تصحيح أخطاء ASA IKEv2 للاستكشاف أخطاء الوصول عن بعد والحالات الخاصة VPN

المحتويات

المقدمة

يصف هذا المستند كيفية فهم تصحيح الأخطاء على جهاز الأمان القابل للتكيف (ASA) من Cisco عند إستخدام Internet Key Exchange الإصدار 2 (IKEv2) مع Cisco AnyConnect Secure Mobility Client. كما يوفر هذا المستند معلومات حول كيفية ترجمة بعض سطور تصحيح الأخطاء في تكوين ASA.

لا يصف هذا المستند كيفية تمرير حركة المرور بعد إنشاء نفق VPN إلى ASA، ولا يتضمن المفاهيم الأساسية ل IPSec أو IKE.

المتطلبات الأساسية

المتطلبات

cisco يوصي أن يتلقى أنت معرفة من الربط تبادل ل IKEv2. لمزيد من المعلومات، ارجع إلى تصحيح أخطاء مستوى البروتوكول و تبادل حزم IKEv2.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- تبادل مفتاح الإنترنت الإصدار 2 (IKEv2)
- Cisco Adaptive Security Appliance (ASA)، الإصدار 8.4 أو إصدار أحدث

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

مسألة أساسية

غالبا ما يستخدم مركز المساعدة التقنية (TAC) من Cisco أوامر تصحيح أخطاء IKE و IPSec لفهم مكان وجود مشكلة في إنشاء نفق IPSec VPN، ولكن يمكن أن تكون الأوامر مشفرة.

سيناريو

أوامر التصحيح

```
debug crypto ikev2 protocol 127
debug crypto ikev2 platform 127
     debug aggregate-auth xml 5
```

تكوين ASA

تكوين ASA هذا أساسي تماما، دون إستخدام للخوادم الخارجية.

```
                                interface Ethernet0/1
                                      nameif outside
                                   security-level 0
                             ip address 10.0.0.1 255.255.255.0

                           ip local pool webvpn1 10.2.2.1-10.2.2.10

                                  crypto ipsec ikev2 ipsec-proposal 3des
                               protocol esp encryption aes-256 aes 3des des
                                     protocol esp integrity sha-1
                        crypto dynamic-map dynmap 1000 set ikev2 ipsec-proposal 3des
                                crypto map crymap 10000 ipsec-isakmp dynamic dynmap
                                crypto map crymap interface outside

                                crypto ca trustpoint Anu-ikev2
                                        enrollment self
                                          crl configure

                                  crypto ikev2 policy 10
                                     encryption aes-192
                                          integrity sha
                                                group 2
                                                prf sha
                                lifetime seconds 86400
```

```
crypto ikev2 enable outside client-services port 443
crypto ikev2 remote-access trustpoint Anu-ikev2
ssl encryption 3des-sha1 aes128-sha1 aes256-sha1 des-sha1
ssl trust-point Anu-ikev2 outside

webvpn
enable outside
anyconnect image disk0:/anyconnect-win-3.0.1047-k9.pkg 1
anyconnect profiles Anyconnect-ikev2 disk0:/anyconnect-ikev2.xml
anyconnect enable
tunnel-group-list enable

group-policy ASA-IKEV2 internal
group-policy ASA-IKEV2 attributes
wins-server none
dns-server none
vpn-tunnel-protocol ikev2
default-domain none
webvpn
anyconnect modules value dart
anyconnect profiles value Anyconnect-ikev2 type user

username Anu password lAuoFgF7KmB3D0WI encrypted privilege 15

tunnel-group ASA-IKEV2 type remote-access
tunnel-group ASA-IKEV2 general-attributes
address-pool webvpn1
default-group-policy ASA-IKEV2
tunnel-group ASA-IKEV2 webvpn-attributes
group-alias ASA-IKEV2 enable
```

ملف XML

```
<ServerList>
<HostEntry>
<HostName>Anu-IKEV2</HostName>
<HostAddress>10.0.0.1</HostAddress>
<UserGroup>ASA-IKEV2</UserGroup>
<PrimaryProtocol>IPsec</PrimaryProtocol>
<HostEntry/>
<ServerList/>
```

ملاحظة: يجب أن يكون اسم UserGroup في ملف تعريف عميل XML هو نفس اسم مجموعة النفق على ASA. وإلا، فإن رسالة الخطأ 'إدخال مضيف غير صالح. يرجى مراجعة الأمر re-enter' على عميل AnyConnect.

سجلات تصحيح الأخطاء والأوصاف

ملاحظة: عادة ما تكون السجلات من أداة التشخيص وإعداد التقارير (DART) كثيرة الدردشة، لذلك تم حذف بعض سجلات DART في هذا المثال بسبب عدم أهميتها.

وصف رسالة الخادم **تصحيح الأخطاء**
التاريخ: 2013/04/23 م
الوقت: 16:24:55
النوع : المعلومات

المصدر: أكفبنوي

الوصف: الوظيفة: ClientIfcBase::الاتصال
الملف: .\ClientIfcBase.cpp
السطر: 964
طلب المستخدم اتصال شبكة VPN ب Anu-IKEV2.
****

التاريخ: 2013/04/23 م
الوقت: 16:24:55
النوع : المعلومات
المصدر: أكفبنوي

الوصف: تم إرسال معلومات نوع الرسالة إلى المستخدم:
الاتصال ببروتوكول Anu-IKEV2.
****

التاريخ: 2013/04/23 م
الوقت: 16:24:55
النوع : المعلومات
المصدر: أكفبنوي

الوصف: الوظيفة: ApiCert::GetCertList
الملف: .\ApiCert.cpp
السطر: 259
عدد الشهادات التي تم العثور عليها: 0
****

التاريخ: 2013/04/23 م
الوقت: 16:25:00
النوع : المعلومات
المصدر: أكفبنوي

الوصف: **بدء اتصال VPN بالبوابة الآمنة https://10.0.0.1/ASA-IKEV2**
****

التاريخ: 2013/04/23 م
الوقت: 16:25:00
النوع : المعلومات
المصدر:

الوصف: النفق الذي بدأه عميل واجهة المستخدم الرسومية.
****

التاريخ: 2013/04/23 م
الوقت: 16:25:02
النوع : المعلومات
المصدر:

الوصف: الوظيفة: CIPsecProtocol::connectTransport
الملف: .\IPsecProtocol.cpp
السطر: 1629
مقبس IKE المفتوح من 192.168.1.1:25170 إلى 10.0.0.1:500
****

—يبدأ تبادل IKE_SA_INIT—

يتلقى ASA رسالة IKE_SA_INIT من

IKEv2-PLAT-4: rev PKT [IKE_SA_INIT] [192.168.1.1]:25170->[10.0.1]:500
InitSPI=0x58aff71141ba436b

العميل.

