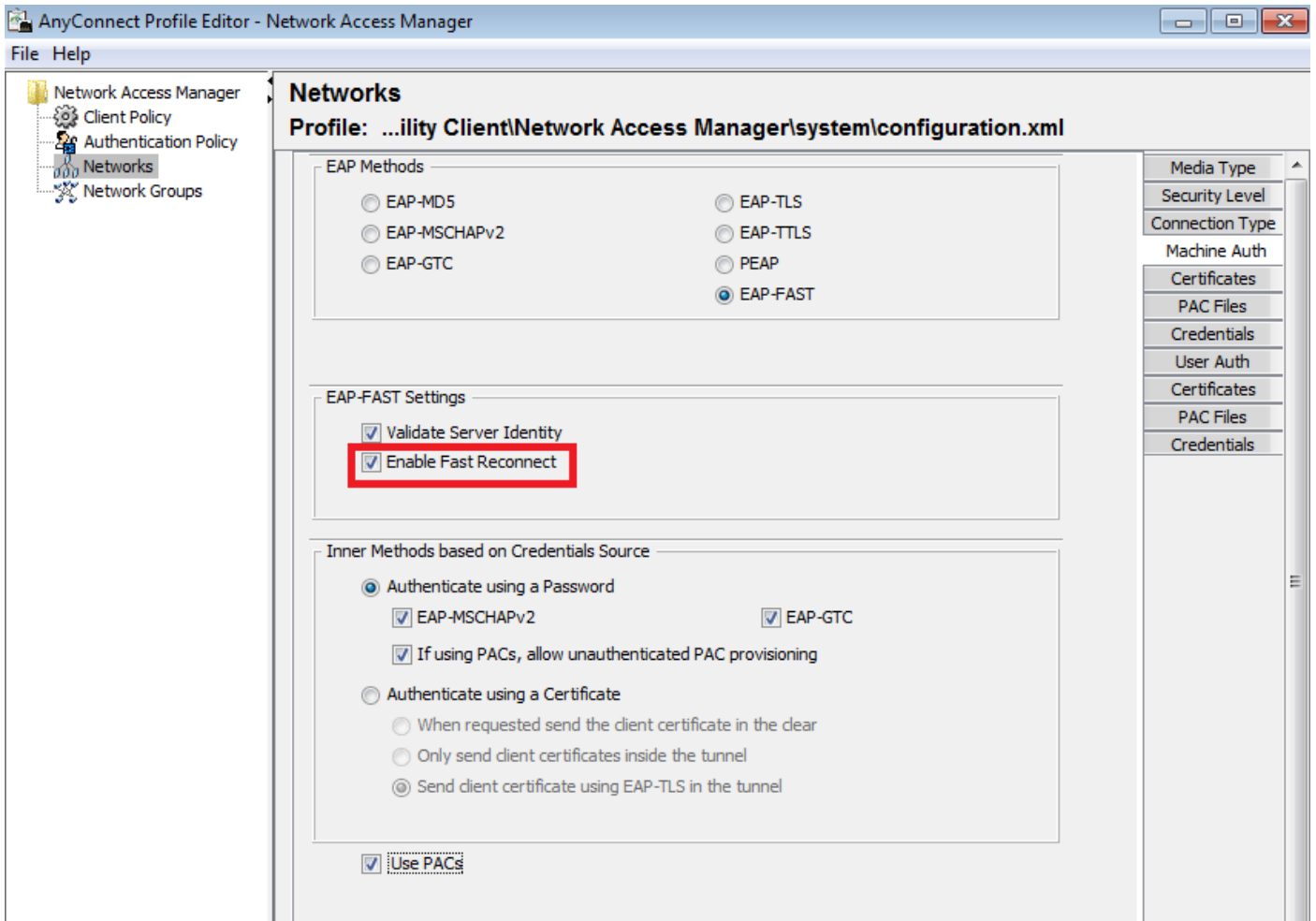
- Length: 180

- Data (180 bytes)

▶ AVP: l=18 t=Message-Authenticator(80): 0cb2477c076ea96d3ba150245e6291e8

ذيفنت AnyConnect NAM

اهنكلو - عيرسل لاصتالاداعإربع (AnyConnect NAM) ليمعالبناجل عاهنيكمت متي طوق ليوختلل (PAC) يمحمال لوصول تاغوسم مادختسا ي فمكحتلل مدختست



TLS قفناش نإل قف نلل يمحمل لوصول غوسم مدختست NAM لظتس، دادعإل ليطعت عم (PAC) يمحمل لوصول تاغوسم رمال اذه مدختسي نل، كلذ عمو. (ةبولطم تاداهش دجوت ال) بولسألا عم 2 ةلحرمل نوكتس، كلذل ةجيتنو. ةلأل او مدختس ملل يروفلا ضيوفتلل امئاد ةبولطم يلخادلا.

طوق هناف NAM لعل لالحل وه امكو. ةلالحل مبدع لمع ةسلج فانئتسإ نيكم تل راخي ISE امامأ مادختساب قف نلل يمحمل لوصول غوسم مادختسإ يف مكحتلال متي. PAC ليوختلل "يمحمل لوصول تاغوسم مادختسإ" تاراخيلا.

Allow EAP-FAST

EAP-FAST Inner Methods


Allow EAP-MS-CHAPv2

Allow Password Change Retries (Valid Range 0 to 3)

Allow EAP-GTC

Allow Password Change Retries (Valid Range 0 to 3)

Allow EAP-TLS

Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy 

Use PACs Don't Use PACs

Tunnel PAC Time To Live

Days 

Proactive PAC update will occur after % of PAC Time To Live has expired

Allow Anonymous In-Band PAC Provisioning

Allow Authenticated In-Band PAC Provisioning

Server Returns Access Accept After Authenticated Provisioning

Accept Client Certificate For Provisioning

Allow Machine Authentication

Machine PAC Time To Live

Weeks 

Enable Stateless Session Resume

Authorization PAC Time To Live

Hours 

Enable EAP Chaining

Preferred EAP Protocol


نيوكت مت اذا. رايخل نيوكت مت اذا (PAC) يمحمل لوصول تاغوسم مادختس NAM لواحس
PAC يمحمل لوصول تاغوسم ISE ملتساو ISE ي (PAC) يمحمل لوصول تاغوسم مادختس مدع
EAP لشف عاجراو يلات ال اطلخال نع غالبالا متيس، TLS دادتما ي قف نل

انه جاردا

تاداع (م) TLS SessionID لى لع انا ب فانئتس اةسلج نكمي نا اضي ايرورضال نام، ISE ي
ايضارتفا لطمع وه. (ةيمومع ال EAP-FAST

EAP FAST Settings

* Authority Identity Info Description

* Master Key Generation Period Weeks 

Revoke all master keys and PACs

PAC-less Session Resume

Enable PAC-less Session Resume

* PAC-less Session Timeout

مادختسا متي . فانئتسالا تاسلج نم طقف دحاو عون مادختسا نكمي هنا عارم عاجرلا متي و، PAC ىلع يوتحت ال يتلا رشنلا تاي لمعل طقف PAC ىلى دننتسم ال SessionID مادختسا، PAC رشن تاي لمعل طقف RFC ىلى دننتسم ال RFC 4507 مادختسا.