أول زوج من الرسائل هو تبادل IKE_SA_INIT. تتفاوض هذه الرسائل على خوارزميات التشفير، واجهات التبادل، وتقوم بتبادل Diffie-Hellman (DH). تحتوي رسالة IKE_SA_INIT التي تم تلقيها من العميل على الحقول التالية:

1. **رأس** - ISAKMP SPI/الإصدار/العلامات.
2. **SAi1** - خوارزمية التشفير التي يدعمها بادئ IKE.
3. **KEi** - قيمة مفتاح DH العام للبادئ.
4. N - Initiator Nonce.

spSPI=0x000000000000mid=00000000mid=00000000000000000000000000000000
00000000000000000000
IKEv2-PROTO-3: Rx [L 10.0.0.1:500/R 192.168.1.1:25170/VRF i0:f0] m_id: 0x0
[IKEv2-proto-3: **HDR.**[i:58AFF71141BA436B - r: 000000000000
IKEv2-proto-4: IKEv2 HDR **ispi: 58AFF71141BA436B - RSPI: 000000000000**
IKEv2-PROTO-4: الحمولة التالية: SA، **الإصدار 2.0**
IKEv2-Proto-4: نوع التبادل: IKE_SA_INIT، **العلامات: البادئ**
IKEv2-PROTO-4: معرف الرسالة: 0x0، الطول: 528

حمولة **SA** التالية: KE، محجوزة: 0x0، الطول: 168
IKEv2-PROTO-4: المقترح الأخير: 0x0، محجوز: 0x0، الطول: 164
المقترح: 1، معرف البروتوكول: IKE، حجم SPI: 0، #trans: 18
IKEv2-PROTO-4: آخر تحويل: 0x3، محجوز: 0x0: الطول: 12
النوع: 1، محجوز: 0x0، المعرف: AES-CBC
IKEv2-PROTO-4: آخر تحويل: 0x3، محجوز: 0x0: الطول: 12
النوع: 1، محجوز: 0x0، المعرف: AES-CBC
IKEv2-PROTO-4: آخر تحويل: 0x3، محجوز: 0x0: الطول: 12
النوع: 1، محجوز: 0x0، المعرف: AES-CBC
IKEv2-PROTO-4: آخر تحويل: 0x3، محجوز: 0x0: الطول: 8
النوع: 1، محجوز: 0x0، المعرف: 3DES
IKEv2-PROTO-4: آخر تحويل: 0x3، محجوز: 0x0: الطول: 8
النوع: 1، محجوز: 0x0، المعرف: DES
IKEv2-PROTO-4: آخر تحويل: 0x3، محجوز: 0x0: الطول: 8
النوع: 2، محجوز: 0x0، المعرف: SHA512
IKEv2-PROTO-4: آخر تحويل: 0x3، محجوز: 0x0: الطول: 8
النوع: 2، محجوز: 0x0، المعرف: SHA384
IKEv2-PROTO-4: آخر تحويل: 0x3، محجوز: 0x0: الطول: 8
النوع: 2، محجوز: 0x0، المعرف: SHA256
IKEv2-PROTO-4: آخر تحويل: 0x3، محجوز: 0x0: الطول: 8
النوع: 2، محجوز: 0x0، المعرف: SHA1
IKEv2-PROTO-4: آخر تحويل: 0x3، محجوز: 0x0: الطول: 8
النوع: 2، محجوز: 0x0، المعرف: MD5
IKEv2-PROTO-4: آخر تحويل: 0x3، محجوز: 0x0: الطول: 8
النوع: 3، محجوز: 0x0، المعرف: SHA512
IKEv2-PROTO-4: آخر تحويل: 0x3، محجوز: 0x0: الطول: 8
النوع: 3، محجوز: 0x0، المعرف: SHA384
IKEv2-PROTO-4: آخر تحويل: 0x3، محجوز: 0x0: الطول: 8
النوع: 3، محجوز: 0x0، المعرف: SHA256
IKEv2-PROTO-4: آخر تحويل: 0x3، محجوز: 0x0: الطول: 8
النوع: 3، محجوز: 0x0، المعرف: SHA96
IKEv2-PROTO-4: آخر تحويل: 0x3، محجوز: 0x0: الطول: 8
النوع: 3، محجوز: 0x0، المعرف: MD596
IKEv2-PROTO-4: آخر تحويل: 0x3، محجوز: 0x0: الطول: 8
النوع: 4، محجوز: 0x0، المعرف: DH_GROUP_1536_MODP/Group 5
IKEv2-PROTO-4: آخر تحويل: 0x3، محجوز: 0x0: الطول: 8
النوع: 4، محجوز: 0x0، المعرف: DH_GROUP_1024_MODP/Group 2
IKEv2-PROTO-4: آخر تحويل: 0x0، محجوز: 0x0: الطول: 8
النوع: 4، محجوز: 0x0، المعرف: DH_GROUP_768_MODP/Group 1

الحمولة التالية **ل KE:N، محجوز: 0x0، الطول: 104**
مجموعة DH: 1، محجوز: 0x0

b 5e 29 fe cb 2e d1 28 ed 4a 54 b1 13 7c b8 89

f7 62 13 6b df 95 88 28 b5 97 ba 52 ef e4 1d 28
ca 06 d1 36 b6 67 32 9a c2 dd 4e d8 c7 80 de 20
c5 b3 3e 1d 83 1a c7 fb 9d b8 c5 f5 ed 5f 34 36
BA 4f b6 b2 e2 2d 43 4f a0 b6 90 9a 11 3f 7d
0a 21 c3 4d3 0a d2 1e 33 43 d3 5e cc 4b 38 e0
الحمولة التالية:VID، محجوزة: 0x0، الطول: 24

8f 22 7b 16 23 52 e4 29 4d 98 c7 fd a8 77 12 20
ce 7c0b4
IKEv2-PROTO-5: تحليل الحمولة الخاصة بالمورد: الحمولة التالية من -Cisco-DELETE REASON: VID، محجوز: 0x0، الطول: 23
الحزمة التي تم فك تشفيرها:البيانات:528 بايت
IKEv2-PLAT-3: معالجة حمولات VID المخصصة
IKEv2-PLAT-3: تم تلقي حماية حقوق النسخ من Cisco من النظير
IKEv2-PLAT-3: تلقي AnyConnect EAP VID من نظير
IKEv2-Proto-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 0000000 CurState: حدث الخمول: **EV_RECV_INIT**
IKEv2-PROTO-3: (6): فحص اكتشاف nat
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 0000000 CurState: حدث الخمول: EV_CHK_REDIRECT
IKEv2-PROTO-5: (6): لا حاجة إلى إعادة توجيه التحقق، وتجاوزه
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 0000000 CurState: حدث الخمول: EV_CHK_CAC
IKEv2-PLAT-5: **تم قبول طلب IKEV2 SA الجديد**
IKEv2-PLAT-5: زيادة عدد عمليات التفاوض الواردة بمقدار واحد
IKEv2-PLAT-5: معالج PSH غير صالح
IKEv2-PLAT-5: معالج PSH غير صالح
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 0000000 CurState: حدث الخمول: EV_CHK_COOKIE
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 0000000 CurState: حدث :Idle EV_CHK_COOKIE_NOTIFY
IKEv2-Proto-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 0000000 CurState: حدث :R_INIT **EV_VERIFY_MSG**
IKEv2-PROTO-3: (6): **التحقق من صحة رسالة SA المضمنة**
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 0000000 CurState: حدث :R_INIT EV_INSERT_SA
IKEv2-PROTO-3: (6) إدراج SA
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 0000000 CurState: حدث :R_INIT EV_GET_IKE_POLICY
IKEv2-PROTO-3: (6): **الحصول على سياسات مكونة**
IKEv2-Proto-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 0000000 CurState: حدث :R_INIT **EV_PROC_MSG**
IKEv2-PROTO-2: (6) معالجة الرسالة الأولية
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B

يقوم مكتب المحاسبة بالتأكد من رسالة IKE_INIT. ال ASA:

1. يختار مجموعة التشفير من التي يقدمها البادئ.
2. يحسب المفتاح السري DH الخاص به.
3. حساب قيمة SKEYID من التي يمكن اشتقاق جميع المفاتيح من أجلها IKE_SA هذا. رؤوس الكل أما الرسائل التالية فهي مشفر ومصادق عليه. يعرض الأمر المفاتيح المستخدمة للتشفير و حماية التكامل مشتقة من SKEYID ومعروفة ب:

- **SK_E** - التشفير.**SK_A** - المصادقة.**SK_D** - مشتق ومستخدم لاشتقاق المزيد مواد تعبئة من أجل CHILD_SAs.فيما يلي نص منفصل ل sk_e و sk_a حسبت لكل إتجاه.