0) ةلحرمل (ي محملا لوصول تاغوسم دادم)

نم 0 ةلحرمل نوكتت . 0 ةلحرمل ي ف ايئاقلت (PAC) ي محملا لوصول تاغوسم ريفوت نكمي

- TLS قفن عاشن
- (ةلخادلا ةقيرطالا) ةقداصملا

لخاد ةحجان ةقداصم دعب (PAC) ذفنملا ب ةصاخلا لوصول ي ف مكحتلا مئاوق ميلست متي (PAC TLV فارتعا) PAC TLV ربع TLS قفن

لوهجم TLS قفن

مادختسا نكمملا نم ، ةيساسالا PKI ةينب نمضتت ال يتلا رشنلا تاي لمعل ةبسنلاب Diffie Hellman - ريفشت ةعومجم مادختساب لوهجملا TLS قفن عاشن متيس . لوهجم TLS قفن يرجت يتلا تامجهلا ي ف ناسنالا ىلى لي مي بارتقالا اذهو . ليمع وا مداخ ةداهش ىلى ةجالحا نودب (لخاتنالا) طسولا ي ف

ي لاتلا نوكملا رايلخا NAM بلطتت ، رايلخا اذه مادختسال

اذه) "هليلع قداصم ريغ PAC ريفوتب حمسي (PAC) ي محملا لوصول تاغوسم مادختسا ناك اذا" ةيساسالا PKI ةينب نودب هنا رورملا ةملك ىلى دننتسم ال يلخادلا بولسالا طقف ي قطنم (ةداهش ىلى دننتسم ال يلخادلا بولسالا مادختسا نكمي ال

ةقداصملا تالوكتورب بجومب اهنوكت مت يتلا ةيلاتلا تانوكملا ىلى ISE جاتحي امك اهب حومسملا

"لوهجملا قاطنالا لخاد PAC ديوزتبا حامسالا"

TrustSec (EAP-FAST) ل NDAC رشن تاي لمعل ي ف قاطنالا لخاد لوهجم PAC دادم مادختسا متي (ةكبشلا زهجا ني اهيلع ضوافتلا متي ةسلج

قداصملا TLS قفن

مت يتلا مداخلا ةداهش ىلى اذانتسا TLS قفن عاشن مت . ةيصوتلا وانام رثكالا رايلخا وه اذه ، طقف مداخلا بناج ىلع ةيساسالا PKI ةينب بلطتي اذهو . بلاطلا ةطساوب اهنم ققحتلا "مداخلا ةي وه نم ققحتلا" رايلخا لي طعت نكمملا نم ، NAM (ىلع) ISE ل ةبولطم نوكت يتلا و

ناي فاضا نارايخ كانه ، ISE ىلى ةبسنلاب

- Allow Anonymous In-Band PAC Provisioning
- Allow Authenticated In-Band PAC Provisioning
 - Server Returns Access Accept After Authenticated Provisioning
 - Accept Client Certificate For Provisioning

لومملا ىلع ضرقي امم لوصول اضفر لاسرا بجي ، ي محملا لوصول غوسم ريفوت دعب ، ةداع ميلست مت دق هنا ارظن نكلو . (PAC) ي محملا لوصول تاغوسم مادختساب ةقداصملا ةداع اهل مكاب ةي لمعل راصتخا نكمملا نم ، ةقداصملا عم TLS قفن ي ف ي محملا لوصول تاغوسم

يتم حلل لوصول غوسم ريفوت دعب اروف لوصول لوبق عاجراو.

طاقن ىلع PKI رشن اذه بلطتي) ليمعلا عدهاش ىلع TLS قفن ينال رايلخا دم تعي
ةيلخادلا ةقيرطال زواجتت يتلاو، ةلدابت مةقداصمب TLS قفن عاشناب حمسي اذهو. (ةياهنلا
في - انه نيرنخ نوكن نأ مهمل نم. يمحمل لوصول غوسم دادع اقلحرم ىل اقرشابم بهذتو
ىرخا ضارغأل ةصصخم) ISE لبق نم اهب قوثوم ريغ عدهاش بلطال مدقم مدقي، نايلخا لضعب
ةسلجال لشفتسو.

EAP-Chaing

بيلاسأ طبر نكمي. ةدحاو RADIUS/EAP لمع ةسلج لالخ زاهجالو مدختسملا ةقداصمب حامسلا
مداخل لسري، حاجنب (زاهجل صاخ لكشب) لوالا ةقداصملا اءاتنا دعب. اع مةددعتم ال EAP
بلطاب ابو حصم TLV نوكني نأ بجي. حاجنلا ىل اريشي (TLS قفن لخاد) ةجيتنلا طسوتم TLV
في ريظنلاو مداخل نم لك ةكراشم تابثال ريفشنتلا مادختسا متي. ريفشنتلل مزلم TLV
و 1 نيئلحرملا نم نيضمضتلا داوم ريفشنتلا ةيلمع مدختست. ةقداصملا ددحملا لسلسلا
ةديج لمع ةسلج ادبب اذه موقبي - EAP-Payload: رخأ TLV قافرا متي، كلذ ىل افاضالابو. 2.
رفشملا طبرلل TLV ةباجتسا I (ISE) RADIUS مداخل لبق تسي نأ درجمب. (مدختسملا ةداع)
ةداع) ةيلال EAP ةقيرط ةبجتم تيسو لسلا في فيلي ام رهظيس، اهتحص نم ققحتي و
(مدختسملا ةقداصملا):

12126 EAP-FAST cryptobinding verification passed

يدخل لشف ةلاح في. لمالكاب EAP ةسلج لشفت، ريفشنتلا طبر ةحص نم ققحتلا لشف اذ
لوؤسملل ISE حمسي، كلذل ةجيتنو - اديج رمأل لازي ال ةيلخادلا ةقداصملا تاي لمع
ليوختلا ةلاح ىل اءانتسا ةددعتم لسالس جئاتن نيوكتب
NetworkAccess:EapChainingResult:

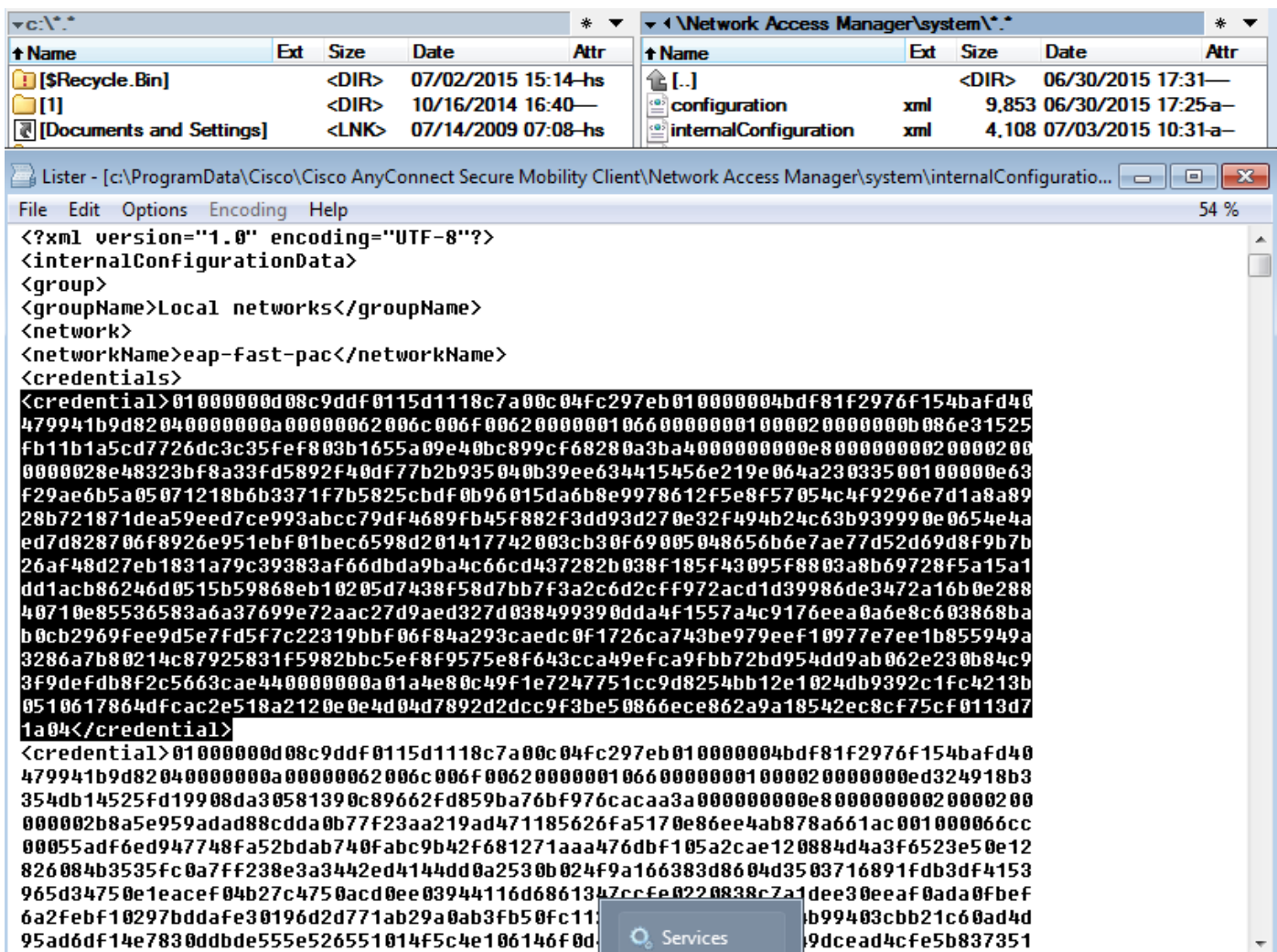
- No chaining
- User and machine both succeeded
- User failed and machine succeeded
- User succeeded and machine failed

EAP-FAST زاهجو مدختسم ةقداصم نيكمت دنع ايئاقلت NAM ىلع EAP-Chaing نيكمت متي

ISE في EAP ةلسلس نيوكتب بجي.

PAC تافل م نيخت متي ثيخ

في زاهجالو قفنلل (PAC) لوصول في مكحتلا مئاقق نيخت متي، يضارتفا لكشب
C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access
Manager\system\internalConfiguration.xml في <credential> ماسقأل في
رفشم.

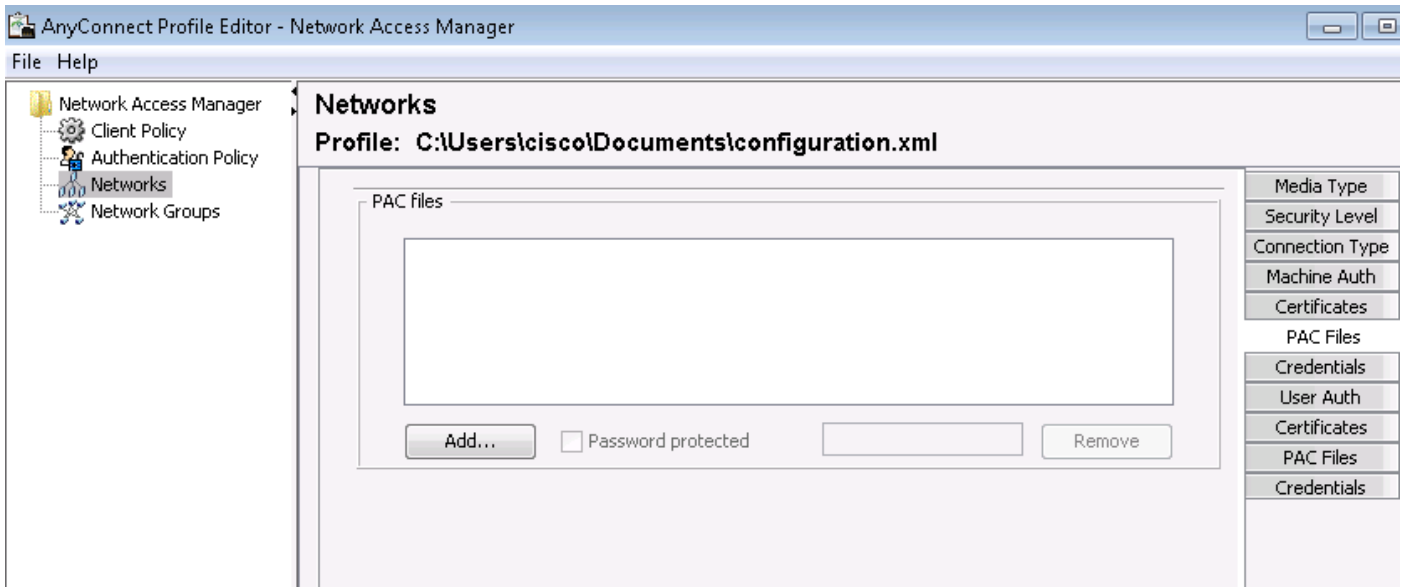


اهتلازا متتو طقف ٲرك اذلا ي ٲضي و ٲتلاب ءصاخلا لوصولا ي ٲم كحتلا مئاو ق ني زخت مت ي NAM ءم د خ لي غشت ءداع ا و ا لي غشتلا ءداع ا د ع ب

زاه ج ل ل PAC و ا Tunnel ءلا زال ءم د خ ل ل لي غشت ءداع ا د ع ب ي

AnyConnect NAM 3.1 ل ب ا ق م 4.0

ي م ح م ل ل لوصولا تا غ و س م ني و ك ت ب لو و س م ل ل NAM 3.x AnyConnect في ر ع ت ف ل م ر ر ح م ح م س ي NAM 4.x AnyConnect في ر ع ت ف ل م ر ر ح م ن م ء ز ي م ل ل ه ذ ه ءلا ز ا ت م ت . ا ي و د ي (PACs)

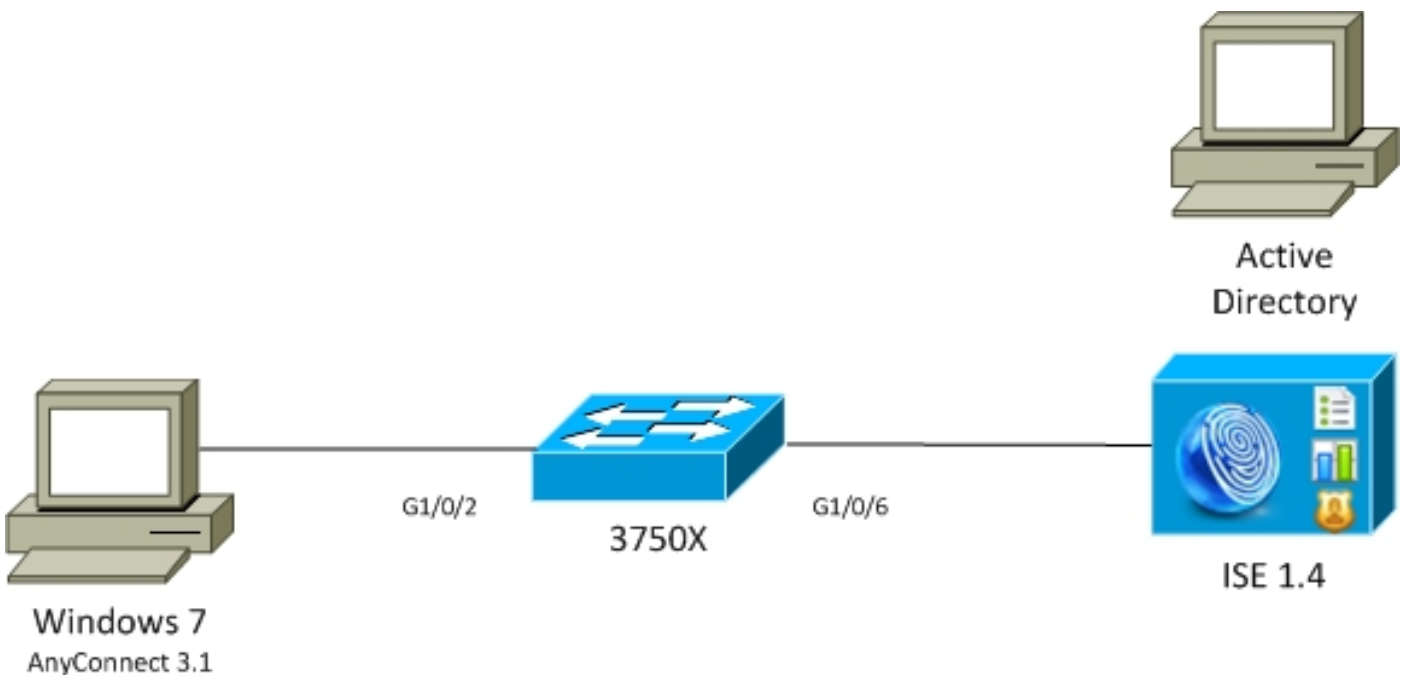


في ظل هذه الظروف، راجع [CSCua13140](#) و [CSCuf31422](#) على [CSC](#).

العثور على

العثور على طيخات المسرلة

اضغط على أيقونة الشبكة في قائمة الإعدادات. في قائمة الإعدادات، اضغط على أيقونة الشبكة. في قائمة الإعدادات، اضغط على أيقونة الشبكة.



العثور على مداخل الترسيل لوصول غوسم عم لصاوت الاب EAP-FAST نودب

تتطلب إعدادات الترسيل لوصول غوسم عم لصاوت الاب EAP-FAST نودب. في إعدادات الترسيل لوصول غوسم عم لصاوت الاب EAP-FAST نودب، يجب إعداد الترسيل لوصول غوسم عم لصاوت الاب EAP-FAST نودب. في إعدادات الترسيل لوصول غوسم عم لصاوت الاب EAP-FAST نودب، يجب إعداد الترسيل لوصول غوسم عم لصاوت الاب EAP-FAST نودب.

- زاهج ل PAC عم TLS Client Hello لاسراب لمكم لما موقوي.
- تاداهش دجوت ال TLS ق فن ينبيو زاهج ل لمحم ل لوصولا غوسم ةحص نم مداخل ققحتي (ةمدختسم).
- نع ثحب ل اارج او زاهج ل PAC ي محم ل لوصولا غوسم ةحص نم ققحت ل مداخل موقوي ي لخال ا بولس ال ا يطختو Active Directory ف باسح ل.

12102 Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as negotiated

12800 Extracted first TLS record; TLS handshake started

12174 Received Machine PAC

12805 Extracted TLS ClientHello message

12806 Prepared TLS ServerHello message

12801 Prepared TLS ChangeCipherSpec message

12816 TLS handshake succeeded

12132 EAP-FAST built PAC-based tunnel for purpose of authentication

24351 Account validation succeeded

24420 User's Attributes retrieval from Active Directory succeeded - example.com

22037 Authentication Passed

12124 EAP-FAST inner method skipped

11503 Prepared EAP-Success

11002 Returned RADIUS Access-Accept

(م دختسم) ةي نال ا ق داصم ل:

- ق فن ل PAC عم Hello نوبز TLS سم تلم لسري.
- تاداهش دجوت ال TLS ق فن ينبيو ي محم ل لوصولا غوسم ةحص نم مداخل ققحتي (ةمدختسم).
- ي لخال ا بولس ال ا ف ، ل ي وخت ل ل PAC ي محم ل لوصولا غوسم ل ع ي وحتي ال قح ل م ل ن ا م ب ة ق داصم ل ل م دختسي (EAP-MSCHAP).