التكوين ذي الصلة:

```
crypto ikev2 policy 10
 encryption aes-192
           integrity
sha group 2  prf sha
           lifetime
       seconds 86400
crypto ikev2 enable
           outside
```

R_INIT: حدث :R_SPI=FC696330E6B94D7F (R) MSGid = 0000000 CurState
EV_DETECT_NAT
6) :IKEv2-PROTO-3): إعلام اكتشاف نقاط الشبكة (NAT) للعملية
6) :IKEv2-PROTO-5): معالجة NAT كشف SRC إعلام
6) :IKEv2-PROTO-5): العنوان البعيد غير مطابق
6) :IKEv2-PROTO-5): معالجة NAT كشف DST إعلام
6) :IKEv2-PROTO-5): العنوان المحلي مطابق
6) :IKEv2-Proto-5): المضيف موجود خارج NAT
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_INIT: حدث :R_SPI=FC696330E6B94D7F (R) MSGid = 0000000 CurState
EV_CHK_CONFIG_MODE
6) :IKEv2-PROTO-3): تم إستلام بيانات وضع التكوين الصحيحة
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_INIT: حدث :R_SPI=FC696330E6B94D7F (R) MSGid = 0000000 CurState
EV_SET_RED_CONFIG mode
6) :IKEv2-PROTO-3): تم إستلام مجموعة بيانات وضع التكوين
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_BLD_INIT :CurState (R) MSGid = 0000000 R_SPI=FC696330E6B94D7F حدث:
EV_SET_POLICY
6) :IKEv2-PROTO-3): **إعداد السياسات المكونة**
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_BLD_INIT :CurState (R) MSGid = 0000000 R_SPI=FC696330E6B94D7F حدث:
EV_CHK_AUTH4PKI عرى
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_BLD_INIT :CurState (R) MSGid = 0000000 R_SPI=FC696330E6B94D7F حدث:
EV_PKI_SSH_Open
6) :IKEv2-PROTO-3): افتتاح دورة PKI
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_BLD_INIT :CurState: 000000 MSGid = (R) R_SPI=FC696330E6B94D7F حدث:
EV_GEN_DH_DH_KEY
6) :IKEv2-PROTO-3): **إستخدام المفتاح العام DH**
6) :IKEv2-PROTO-3):
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_BLD_INIT :CurState (R) MSGid = 0000000 R_SPI=FC696330E6B94D7F حدث:
EV_NO_EVENT
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_BLD_INIT :CurState (R) MSGid = 0000000 R_SPI=FC696330E6B94D7F حدث:
EV_OK_OK_RED_RD Pubkey_RESP
6) :IKEv2-PROTO-5): الإجراء: action_null
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_BLD_INIT :CurState (R) MSGid = 0000000 R_SPI=FC696330E6B94D7F حدث:
EV_GEN_DH_DH_SECRET
6) :IKEv2-PROTO-3): **حساب مفتاح DH السري**
6) :IKEv2-PROTO-3):
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_BLD_INIT :CurState (R) MSGid = 0000000 R_SPI=FC696330E6B94D7F حدث:
EV_NO_EVENT
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_BLD_INIT :CurState (R) MSGid = 0000000 R_SPI=FC696330E6B94D7F حدث:
EV_OK_OK_RED_RD secret_resp
6) :IKEv2-PROTO-5): الإجراء: action_null
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_BLD_INIT :CurState (R) MSGid = 0000000 R_SPI=FC696330E6B94D7F حدث:

EV_GEN_SKEYID
6) :(IKEv2-PROTO-3: **إنشاء skeyid**
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MSGid = 0000000 CurState: R_BLD_INIT حدث:
EV_GET_CONFIG_MODE
يقوم ASA بإنشاء رسالة الاستجابة لتبادل IKE_SA_INIT.
تحتوي هذه الحزمة على:
1. **رأس** - ISAKMP SPI/الإصدار/العلاما ت.
2. **SAr1** - خوارزمية التشفير التي تختارها IKE Responder.
3. **KEr** - قيمة مفتاح DH العام لمستجيب الاستجابة.
4. **N** - Responder Nonce.

IKEv2-Proto-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MSGid = 0000000 CurState: R_BLD_INIT حدث:
EV_BLD_MSG
6) :(IKEv2-PROTO-2: **إرسال رسالة أولية**
IKEv2-Proto-3: مقترح 1 :IKE، حجم SPI: صفر (التفاوض الأولي)،
عدد عمليات التحويل: 4
AES-CBC SHA1 SHA96 DH_GROUP_768_MODP/Group 1
IKEv2-PROTO-5: إنشاء حمولة خاصة بالمورد: DELETE-REASONIKEv2-PROTO-5: إن
حمولة خاصة بالمورد: (CUSTOM)IKEv2-PROTO-5: إنشاء حمولة خاصة بالمورد:
(CUSTOM)IKEv2-PROTO-5: إنشاء Notify Payload:
NAT_DETECTION_SOURCE_IPIKEv2-PROTO-5: إنشاء حمولة الإعلام:
NAT_DETECTION_DESTINATION_IPIKE5 2-PLAT-2: فشل في إسترداد تجزئة المصدر
الموثوق به أو عدم توفر أي
IKEv2-PROTO-5: إنشاء حمولة المورد المحددة: التجزئة L] IKEv2-PROTO-3: Tx
10.0.0.1:500/R 192.168.1.1:25170/VRF i0:f0] m_id: 0x0
[IKEv2-Proto-3: **HDR.**[i:58AFF71141BA436B - R: FC696330E6B94D7F
Ev2-proto-4: IKEv2 HDR **ispi: 58AFF71141BA436B - RSPI: FC696330E6B94D7F**
IKEv2-PROTO-4: الحمولة التالية: SA، الإصدار 2.0
IKEv2-Proto-4: نوع Exchange: IKE_SA_INIT، **العلامات: المستجيب msg-response**
IKEv2-PROTO-4: معرف الرسالة: 0x0، الطول: 386
حمولة **SA** التالية: KE، محجوزة: 0x0، الطول: 48
IKEv2-PROTO-4: المقترح الأخير: 0x0، محجوز: 0x0، الطول: 44
المقترح: 1، معرف البروتوكول: IKE، حجم #trans: 4 ،SPI: 0
IKEv2-PROTO-4: آخر تحويل: 0x3، محجوز: 0x0: الطول: 12
النوع: 1، محجوز: 0x0، المعرف: AES-CBC
IKEv2-PROTO-4: آخر تحويل: 0x3، محجوز: 0x0: الطول: 8
النوع: 2، محجوز: 0x0، المعرف: SHA1
IKEv2-PROTO-4: آخر تحويل: 0x3، محجوز: 0x0: الطول: 8
النوع: 3، محجوز: 0x0، المعرف: SHA96
IKEv2-PROTO-4: آخر تحويل: 0x0، محجوز: 0x0: الطول: 8
النوع: 4، محجوز: 0x0، المعرف: DH_GROUP_768_MODP/Group 1

الحمولة التالية **ل KE:N، محجوز: 0x0، الطول: 104**
مجموعة DH: 1، محجوز: 0x0

c9 30 f9 32 d4 7c d1 a7 5b 71 09 6e 7e 91 0c
e1 ce b4 a4 3c f2 8b 74 4e 20 59 b4 0b1 ff 65
cc c4 a4 b6 fa 4a 63 03 93 89 e1 bd 6a 88 37
9a 38 24 e2 a8 40 f5 a3 d6 ef f7 1a df 33 cc 64
a1 8e fa dc 9c 34 45 79 1a 7c 29 05 87 8a ac 02
2e 7d cb 41 51 d6 fe fc c7 76 83 1d 03 b0 d7 98
الحمولة التالية:VID، محجوزة: 0x0، الطول: 24

c2 28 7f 8c 7d b3 1e 51 fc eb f1 97 ec 97 b8 67
d5 e7 c2 f5
حمولة VID التالية: VID، محجوز: 0x0، الطول: 23
يرسل ASA رسالة الاستجابة لتبادل IKEv2-PLAT-4: Sent PKT ********** التاريخ: 2013/04/23 م -500:[10.0.0.1] [IKE_SA_INIT]

IKE_SA_INIT. تم الآن إكمال تبادل IKE_SA_INIT. يبدأ ال ASA المؤقت لعملية المصادقة.