12102 Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as negotiated

12800 Extracted first TLS record; TLS handshake started

12175 Received Tunnel PAC

12805 Extracted TLS ClientHello message

12806 Prepared TLS ServerHello message

12801 Prepared TLS ChangeCipherSpec message

12816 TLS handshake succeeded

12132 EAP-FAST built PAC-based tunnel for purpose of authentication

12125 EAP-FAST inner method started

11806 Prepared EAP-Request for inner method proposing **EAP-MSCHAP** with challenge

24402 User authentication against Active Directory succeeded - example.com

22037 Authentication Passed

11503 Prepared EAP-Success

11002 Returned RADIUS Access-Accept

نم ل كل ةبس ن ل ا ب ل ي ا م طح ال ي ، ISE ي ل ص ف م ل ر ي رقت ل نم "رأ تامس" مس ق ي ف ةي ل ل ال ا ق داصم ل او م دختسم ل ا ق داصم

EapChainingResult: No chaining

PAC ل ي صوت ةداع ا ب ع ي رس ل ال EAP ل ي صوت عم EAP-FAST

عم ءحل اص ق فن (PAC) يمحم لوصو تاغوسم لعفلاب بللاطم لل نوكي ، قفدتلا اذه يف ءة لآل او مدختسم لاضيفو فتب ءصاخلا (PAC) يمحم ل لوصولا تاغوسم

- ق فن ل PAC عم Hello نوبز TLS سم تلم لسري
- تاداهش دجوت ال) TLS ق فن ينبيو يمحم ل لوصولا غوسم ءحص نم مءاخلا ق قحتي (ءمءختسم
- ءة لآل او مدختسم ل لاضيفو فتل PACs سم تلم طبري و ، EAP ليصوت ليغش تب ISE موقوي TLS ق فن لءاد TLV مءختساب
- نم ق قحتي و ، (ءبولطم ءة لءاد ءقيرط دجوت ال) ليوختل تاغوسم ءحص نم ISE ق قحتي .ءءنل اءرا ل ل ءوئي و ، (ءيفاضل ءقءاصم دجوت ال) Active Directory يف تاباسءل دجو

```
12102 Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as negotiated
12800 Extracted first TLS record; TLS handshake started
12175 Received Tunnel PAC
12805 Extracted TLS ClientHello message
12806 Prepared TLS ServerHello message
12801 Prepared TLS ChangeCipherSpec message

12816 TLS handshake succeeded
12132 EAP-FAST built PAC-based tunnel for purpose of authentication
12209 Starting EAP chaining
12210 Received User Authorization PAC
12211 Received Machine Authorization PAC

24420 User's Attributes retrieval from Active Directory succeeded - example.com
22037 Authentication Passed

24439 Machine Attributes retrieval from Active Directory succeeded - example.com
22037 Authentication Passed

11503 Prepared EAP-Success
11002 Returned RADIUS Access-Accept
```

ظءالي ، تاءاصء ل ل لودلا ده عم ل ريرقت يف لصفم ل ريرقتل نم "لرءء تامس" مسق يف و ل ل ام

EapChainingResult: **EAP Chaining**

وه امك لءس ل س فن يف ءة لآل او مدختسم ل تاغوسم نم لك نيمضت متي ، لكذ ل ءة فاضل اب هانءا ءضوم

Username: cisco,host/mgarcarz-PC

EAP-FAST عم ءل صو ء PAC نوبء

ISE نيموكت مت امك ، PAC يمحم لوصو غوسم مءءءسا مدءل NAM نيموكت مت ، قفدتلا اذه يف ءل صو ء عم نكل) يمحم ل لوصولا غوسم مءءءسا مدءل

- ق فن ل PAC نوبء TLS Client Hello لاسراب لمءم ل موقوي
- ءءاهش ل بلطو TLS ءءاهش ءلومء عم مءاخلا بءءتسي
- (رفص ءءاهش ل ءلومء) ليمء ءءاهش ل لسري نلو ، مءءءل ءءاهش ب لاطلا قءل نأ بءل ، TLS ق فن ءاشن مءل و
- نم س ل ل) سم تلم دجوي ال نكل و ، TLS ق فن لءاد ليمءل ءءاهش ل TLV بلط ISE لسرا (ءءءاتم ل لءا نم هل نوكي نأ رورءل)

- MSCHAPv2 ةقداصم ب ي لخدال بولسأل مادختساب ،مدختسم لل EAP لي صوت أدبي
- MSCHAPv2 ةقداصم عم ي لخدال بولسأل مادختساب ،زاهال ةقداصم ي ف رمتسي
- (PAC) ذفنم لبا ةصاخال لوصول ي ف مكحتال مئوق ريفوت متي ال

```

12102      Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST
as negotiated
12800      Extracted first TLS record; TLS handshake started
12805      Extracted TLS ClientHello message
12806      Prepared TLS ServerHello message
12807      Prepared TLS Certificate message
12809      Prepared TLS CertificateRequest message
12811      Extracted TLS Certificate message containing client certificate
12812      Extracted TLS ClientKeyExchange message

12816      TLS handshake succeeded
12207      Client certificate was requested but not received during tunnel establishment. Will
renegotiate and request client certificate inside the tunnel.
12226      Started renegotiated TLS handshake

12104      Extracted EAP-Response containing EAP-FAST challenge-response
12811      Extracted TLS Certificate message containing client certificate
12812      Extracted TLS ClientKeyExchange message
12804      Extracted TLS Finished message
12801      Prepared TLS ChangeCipherSpec message
12802      Prepared TLS Finished message
12226      Started renegotiated TLS handshake
12205      Client certificate was requested but not received inside the tunnel. Will continue
with inner method.
12176      EAP-FAST PAC-less full handshake finished successfully

12209      Starting EAP chaining
12218      Selected identity type 'User'

11806      Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge

24402      User authentication against Active Directory succeeded - example.com
22037      Authentication Passed

12219      Selected identity type 'Machine'

11806      Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge

24470      Machine authentication against Active Directory is successful - example.com
22037      Authentication Passed

11503      Prepared EAP-Success
11002      Returned RADIUS Access-Accept

```

EAP لس لس لتال ضي وف تل PAC ةي حالص اهاتنا عم EAP-FAST

نكلول لي وختلل ةحالص (PAC) ي محم لوصول و تاغوسم لعل لوممالي وحتي ،ق فدتال اذه ي ف اهات ي حالص تهاتنا:

- ق فنال PAC عم Hello نوبز TLS سم تلم لسري
- تاداهش دجوت ال) TLS ق فن ي نبي و ي محمالي لوصول و غوسم ةحص نم مدخال ق قحتي (ةمدختسم
- ةلأل او مدختسم لل ضي وف تل PACs سم تلم طبري و ،EAP لي صوت لي غشتب ISE موق ي TLS ق فن لخد TLV مادختساب
- مدختسم ل نم لكل ي لخدال بولسأل أدبي ،ي محمالي لوصول و تاغوسم ةي حالص اهاتنا عم

12809 Prepared TLS CertificateRequest message
 12105 Prepared EAP-Request with another EAP-FAST challenge
 11006 Returned RADIUS Access-Challenge
 11001 Received RADIUS Access-Request

12816 TLS handshake succeeded
 12207 **Client certificate was requested but not received during tunnel establishment. Will renegotiate and request client certificate inside the tunnel.**
 12226 Started renegotiated TLS handshake

 12104 Extracted EAP-Response containing EAP-FAST challenge-response
12811 Extracted TLS Certificate message containing client certificate
 12812 Extracted TLS ClientKeyExchange message
 12804 Extracted TLS Finished message
 12801 Prepared TLS ChangeCipherSpec message
 12802 Prepared TLS Finished message
 12226 Started renegotiated TLS handshake
12205 Client certificate was requested but not received inside the tunnel. Will continue with inner method.
12149 EAP-FAST built authenticated tunnel for purpose of PAC provisioning
 12105 Prepared EAP-Request with another EAP-FAST challenge
 11006 Returned RADIUS Access-Challenge
 11001 Received RADIUS Access-Request
 11018 RADIUS is re-using an existing session
 12104 Extracted EAP-Response containing EAP-FAST challenge-response
12209 Starting EAP chaining
12218 Selected identity type 'User'
11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge

24402 User authentication against Active Directory succeeded - example.com
22037 Authentication Passed

12126 EAP-FAST cryptobinding verification passed
 12200 Approved EAP-FAST client Tunnel PAC request
 12202 Approved EAP-FAST client Authorization PAC request
12219 Selected identity type 'Machine'

11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge

24470 Machine authentication against Active Directory is successful - example.com
22037 Authentication Passed

12169 Successfully finished EAP-FAST tunnel PAC provisioning/update
12171 Successfully finished EAP-FAST user authorization PAC provisioning/update
12170 Successfully finished EAP-FAST machine PAC provisioning/update
12179 Successfully finished EAP-FAST machine authorization PAC provisioning/update

 11503 Prepared EAP-Success
 11002 Returned RADIUS Access-Accept

EAP-FAST ق فن TLS PAC ري فوتو EAP لس لس لت عم

لي طعت مت) PAC ري فوتو ل NAM Anonymous TLS و ISE ق فن ني وكت مت ، ق فدت لا اذه في ق فن PAC: ديوزت بلط ودبي (PAC ري فوتو ل TLS ق دصم ال ISE ق فن

- تارفش م ال نم دي دعال نودب TLS Client Hello ل اس راب لم كم ال موقوي.
- TLS Anonymous Diffie Hellman و TLS Hello ةرفش مادخت ساب مداخل البيجت سي (لج) TLS_DH_Anon_WITH_AES_128_CBC_SHA ل ث م ال لبس
- (تاداهش ل لدابت متي ال) لوهج م ال TLS ق فن انب متي و كلذ بلط ال ل بقوي.

- MSCHAPv2 ةقداصم ب ي لخدال بولسأل مادختساب ،مدختسملل EAP لي صوت أدبي
- MSCHAPv2 ةقداصم عم ي لخدال بولسأل مادختساب ،زاهال ةقداصم ي ف رمتسي
- لي وختلل PAC تادحوب حومسم ريغ لوهجم ق فن TLS ءانب متي هنأل ارطن
- لوصو غوسم مادختساب) ةقداصم لاداع لىل لمكلم رابحال RADIUS ضفر عاچرا متي (دوزم يمحم

12102 Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as negotiated

12800 Extracted first TLS record; TLS handshake started

12805 Extracted TLS ClientHello message

12806 Prepared TLS ServerHello message

12808 Prepared TLS ServerKeyExchange message

12810 Prepared TLS ServerDone message

12812 Extracted TLS ClientKeyExchange message

12804 Extracted TLS Finished message

12801 Prepared TLS ChangeCipherSpec message

12802 Prepared TLS Finished message

12816 TLS handshake succeeded

12131 EAP-FAST built anonymous tunnel for purpose of PAC provisioning

12209 Starting EAP chaining

12218 Selected identity type 'User'

11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge

24402 User authentication against Active Directory succeeded - example.com

22037 Authentication Passed

12162 Cannot provision Authorization PAC on anonymous provisioning. Authorization PAC can be provisioned only on authenticated provisioning

12200 Approved EAP-FAST client Tunnel PAC request

12219 Selected identity type 'Machine'

24470 Machine authentication against Active Directory is successful - example.com

22037 Authentication Passed

12162 Cannot provision Authorization PAC on anonymous provisioning. Authorization PAC can be provisioned only on authenticated provisioning

12169 Successfully finished EAP-FAST tunnel PAC provisioning/update

12170 Successfully finished EAP-FAST machine PAC provisioning/update

11504 Prepared EAP-Failure

11003 Returned RADIUS Access-Reject

ةلوهجم TLS ق فن تاضوافمل Wireshark ةمزح طاقتلا:

Source	Destination	Protocol	Length	Info	User-Name
10.62.148.109	10.48.17.14	RADIUS	301	Access-Request(1) (id=190,	anonymous
10.48.17.14	10.62.148.109	RADIUS	193	Access-Challenge(11) (id=19	
10.62.148.109	10.48.17.14	RADIUS	498	Access-Request(1) (id=191,	anonymous
10.48.17.14	10.62.148.109	RADIUS	793	Access-Challenge(11) (id=19	
10.62.148.109	10.48.17.14	RADIUS	706	Access-Request(1) (id=192,	anonymous
10.48.17.14	10.62.148.109	RADIUS	232	Access-Challenge(11) (id=19	
10.62.148.109	10.48.17.14	RADIUS	378	Access-Request(1) (id=193,	anonymous
10.48.17.14	10.62.148.109	RADIUS	226	Access-Challenge(11) (id=19	
10.62.148.109	10.48.17.14	RADIUS	468	Access-Request(1) (id=194,	anonymous
10.48.17.14	10.62.148.109	RADIUS	258	Access-Challenge(11) (id=19	

Code: Request (1)

Id: 161

Length: 622

Type: Flexible Authentication via Secure Tunneling EAP (EAP-FAST) (43)

▷ EAP-TLS Flags: 0x01

▽ Secure Sockets Layer

▽ TLSv1 Record Layer: Handshake Protocol: Server Hello

Content Type: Handshake (22)

Version: TLS 1.0 (0x0301)

Length: 74

▽ Handshake Protocol: Server Hello

Handshake Type: Server Hello (2)

Length: 70

Version: TLS 1.0 (0x0301)

▷ Random

Session ID Length: 32

Session ID: 41aee5db065f48165c56144aa9dccdc93f67167fbae96393...