>[192.168.1.1]:25170
InitSPI=0x58aff71141ba436b
RespSPI=0xfc69630e6b94d7f
mid=0000000000000000000000b
0
IKEv2-PROTO-5: (6): SM Trace->
SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R)
MSGid = 0000000 CurState:
INIT_DONE حدث: EV_DONE
6) :IKEv2-PROTO-3): تم تمكين
التجزئة
6) :IKEv2-PROTO-3): تم تمكين
Cisco DeleteReason Notify
6) :IKEv2-PROTO-3): استكمال تبادل
SA Init
IKEv2-PROTO-5: (6): SM Trace->
SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R)
MSGid = 0000000 CurState: حدث
INIT_DONE: EV_CHK4_ROLE
IKEv2-PROTO-5: (6): SM Trace->
SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R)
MSGid = 0000000 CurState:
INIT_DONE حدث:
.EV_START_TMR
6) :IKEv2-PROTO-3): بدء المؤقت
لانتظار رسالة المصادقة (30 ثانية)
IKEv2-PROTO-5: (6): SM Trace->
SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R)
MSGid = 0000000 CurState:
R_WAIT_AUTH الحدث:
EV_NO_EVENT
—IKE_SA_INIT كامل—
— تبدأ IKE_AUTH—
****

التاريخ: 2013/04/23 م
الوقت: 16:25:00
النوع : المعلومات
المصدر:

الوصف: معلمات العبارة الآمنة:
عنوان IP: 10.0.0.1
المنفذ: 443
"URL: "10.0.0.1
أسلوب المصادقة: **IKE - EAP-AnyConnect**
هوية IKE:
****

التاريخ: 2013/04/23 م
الوقت: 16:25:00
النوع : المعلومات

الوقت: 16:25:02
النوع : المعلومات
المصدر:

الوصف: الوظيفة: CIPsecProtocol::startTunnel
الملف: .\IPsecProtocol.cpp
السطر: 345
يتم الآن بدء تشغيل نفق IPsec
****

المصدر:

الوصف: **بدء تشغيل اتصال Cisco AnyConnect Secure Mobility Client، الإصدار 3.0.1047**
****
التاريخ: 2013/04/23 م
الوقت: 16:25:02
النوع : المعلومات
المصدر:

الوصف: الوظيفة: ikev2_log
الملف: .\ikev2_anyconnect_osal.cpp
السطر: 2730
تم تلقي طلب لإنشاء نفق IPsec؛ محدد حركة المرور المحلية = نطاق العنوان: 0.0.0.0-255.255.255.255 البروتوكول: 0 نطاق منفذ: 0-65535؛ محدد حركة المرور عن بعد = نطاق العنوان: 0.0.0.0-255.255.255.255 البروتوكول: 0 نطاق منفذ: 0-65535
****
التاريخ: 2013/04/23 م
الوقت: 16:25:02
النوع : المعلومات
المصدر:

الوصف: الوظيفة: CIPsecProtocol::connectTransport
الملف: .\IPsecProtocol.cpp
السطر: 1629
مقبس IKE المفتوح من 192.168.1.1:25171 إلى 10.0.0.1:4500
****

تتم المصادقة مع EAP. يسمح فقط بأسلوب مصادقة EAP واحد في محادثة EAP. يتلقى ASA رسالة IKE_AUTH من العميل.

IKEv2-PLAT-4:**RECV PKT [IKE_AUTH]** [192.168.1.1]:25171->[10.0.1]:**4500** InitSPI=0x58aff71141ba436b RespSPI=0xfc69630e6b94d7MID=0000 0001
IKEv2-PROTO-3: **Rx** [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id: 0x1

عندما يتضمن العميل حمولة IDi ولكن ليس حمولة المصادقة، وهذا يشير لقد أعلن العميل عن هوية لكنه لم يثبت ذلك. في تصحيح الأخطاء، المصادقة الحمولة غير موجودة في IKE_AUTH

[IKEv2-Proto-3: **HDR.**[i:58AFF71141BA436B - R: FC696330E6B94D7F
Ev2-proto-4: IKEv2 **HDR ispi: 58AFF71141BA436B - RSPI: FC696330E6B94D7F**
IKEv2-PROTO-4: الحمولة التالية: ENCR، **الإصدار: 2.0**
IKEv2-PROTO-4: نوع التبادل: IKE_AUTH، **العلامات: البادئ**
IKEv2-PROTO-4: معرف الرسالة: 0x1، الطول: 540
6) :IKEv2-PROTO-5): يحتوي الطلب على 1 MESS_ID، متوقع من 1 إلى 1
حزمة تم فك تشفيرها فعليا:بيانات: 465 بايت
IKEv2-PROTO-5: تحليل الحمولة الخاصة بالمورد: (CUSTOM) الحمولة التالية: IDi، محجوز: 0x0، الطول: 20

الحزمة المرسلة بواسطة العميل. العميل إرسال حمولة المصادقة فقط بعد تم تبادل EAP بنجاح. إذا مستعد لاستخدام موسع أسلوب المصادقة، فإنه يضع EAP الحمولة في الرسالة 4 وتأجيل الإرسال TSi ،SAr2، و TSr حتى

58 أف 6 و 11 و 52 ث 8 ب0 و 2c b8 و 30 و 46 ب 91 و 56 أ
الحمولة التالية **من IDi:CERTREQ، محجوزة: 0x0، الطول: 28**
نوع المعرف: اسم المجموعة، محجوز: 0x0 0x0

2a 24 41 6e 79 43 6f 6e 65 63 74 43 6c 69 65
6e 74 24 2a
الحمولة التالية **ل** CFG :**CERTREQ**، محجوزة: 0x0، الطول: 25
شهادة ترميز X.509 - توقيع
CertReq Data&colon؛ 20 بايت
الحمولة التالية من SA :**CFG**، محجوزة: 0x0، الطول: 196
cfg نوع: **CFG_REQUEST**، محجوز: 0x0، محجوز: 0x0

البادئ
اكتملت المصادقة في تبادل IKE_AUTH اللاحق.
تحتوي حزمة بادئ IKE_AUTH على:

1. **رأس ISAKMP** - SPI/الإصدار/العلاما ت.
2. **IDi** - اسم مجموعة النفق الذي يرغب العميل في الاتصال ب قد يتم تسليمها بواسطة IDi الحمولة من النوع ID_KEY_ID في الرسالة الأولية تبادل IKE_AUTH. هذا يحدث عندما يكون ملف تعريف العميل* مكون مسبقا باسم مجموعة أو بعد نجاح سابق المصادقة، لدى العميل تم تخزين اسم المجموعة مؤقتا في ملف التفضيلات. ال ASA محاولات لمطابقة مجموعة نفق الاسم مع محتويات IKE حمولة IDi. بعد الأول الشبكة الخاصة الظاهرية (VPN) الناجحة ل IPSec التي تم إنشاؤها، يقوم العميل بتخزين ذاكرة التخزين المؤقت اسم المجموعة (الاسم المستعار للمجموعة) الذي يتم الوصول إليه قام المستخدم بالتصديق. هذه

نوع الجهاز: عنوان IP4 داخلي، الطول: 0

نوع الجهاز: قناع الشبكة الداخلي ل IP4، الطول: 0

نوع Attrib: DNS داخلي ل IP4، الطول: 0

نوع الجهاز: IP4 NBNS داخلي، الطول: 0

نوع attrib: انتهاء صلاحية العنوان الداخلي، الطول: 0

النوع ATTRIB: إصدار التطبيق، الطول: 27

6e 79 43 6f 6e 6e 65 63 74 20 57 69 6e 64 6f 41
2e 30 2e 31 30 34 37 33 20 73 77

نوع الجهاز: عنوان IP6 داخلي، الطول: 0

نوع الجهاز: شبكة IP4 الفرعية الداخلية، الطول: 0

نوع attrib: غير معروف - 28682، الطول: 15

6e 78 70 36 34 74 65 6d 70 6c 61 74 65 69 77

نوع attrib: غير معروف - 28704، الطول: 0

نوع attrib: غير معروف - 28705، الطول: 0

نوع attrib: غير معروف - 28706، الطول: 0

نوع attrib: غير معروف - 28707، الطول: 0

نوع attrib: غير معروف - 28708، الطول: 0

نوع attrib: غير معروف - 28709، الطول: 0

نوع attrib: غير معروف - 28710، الطول: 0

نوع attrib: غير معروف - 28672، الطول: 0

نوع attrib: غير معروف - 28684، الطول: 0

نوع attrib: غير معروف - 28711، الطول: 2

057 اس

نوع attrib: غير معروف - 28674، الطول: 0

نوع attrib: غير معروف - 28712، الطول: 0

نوع attrib: غير معروف - 28675، الطول: 0

نوع attrib: غير معروف - 28679، الطول: 0

نوع attrib: غير معروف - 28683، الطول: 0

المجموعة
نوع attrib: غير معروف - 28717، الطول: 0

تم تسليم الاسم في IDi
نوع attrib: غير معروف - 28718، الطول: 0

حمولة الاتصال التالي محاولة للإشارة إلى
نوع attrib: غير معروف - 28719، الطول: 0

مجموعة محتملة مرغوبة
نوع attrib: غير معروف - 28720، الطول: 0

مستخدم. عندما تكون مصادقة EAP
نوع attrib: غير معروف - 28721، الطول: 0

محدد أو ضمني من قبل العميل
نوع attrib: غير معروف - 28722، الطول: 0

التوصيف ولا يحتوي على <IKEIdentity>
نوع attrib: غير معروف - 28723، الطول: 0

عنصر، يرسل العميل حمولة ID_GROUP IDi
نوع attrib: غير معروف - 28724، الطول: 0

مع السلسلة الثابتة *$AnyConnectCli$ent*.
نوع attrib: غير معروف - 28725، الطول: 0

نوع attrib: غير معروف - 28726، الطول: 0

نوع attrib: غير معروف - 28727، الطول: 0

نوع attrib: غير معروف - 28729، الطول: 0

3. **CERTREQ** -

العميل هو طلب ASA ل الشهادة المفضلة. شهادة قد يتم تضمين حمولة الطلب في تبادل عندما يقوم المرسل بحاجة للحصول على شهادة جهاز إستقبال. طلب الشهادة تتم معالجة الحمولة بواسطة فحص 'ترميز Cert' لتحديد الحقل ما إذا كان المعالج يحتوي على شهادات من هذا النوع. وإذا كان الأمر كذلك، فإن حقل 'المرجع المصدق' هو تم فحصها لتحديد ما إذا للمعالج أي شهادات

حمولة **SA** التالية: TSi، محجوزة: 0x0، الطول: 124
IKEv2-PROTO-4: المقترح الأخير: 0x0، محجوز: 0x0، الطول: 120
المقترح: 1، معرف البروتوكول: ESP، حجم SPI: 4، #trans: 12
IKEv2-PROTO-4: آخر تحويل: 0x3، محجوز: 0x0: الطول: 12
النوع: 1، محجوز: 0x0، المعرف: AES-CBC
IKEv2-PROTO-4: آخر تحويل: 0x3، محجوز: 0x0: الطول: 12
النوع: 1، محجوز: 0x0، المعرف: AES-CBC
IKEv2-PROTO-4: آخر تحويل: 0x3، محجوز: 0x0: الطول: 12
النوع: 1، محجوز: 0x0، المعرف: AES-CBC
IKEv2-PROTO-4: آخر تحويل: 0x3، محجوز: 0x0: الطول: 8
النوع: 1، محجوز: 0x0، المعرف: 3DES
IKEv2-PROTO-4: آخر تحويل: 0x3، محجوز: 0x0: الطول: 8
النوع: 1، محجوز: 0x0، المعرف: DES
IKEv2-PROTO-4: آخر تحويل: 0x3، محجوز: 0x0: الطول: 8
النوع: 1، محجوز: 0x0، المعرف: NULL
IKEv2-PROTO-4: آخر تحويل: 0x3، محجوز: 0x0: الطول: 8
النوع: 3، محجوز: 0x0، المعرف: SHA512
IKEv2-PROTO-4: آخر تحويل: 0x3، محجوز: 0x0: الطول: 8
النوع: 3، محجوز: 0x0، المعرف: SHA384
IKEv2-PROTO-4: آخر تحويل: 0x3، محجوز: 0x0: الطول: 8
النوع: 3، محجوز: 0x0، المعرف: SHA256
IKEv2-PROTO-4: آخر تحويل: 0x3، محجوز: 0x0: الطول: 8
النوع: 3، محجوز: 0x0، المعرف: SHA96
IKEv2-PROTO-4: آخر تحويل: 0x3، محجوز: 0x0: الطول: 8
النوع: 3، محجوز: 0x0، المعرف: MD596
IKEv2-PROTO-4: آخر تحويل: 0x0، محجوز: 0x0: الطول: 8
النوع: 5، محجوز: 0x0، المعرف:

الحمولة التالية ل TSr :**TSi**، محجوزة: 0x0، الطول: 24

num of TSs: 1، محجوز 0x0، محجوز 0x0
نوع TS: TS_IPv4_ADDR_RANGE، معرف الإصدار: 0، الطول: 16
منفذ البدء: 0 ومنفذ النهاية: 65535
بداية العنوان: 0.0.0.0، نهاية العنوان: 255.255.255.255
الحمولة التالية ل **TSr**: الإعلام، محجوز: 0x0، الطول: 24
num of TSs: 1، محجوز 0x0، محجوز 0x0
نوع TS: TS_IPv4_ADDR_RANGE، معرف الإصدار: 0، الطول: 16
منفذ البدء: 0 ومنفذ النهاية: 65535
بداية العنوان: 0.0.0.0، نهاية العنوان: 255.255.255.255

يمكن التحقق من صحة حتى واحد من الشهادة المحددة السلطات. يمكن أن تكون هذه سلسلة من الشهادات.

4. **cfg** - /CFG_REQUEST يسمح CFG_REPLY باستخدام IKE نقطة النهاية لطلب المعلومات من نظيرتها. في حالة وجود سمة في تكوين CFG_REQUEST الحمولة ليست صفرية الطول، إنها اتخذ كاقتراح لذلك attribute.ال cfg_REPLY قد تعود حمولة التكوين تلك القيمة أو قيمة جديدة. قد يكون أيضا أضف سمات جديدة ولا اشملوا بعض الطلبات. تم إرجاع الطالب المتجاهل سمات لا تعرف على. في هذه التصحيح، العميل يطلب النفق التكوين في cfg_request. ال ASA يرد على هذا ويرسل النفق سمات التكوين فقط بعد تم تبادل EAP بنجاح.
5. **SAi2** - يبدأ SAi2 SA،

وهو ما يشبه المرحلة الثانية
تحويل مجموعة التبادل في IKEv1.

6. **TSi** و**TSr** - البادئ و محددات حركة مرور المستجيب يحتوي، على التوالي، على المصدر و غاية عنوان البادئ والمستجيب من أجل تشفير إعادة التوجيه والاستقبال المرور. نطاق العنوان يحدد أن كل حركة المرور من وإلى ذلك المدى هو نفق. إذا الاقتراح مقبول لدى المستجيب، هو يرسل TS متماثل الحمولات إلى الخلف.

السمات التي يجب على العميل تسليمها
يتم تخزين مصادقة المجموعة في ملف تعريف AnyConnect.