Cipher Suite: TLS_DH_anon_WITH_AES_128_CBC_SHA (0x0034)

Compression Method: null (0)

▽ TLSv1 Record Layer: Handshake Protocol: Server Key Exchange

Content Type: Handshake (22)

طوق مَدْخْتَسَمِلا ةَقْدَاصَم لَصَوِي EAP FAST مَع EAP-TLS

ةَقْدَاصَم مَو (EAP-TLS) مَدْخْتَسَمِلا ةَقْدَاصَم لَصَوِي EAP FAST مَع AnyConnect NAM نِي وَكْت مَت ، قَفْدَتِلا اذَه يَفِ دَامَتَعَا تَانَايِب رِي فَوْت مَتِي مَل نَك لَو Windows رَتَوِي بَمَك دِي هَمَت مَت . (EAP-TLS) زَاهَجَلَا بِي جَتَسَت نَأ بَجِي ، كَلْذ نَم مَغْرَلَا يَلَعَو 802.1x لَمَع ةَسَلَج ةَيَّهَتَب لَو حَمَلَا مَو قِي . مَدْخْتَسَمِلا مَدْخْتَسَمِلا نَزْحَم يَلَا لَو وُصَو دَجَوِي (ال) ، مَدْخْتَسَمِلا دَامَتَعَا تَانَايِب رِي فَوْت مَتِي مَلَو ، NAM ISE authz طَرَش - زَاهَجَلَا حَجْنِي سَامَنِي ب مَدْخْتَسَمِلا ةَقْدَاصَم لَشَفَتَس . كَلْذَل (دَعَب ةَدَاهَشَلَا ةَقْدَاصَم لَخَدِي س ، اِقْحَال . زَاهَجَلَا حَجْنَو لَشَف EapChaingResult equals User : ةَكْبَشَلَا لَو وُصَو ةَلْأَلَا ةَقْدَاصَم لَخَدِي سَامَنِي نَم لَك حَجْنِي سَو ، يَرْخَأ ةَقْدَاصَم اَدْبَتَسَو

- زَاهَجَلَلَا PAC مَع TLS Client Hello لَاسَرَاب لَمَكَمَلَا مَو قِي .
- يَلَع TLS قَفْنِ ءَاَشْنِ مَتِي - TLS رِي غَت رِي فَشَت تَا فَاوَم مَادَخْتَسَاب مَادَخَلَا بِي جَتَسِي . اذَه PAC يَلَا اِدَانَتَسَا رَوَفَلَا .
- مَدْخْتَسَمِلا ةَيَّهَو بَلَطَو EAP لَسَلَسَت ةَيَّهَتَب ISE مَو قِي .
- بَوَلَسْأَلَا نَم يَهَتَنِي وَ ، (دَعَب زَاهَج رِي غ مَدْخْتَسَمِلا) كَلْذ نَم اَلدَب زَاهَجَلَا ةَيَّهَو بَلَطَمَلَا رَفَوِي .

EAP-TLS يخلخال

- اهرفوت بلالاملل نكمي الو، رخأ ةرم مدختسمل ةوه ISE بلطي.
 - (مدختسمل ةقداصل) لشف = ةطيسو ةجيتن عم ISE TLV لسري.
 - ل لوصول طارش ISE، ةئاهنل EAP حاجن ةلسرر عرت ISE ةلال.
- ضارحجان رتوي بمكل لاولش اف مدختسم = EapChaingResult: ةكبش ل

```
12102  Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as negotiated
12800  Extracted first TLS record; TLS handshake started
12174  Received Machine PAC

12805  Extracted TLS ClientHello message
12806  Prepared TLS ServerHello message
12801  Prepared TLS ChangeCipherSpec message
12802  Prepared TLS Finished message

12816  TLS handshake succeeded
12132  EAP-FAST built PAC-based tunnel for purpose of authentication

12209  Starting EAP chaining
12218  Selected identity type 'User'

12213  Identity type provided by client is not equal to requested type
12215  Client suggested 'Machine' identity type instead

12104  Extracted EAP-Response containing EAP-FAST challenge-response
12523  Extracted EAP-Response/NAK for inner method requesting to use EAP-TLS instead

12805  Extracted TLS ClientHello message
12806  Prepared TLS ServerHello message
12807  Prepared TLS Certificate message
12809  Prepared TLS CertificateRequest message

12816  TLS handshake succeeded
12509  EAP-TLS full handshake finished successfully

22070  Identity name is taken from certificate attribute
15013  Selected Identity Source - Test-AD
24323  Identity resolution detected single matching account
22037  Authentication Passed

12202  Approved EAP-FAST client Authorization PAC request
12218  Selected identity type 'User'
12213  Identity type provided by client is not equal to requested type
12216  Identity type provided by client was already used for authentication
12967  Sent EAP Intermediate Result TLV indicating failure

12179  Successfully finished EAP-FAST machine authorization PAC provisioning/update
12106  EAP-FAST authentication phase finished successfully
11503  Prepared EAP-Success
11002  Returned RADIUS Access-Accept
```

ةنمازتمل ريغ TLS قفن تاداعو EAP لسالس عم EAP-FAST

TLS قفن ربع طقف (PAC) يمحمل لوصول و غوسم ريفوتل ISE نيوكت مت، قفدتل اذه يف ISE ةطساوب يلي ام ليحست متيسو، هيلع قدصم TLS قفن مدختست NAM نكلو، لوهجمل

```
12102  Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as negotiated
```

```
12800 Extracted first TLS record; TLS handshake started
12805 Extracted TLS ClientHello message
12814 Prepared TLS Alert message
12817 TLS handshake failed
12121 Client didn't provide suitable ciphers for anonymous PAC-provisioning
```

```
11504 Prepared EAP-Failure
11003 Returned RADIUS Access-Reject
```

الو- ابة صاخلا TLS ةرفش مادختساب قوصم TLS قفن ءاشنإ NAM لواحت امدنع ثدح اذهو DH تارفش لوبق) لوهجم TLS قفنل اهنوك مت يتل ISE لبق نم تارفشلا هذه لبق (طوق)

اهحال صإو ءاطخال فاشكتسا

ةيوهلا فشك تامدخ كرحم (ISE)