***تكوين ملف التعريف ذي الصلة:**

```
<ServerList>
 <HostEntry>
HostName>Anu-IKEV2>
 <HostName/>
HostAddress>10.0.0.1>
 <HostAddress/>
```

```
PrimaryProtocol>IPsec>
 <PrimaryProtocol/>
 <HostEntry/>
<ServerList/>
```

الحزمة التي تم فك تشفيرها: Data&colon؛ 540 بايت
يقوم ASA بإنشاء إستجابة لرسالة IKE_AUTH ويستعد للمصادقة على IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 000001 CurState: R_WAIT_AUTH الحد

العميل.
EV_RECV_AUTH
6) :IKEv2-PROTO-3): إيقاف المؤقت لانتظار رسالة المصادقة
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MSGid = 000001 CurState: R_WAIT_AUTH الحد
EV_CHK_NAT_T
6) :IKEv2-PROTO-3): فحص اكتشاف nat
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MSGid = 000001 CurState: R_WAIT_AUTH الحد
EV_CHG_NAT_T المنفذ
IKEv2-PROTO-2: (6): NAT Detected float to init port 25171، resp port 4500
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MSGid = 0000001 CurState: R_WAIT_AUTH
EV_PROC_ID الحدث:
6) :IKEv2-PROTO-2): معلمات صحيحة تم الحصول عليها في معرف العملية
6) :IKEv2-PLAT-3) طريقة مصادقة النظير المعينة إلى: 0
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MSGid = 000001 CurState: R_WAIT_AUTH الحد
EV_CHK_IF_PEER cert_needs_to_be_get_for_prof_sel
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MSGid = 000001 CurState: R_WAIT_AUTH الحد
EV_GET_POLICY_BY_PEE جريد
6) :IKEv2-PROTO-3): الحصول على سياسات مكونة
IKEv2-PLAT-3: تم اكتشاف اتصال عميل AnyConnect جديد استنادا إلى حمولة المعرف
IKEv2-PLAT-3: my_auth_method = 1
6) :IKEv2-PLAT-3) طريقة مصادقة النظير المعينة إلى: 256
IKEv2-PLAT-3: supported_peers_auth_method = 16
IKEv2-PLAT-3: (6) tp_name معين إلى: Anu-ikev2
IKEv2-PLAT-3: **تم تعيين نقطة الثقة إلى:** Anu-ikev2
IKEv2-PLAT-3: معرف 0 = P1
IKEv2-PLAT-3: ترجمة ike_ID_AUTO إلى = 9
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MSGid = 000001 CurState: R_WAIT_AUTH الحد
EV_SET_POLICY
6) :IKEv2-PROTO-3): **إعداد السياسات المكونة**
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MSGid = 0000001 CurState: R_WAIT_AUTH
EV_VERIFY_POLICY_BY_PEE جريد الحدث:
6) :IKEv2-PROTO-3): التحقق من سياسة النظير
6) :IKEv2-PROTO-3): **تم العثور على شهادة مطابقة**
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MSGid = 000001 CurState: R_WAIT_AUTH الحد
EV_CHK_CONFIG
6) :IKEv2-PROTO-3): تم إستلام بيانات وضع التكوين الصحيحة
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MSGid = 000001 CurState: R_WAIT_AUTH الحد
EV_SET_RED_CONFIG نمط
6) :IKEv2-PLAT-3) تم تعيين اسم مضيف DHCP ل DDNS على: WinXP64template
6) :IKEv2-PROTO-3): تم إستلام مجموعة بيانات وضع التكوين
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MSGid = 000001 CurState: R_WAIT_AUTH الحد
EV_CHK_AUTH4EAP
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MSGid = 000001 CurState: R_WAIT_AUTH الحد

EV_CHK_EAP
6) :IKEv2-PROTO-3): **التحقق من تبادل EAP**
IKEv2-Proto-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MSGid = 000001 CurState: **R_BLD_AUTH** الحدث
EV_GEN_AUTH عرى
6) :IKEv2-PROTO-3): **إنشاء بيانات المصادقة الخاصة بي**
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MSGid = 000001 CurState: R_BLD_AUTH الحدث
EV_CHK4_SIGN
6) :IKEv2-PROTO-3): احصل على طريقة المصادقة الخاصة بي
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MSGid = 000001 CurState: R_BLD_AUTH حدث:
EV_SIGN
6) :IKEv2-PROTO-3): **توقيع بيانات المصادقة**
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MSGid = 000001 CurState: R_BLD_AUTH الحدث
EV_OK_AUTH_AUGEN
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MSGid = 000001 CurState:
R_BLD_EAP_AUTH_REQ حدث: EV_THEN_req
6) :IKEv2-PROTO-2): **الطلب من المصدق إرسال طلب EAP**
قيمة config-auth للعنصر الذي تم إنشاؤه
قيمة عميل اسم السمة المضافة VPN إلى عنصر config-auth
قيمة نوع اسم السمة المضافة مرحبا بها للعنصر config-auth
قيمة الإصدار 9.0(2)8 الخاصة باسم العنصر الذي تم إنشاؤه
قيمة إصدار اسم العنصر المضاف 9.0(2)8 إلى عنصر config-auth
اسم السمة المضافة الذي يقدر sg لإصدار العنصر
رسالة XML المنشأة أدناه
<؟"xml version="1.0" encoding="UTF-8؟>
<"config-auth client="vpn" **type="hello>**
<version who="sg">9.0(2)8</version>
<config-auth/>

IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MSGid = 000001 CurState:
R_BLD_EAP_AUTH_REQ حدث: V_REQ_EAP_AUTH
6) :IKEv2-PROTO-5): الإجراء: action_null
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MSGid = 000001 CurState:
R_BLD_EAP_AUTH_REQ حدث: EV_k_إعادة التوجيه
6) :IKEv2-PROTO-3): إعادة توجيه الفحص باستخدام النظام الأساسي لموازنة الأحمال
IKEv2-PLAT-3: مراجعة إعادة التوجيه للنظام الأساسي
IKEv2-PLAT-3: ikev2_osal_redirect: جلسة مقبولة من قبل 10.0.0.1
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MSGid = 000001 CurState:
EV_SEND_EAP_AUTH_REQ حدث: R_BLD_EAP_AUTH_REQ
6) :IKEv2-PROTO-2): **إرسال طلب EAP**
IKEv2-PROTO-5: إنشاء حمولة خاصة بالمورد: 6) :Cisco-GraniteikeV2-Proto-3): إنشاء
الحمولة التالية:CERT، محجوزة: 0x0، الطول: 36
نوع المعرف: DER ASN1 DN، محجوز: 0x0 0x0

يرسل ASA حمولة المصادقة لطلب بيانات اعتماد المستخدم من العميل. يرسل ASA أسلوب المصادقة ك 'RSA،' لذلك

30 01 09 0d f7 86 48 86 09 2a 06 16 30 18 31 1a
02 09 16 41 53 41 32 56 45 4b 49 2d

يرسل شهادته الخاصة إلى العميل، بحيث يمكن للعميل مصادقة خادم ASA.
بما أن ASA يرغب في إستخدام أسلوب مصادقة قابل للتوسيع، فإنه يضع حمولة EAP في الرسالة 4 ويؤجل إرسال SAr2 و TSi و TSr حتى تكتمل مصادقة البادئ في تبادل IKE_AUTH لاحق.
وبالتالي، هذه الحمولات الثلاث غير موجودة في عمليات تصحيح الأخطاء.
تحتوي حزمة EAP على:

1. **الرمز: الطلب** - يتم إرسال هذا الرمز بواسطة المصدق إلى النظير.
2. **المعرف: 1** - يساعد المعرف في مطابقة استجابات EAP مع الطلبات. هنا القيمة 1، وهو ما يشير إلى أنها الحزمة الأولى في تبادل EAP. يحتوي طلب EAP هذا على نوع "config-auth" من "hello"؛ حيث يتم إرساله من ASA إلى العميل لبدء تبادل EAP.
3. **الطول: 150** - يتضمن طول حزمة EAP الرمز ومعرف البيانات وطولها وبيانات EAP.
4. **بيانات EAP**.

الحمولة التالية:CERT، محجوزة: 0x0، الطول: 436
شهادة **ترميز X.509** - توقيع
CERT Data&colon؛ 431 بايت
الحمولة التالية: المصادقة، المحجوزة: 0x0، الطول: 436
شهادة ترميز X.509 - توقيع
CERT Data&colon؛ 431 بايت
حمولة **المصادقة** التالية: EAP، محجوزة: 0x0، الطول: 136
RSA لطريقة المصادقة، محجوز: 0x0، محجوز 0x0
بيانات المصادقة والقولون، 128 بايت
حمولة **EAP** التالية: لا شيء، محجوز: 0x0، الطول: 154
الرمز: الطلب: **المعرف**: 1، **الطول**: 150
نوع: غير معروف - 254
بيانات 145 :**EAP** بايت

IKEv2-PROTO-3: Tx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id: 0x1
[IKEv2-Proto-3: **HDR.**[i:58AFF71141BA436B - R: FC696330E6B94D7F
Ev2-Proto-4: **IKEv2 HDR ispi: 58AFF71141BA436B - RSPI: FC696330E6B94D7F**
IKEv2-PROTO-4: الحمولة التالية: ENCR، الإصدار: 2.0
IKEv2-Proto-4: نوع Exchange: IKE_AUTH، **العلامات: المستجيب msg-response**
IKEv2-PROTO-4: معرف الرسالة: 0x1، الطول: 1292
الحمولة التالية ل ENCR: VID، محجوز: 0x0، الطول: 1264
بيانات مشفرة&1260، colon بايت

يمكن أن ينتج عن التجزئة إذا كانت الشهادات كبيرة أو إذا تم تضمين سلاسل شهادات. كما يمكن أن تتضمن كل من حمولة KE الخاصة بالمنشئ والمستجيب مفاتيح كبيرة، والتي يمكن أن تساهم أيضا في التجزئة.

(6 :IKEv2-Proto-5): تجزئة الحزمة، تجزئة وحدة الحد الأقصى للنقل (MTU: 544)، **عدد الأجزاء**
معرف الجزء: 1
IKEv2-PLAT-4: Sent PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc69630e6b94d7f
mid=000000000010000b
IKEv2-PLAT-4: Sent PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc69630e6b94d7f
mid=000000000010000b
IKEv2-PLAT-4: Sent PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc69630e6b94d7f
mid=000000000010000b
****

التاريخ: 2013/04/23 م
الوقت: 16:25:02
النوع : المعلومات
المصدر:

الوصف: الدالة: ikev2_verify_x509_sig_certs
الملف: .\ikev2_anyconnect_osal.cpp
السطر: 2077
طلب قبول الشهادة من المستخدم
****

التاريخ: 2013/04/23 م
الوقت: 16:25:02
النوع: خطأ
المصدر: أكفبنوي

الوصف: الوظيفة: CapiCertificate::verifyChainPolicy
الملف: .\Certificates\CapiCertificate.cpp
السطر: 2032
دالة تم الاستدعاء: CertVerifyCertificateChainPolicy
رمز الإرجاع: -2146762487 (0x800b0109)
الوصف: تمت معالجة سلسلة شهادات لكنها انتهت في شهادة جذر غير موثوق بها من قبل موفر الضمان.
****

التاريخ: 2013/04/23 م
الوقت: 16:25:04
النوع : المعلومات
المصدر:

الوصف: الوظيفة: CEAPMgr::DataRequestCB
الملف: .\EAPMgr.cpp
السطر: 400
النوع المقترح من EAP: EAP-Anyconnect
****

يستجيب العميل لطلب EAP باستجابة.
تحتوي حزمة EAP على:

1. **الرمز: الاستجابة** - يتم إرسال هذا الرمز بواسطة النظير إلى المصدق إستجابة لطلب EAP.
2. **المعرف: 1** - يساعد المعرف في مطابقة استجابات EAP مع الطلبات. هنا القيمة 1، وهو ما يشير إلى أن هذا هو إستجابة للطلب الذي تم إرساله مسبقا من قبل ASA (المصدق). تحتوي

IKEv2-PLAT-4: **RECV PKT [IKE_AUTH]** [192.168.1.1]:25171->[10.0.1]:4500 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f=0000000000 002
IKEv2-PROTO-3: Rx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id: 0x2
[IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: FC696330E6B94D7F
IKEv2-PROTO-4: IKEv2 HDR ispi: 58AFF71141BA436B - RSPI: FC696330E6B94D7F
IKEv2-PROTO-4: الحمولة التالية: ENCR، الإصدار: 2.0
IKEv2-PROTO-4: نوع التبادل: IKE_AUTH، العلامات: البادئ
IKEv2-PROTO-4: معرف الرسالة: 0x2، الطول: 332
IKEv2-PROTO-5: (6): يحتوي الطلب على 2 MESS_ID؛ المتوقع من 2 إلى 2
حزمة تم فك تشفيرها فعليا:بيانات: 256 بايت
حمولة **EAP** التالية: لا شيء، محجوز: 0x0، الطول: 256
الرمز: الرد: **المعرف: 1**، **الطول**: 252
نوع: غير معروف - 254
بيانات 247:**EAP** بايت
الحزمة التي تم فك تشفيرها: Data&colon؛ 332 بايت
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B SPI=FC696330E6B94D7F (R) MSGid = 0000002 CurState: R_WAIT_EAP_RESP
الحدث: EV_REV_AUTH
IKEv2-PROTO-3: (6): إيقاف المؤقت لانتظار رسالة المصادقة

إستجابة EAP هذه على النوع 'config-auth' من 'init'؛ يقوم العميل بتهيئة تبادل EAP وينتظر أن يقوم ASA بإنشاء طلب المصادقة.

3. **الطول: 252** - يتضمن طول حزمة EAP الرمز ومعرف البيانات وطولها وبيانات EAP.
4. **بيانات EAP**.

يقوم ASA بفك تشفير هذه الاستجابة، ويقول العميل إنه استلم حمولة المصادقة في الحزمة السابقة (مع الشهادة) وتلقى أول حزمة طلب EAP من ASA. هذا ما تحتوي عليه حزمة إستجابة EAP "init".

هذا هو الطلب الثاني الذي يتم إرساله من قبل ASA إلى العميل.

تحتوي حزمة EAP على:

1. **الرمز: الطلب** - يتم إرسال هذا الرمز بواسطة المصدق إلى النظير.
2. **المعرف: 2** - يساعد المعرف في مطابقة استجابات EAP مع الطلبات. هنا القيمة 2، وهو ما يشير إلى أنها الحزمة الثانية في التبادل. يحتوي هذا الطلب على النوع "config-auth" من "طلب المصادقة"؛ يطلب ASA من العميل إرسال بيانات اعتماد مصادقة المستخدم.
3. **الطول: 457** - يتضمن طول حزمة EAP الرمز ومعرف البيانات وطولها وبيانات EAP.
4. **بيانات EAP**.

```
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
SPI=FC696330E6B94D7F (R) MSGid = 0000002 CurState: R_WAIT_EAP_RESP
الحدث: EV_REV_EAP_RESP
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
_SPI=FC696330E6B94D7F (R) MSGid = 000002 CurState: R_PROC_EAP_RESP
حدث: EV_PROC_MSSP G
(IKEv2-Proto-2: (6 معالجة إستجابة EAP
تم تلقي رسالة XML أدناه من العميل
<؟"xml version="1.0" encoding="UTF-8؟>
<"config-auth client="vpn" type="init>
<device-id>win</device-id>
<version who="vpn">3.0.1047</version>
<group-select>ASA-IKEV2</group-select>
<group-access>ASA-IKEV2</group-access>
<config-auth/>
IKEv2-Proto-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MSGid = 0000002 CurState:
R_PROC_EAP_RESP event: EV_RECP_EAP_AUTH
(IKEv2-PROTO-5: (6: الإجراء: action_null
IKEv2-Proto-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MSGid = 0000002 CurState: R_BLD_EAP_REQ
حدث: EV_REQ_EAP_REQ
(IKEv2-PROTO-2: (6 إرسال طلب EAP
رسالة XML المنشأة أدناه
xml version="1.0"؟>
encoding="UTF-8"؟>
config-auth client="vpn">
<"type="auth-request
version>
<who="sg">9.0(2)8</version
<"opaque is-for="sg>
tunnel-group>ASA-<
IKEV2</tunnel-group>
config-<
hash>1367268141499</config-
hash>
<opaque/>
<csport>443</csport>
<"auth id="main>
<نموذج>
input type="text">
name="username"
<label="username:"></input
input type="password">
name="password"
<label="password:"></input
<form/>
<auth/>
<config-auth/>
(IKEv2-PROTO-3: (6: حزمة بناء للتشفير؛ المحتويات هي:

**********
التاريخ: 2013/04/23 م
الوقت: 16:25:04
النوع : المعلومات
المصدر: أكفبنوي

الوصف: الوظيفة: SDIMgr::ProcessPromptData
الملف: .\SDIMgr.cpp
السطر: 281
نوع المصادقة ليس SDI.
**********
التاريخ: 2013/04/23 م
الوقت: 16:25:07
النوع : المعلومات
المصدر: أكفبنوي

الوصف: الوظيفة: ConnectMgr::userResponse
الملف: .\ConnectMgr.cpp
السطر: 985
يتم الآن معالجة إستجابة المستخدم.
**********
```