ىلع AAA ليغشلتا تقو ءاطخال حيصت نيكمت بجي، ةيليصفتلا تالجس لل ةبسنلاب prrt-server.log نم ةلثمألا تالجس ضعب يلي اميف. ةلباقم ال PSN ةدقع

زاهلل (PAC) يمحمل لوصول تاغوسم ءاشنإ:

```
DEBUG, 0x7fd5332fe700, cntx=0001162745, sesn=mgarcarz-
ise14/223983918/29245, CPMSessionID=0A3E946D0000FE5131F9D26, CallingStationID=00-50-B6-11-ED-
31, FramedIPAddress=10.0.13.127, Using IID from PAC request for machine, EapFastTlv.cpp:1234

DEBUG, 0x7fd5332fe700, cntx=0001162745, sesn=mgarcarz-
ise14/223983918/29245, CPMSessionID=0A3E946D0000FE5131F9D26, CallingStationID=00-50-B6-11-ED-
31, FramedIPAddress=10.0.13.127, Adding PAC of type=Machine Authorization, EapFastProtocol.cpp:3610

DEBUG, 0x7fd5332fe700, cntx=0001162745, sesn=mgarcarz-
ise14/223983918/29245, CPMSessionID=0A3E946D0000FE5131F9D26, CallingStationID=00-50-B6-11-ED-
31, FramedIPAddress=10.0.13.127, Eap-Fast: Generating Pac, Issued PAC type=Machine Authorization
with expiration time: Fri Jul 3 10:38:30 2015
```

يمحمل لوصول تاغوسم بلط ىلع ةقفاوملا:

```
INFO , 0x7fd5330fc700, cntx=0001162745, sesn=mgarcarz-
ise14/223983918/29245, CPMSessionID=0A3E946D0000FE5131F9D26, user=host/mgarcarz-
pc, CallingStationID=00-50-B6-11-ED-31, FramedIPAddress=10.0.13.127, Eap-Fast: client PAC request
approved for PAC type - Requested PAC type=Machine, EapFastProtocol.cpp:955

INFO , 0x7fd5330fc700, cntx=0001162745, sesn=mgarcarz-
ise14/223983918/29245, CPMSessionID=0A3E946D0000FE5131F9D26, user=host/mgarcarz-
pc, CallingStationID=00-50-B6-11-ED-31, FramedIPAddress=10.0.13.127, Eap-Fast: client PAC request
approved for PAC type - Requested PAC type=Machine Authorization, EapFastProtocol.cpp:955
```

يمحمل لوصول غوسم ةحص نم ققحتلا:

```
DEBUG, 0x7fd5330fc700, cntx=0001162499, sesn=mgarcarz-
ise14/223983918/29243, CPMSessionID=0A3E946D0000FE5131F9D26, user=anonymous, CallingStationID=00-
50-B6-11-ED-31, FramedIPAddress=10.0.13.127, Authorization PAC is valid, EapFastProtocol.cpp:3403

Eap, 2015-07-03 09:34:39, 208, DEBUG, 0x7fd5330fc700, cntx=0001162499, sesn=mgarcarz-
ise14/223983918/29243, CPMSessionID=0A3E946D0000FE5131F9D26, user=anonymous, CallingStationID=00-
```

50-B6-11-ED-31, FramedIPAddress=10.0.13.127, Authorization PAC accepted, EapFastProtocol.cpp:3430

(PAC): يمحمل لوصول تاغوسم عاشنال حج انال صخلم لىل لاثم

```
DEBUG, 0x7fd5331fd700, cntx=0001162749, sesn=mgarcarz-ise14/223983918/29245, CPMSessionID=0A3E946D00000FE5131F9D26, user=cisco, CallingStationID=00-50-B6-11-ED-31, FramedIPAddress=10.0.13.127, Conversation summary: Provisioning. Authenticated. Inner method succeeded. Inner method succeeded. Generated PAC of type Tunnel V1A. Generated PAC of type User Authorization. Generated PAC of type Machine. Generated PAC of type Machine Authorization. Success
```

يمحمل لوصول تاغوسم ةحص نم ققحتلل حج ان صخلم لىل لاثم:

```
DEBUG, 0x7fd5330fc700, cntx=0001162503, sesn=mgarcarz-ise14/223983918/29243, CPMSessionID=0A3E946D00000FE5131F9D26, user=host/mgarcarz-pc, CallingStationID=00-50-B6-11-ED-31, FramedIPAddress=10.0.13.127, Conversation summary: Authentication. PAC type Tunnel V1A. PAC is valid. Skip inner method. Skip inner method. Success
```

AnyConnect NAM

ةيلات لىل صافاتال NAM نم DART تالاجس رفوت:

عيرس لىل صوت ةداع| نودب زاهجال ةقداصم، EAP طبرمدع لمع ةسلجل لاثم

```
EAP: Identity requested
Auth[eap-fast-pac:machine-auth]: Performing full authentication
Auth[eap-fast-pac:machine-auth]: Disabling fast reauthentication
```

(EAP-Network) ريغ لمع ةسلجل زاهجال ةقداصم) لىل وختلل PAC ثحب لىل لاثم

```
Looking for matching pac with iid: host/ADMIN-PC2
Requested machine pac was sen
```

هاندا تالاجسالا نم (MSCHAP) لىل خادال بولسأال تالاج عيجم نم ققحتال نكمي:

```
EAP (0) EAP-MSCHAP-V2: State: 0 (eap_auth_mschapv2_c.c 731)
EAP (0) EAP-MSCHAP-V2: State: 2 (eap_auth_mschapv2_c.c 731)
EAP (0) EAP-MSCHAP-V2: State: 1 (eap_auth_mschapv2_c.c 731)
EAP (0) EAP-MSCHAP-V2: State: 4 (eap_auth_mschapv2_c.c 73)
```

اهظا فحتو EAP مزح عيجم لىل ضربقتس يتلل عسومال لىل جس تال ةزيم نيوكتت NAM حمست ىت ح EAP مزح طاق تال متي) Start Before Login ةفي طول اصوصخ دي فم اذهو. PCAP فلم يفسدنهم لاسا، تازيمل طيش ننتل. (مدختس مال لوخد لىل جس تال بق ثدحت يتلل ةقداصم لل TAC.

عجارملا

- [Cisco AnyConnect Secure Mobility Client. رادصلال نيوكت. EAP-FAST 4.0 رادصلال نيوكت](#)
- [Cisco، نم ةيوهال تامدخ كرحم لوؤسم لىل](#)
- [Cisco نم ةيوهال تامدخ كرحم ميمصت ةلدا](#)
- [Cisco ISE و AnyConnect NAM عم EAP لىل صوت رشن](#)
- [Cisco Systems - تادنتس مال او يبق تال معدلا](#)

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 إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةل صأل ةل ءل ءن إل دن تسمل