حمولة **ENCR**:
يتم فك تشفير هذه الحمولة، ويتم تحليل محتوياتها كحمولات إضافية.

حمولة **EAP** التالية: لا شيء، محجوز: 0x0، الطول: 461
الرمز: الطلب: المعرف: 2، الطول: 457
نوع: غير معروف - 254
بيانات 452 :**EAP** بايت

IKEv2-PROTO-3: Tx [L
10.0.0.1:4500/R
192.168.1.1:25171/VRF i0:f0]
m_id: 0x2
IKEv2-Proto-3:
HDR.[i:58AFF71141BA436B - R:
FC696330E6B94D7F]
IKEv2-PROTO-4: IKEv2 HDR ispi:
58AFF71141BA436B - RSPI:
FC696330E6B94D7F
IKEv2-PROTO-4: الحمولة التالية:
ENCR، الإصدار: 2.0
IKEv2-Proto-4: نوع :Exchange
IKE_AUTH، العلامات: **Responder**
MSG-RESPONSE
IKEv2-PROTO-4: معرف الرسالة:
0x2، الطول: 524
الحمولة التالية **ل** EAP :**ENCR**،
محجوزة: 0x0، الطول: 496
بيانات مشفرة&492 ،colon بايت

PKT IKEv2-PLAT-4: **المرسل**
IKE_AUTH] [10.0.0.1]:4500-[
>[192.168.1.1]:25171<
InitSPI=0x58aff71141ba436b
RespSPI=0xfc69630e6b94d7f=000
0000000000b 002
IKEv2-PROTO-5: (6): SM Trace->
SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R)
MSGid = 000002 CurState:
R_BLD_EAP_REQ event:
.EV_START_TMR
6) :IKEv2-PROTO-3): **بدء عداد الوقت**
لانتظار رسالة مصادقة المستخدم (120
ثانية)
IKEv2-PROTO-5: (6): SM Trace->
SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R)
MSGid = 0000002 CurState:
R_WAIT_EAP_RESP حدث:
EV_NO_EVENT

يرسل العميل رسالة بدء IKE_AUTH أخرى بحمولة EAP.
IKEv2-PLAT-4: Recv PKT [IKE_AUTH] [192.168.1.1]:25171->[10.0.0.1]:4500 InitSPI=0x58aff71141ba436b RespSPI=0xfc69630e6b94d7f mid=00000000000000000000000b000000b0b 3

تحتوي حزمة EAP على:
1. **الرمز: الاستجابة** -
IKEv2-PROTO-3: Rx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id: 0x3
[IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: FC696330E6B94D7F

يتم إرسال هذا الرمز بواسطة النظير إلى المصدق إستجابة لطلب EAP.

IKEv2-PROTO-4: IKEv2 HDR ispi: 58AFF71141BA436B - RSPI: FC696330E6B94D7F
IKEv2-PROTO-4: الحمولة التالية: ENCR، الإصدار: 2.0
IKEv2-PROTO-4: **نوع Exchange: IKE_AUTH، العلامات: البادئ**
IKEv2-PROTO-4: معرف الرسالة: 0x3، الطول: 492
IKEv2-PROTO-5: (6): يحتوي الطلب على MESS_ID 3؛ المتوقع من 3 إلى 3

2. **المعرف: 2** - يساعد المعرف في مطابقة استجابات EAP مع الطلبات. هنا القيمة 2، وهو ما يشير إلى أن هذا هو إستجابة للطلب الذي تم إرساله مسبقا من قبل ASA (المصدق).

حزمة تم فك تشفيرها فعليا:بيانات: 424 بايت
حمولة **EAP** التالية: لا شيء، محجوز: 0x0، الطول: 424
الرمز: الرد: المعرف: 2، الطول: 420
نوع: غير معروف - 254
بيانات 415 :**EAP** بايت

3. **الطول: 420** - يتضمن طول حزمة EAP الرمز ومعرف البيانات وطولها وبيانات EAP.
4. **بيانات EAP**.

يعالج ASA هذه الاستجابة. طلب العميل من المستخدم إدخال بيانات الاعتماد. تحتوي إستجابة EAP هذه على نوع "config-auth" من "auth-reply". تحتوي هذه الحزمة على بيانات الاعتماد التي أدخلها المستخدم.

الحزمة التي تم فك تشفيرها:البيانات: 492 بايت
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B _SPI=FC696330E6B94D7F (R) MSGid = 000003 CurState: R_WAIT_EAP_RESP
الحدث: EV_REV_AUTH
IKEv2-PROTO-3: (6): إيقاف المؤقت لانتظار رسالة المصادقة
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B _SPI=FC696330E6B94D7F (R) MSGid = 000003 CurState: R_WAIT_EAP_RESP
حدث: EV_REV_EAP_RESP
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B SPI=FC696330E6B94D7F (R) MSGid = 000003 CurState: R_PROC_EAP_RESP
حدث: EV_PROC_MSSP G
IKEv2-Proto-2: (6) **معالجة إستجابة EAP**
تم تلقي رسالة XML أدناه من العميل

```
<؟"xml version="1.0" encoding="UTF-8؟>
<"config-auth client="vpn" type="auth-reply">
<device-id>win</device-id>
<version who="vpn">3.0.1047</version>
<session-token></session-token>
<session-id></session-id>
<"opaque is-for="sg>
<tunnel-group>ASA-IKEV2</tunnel-group>
<config-hash>1367268141499</config-hash></opaque>
<auth>
<password>Cisco123</password>
<username>anu</username></auth>
<config-auth/>
```

IKEv2-PLAT-1: **EAP:بدء مصادقة المستخدم**
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B _SPI=FC696330E6B94D7F (R) MSGid = 000003 CurState: R_PROC_EAP_RESP
حدث: EV_NO_AP
IKEv2-PLAT-5: رد اتصال EAP:في المصادقة والتفويض والمحاسبة (AAA)

يقوم ASA بإنشاء طلب EAP ثالث في التبادل.
تحتوي حزمة EAP على:

1. **الرمز: الطلب** - يتم إرسال هذا الرمز بواسطة المصدق إلى النظير.
2. **المعرف: 3** - يساعد المعرف في مطابقة استجابات EAP مع الطلبات. هنا القيمة 3، وهو ما يشير إلى أنها الحزمة الثالثة في التبادل. تحتوي هذه الحزمة على نوع "config-auth" من "full"؛ وقد تلقى ASA ردا، وتم تبادل EAP.
3. **الطول: 4235** - يتضمن طول حزمة EAP الرمز ومعرف الهوية والطول وبيانات EAP.
4. **بيانات EAP**.

حمولة **ENCR**:
يتم فك تشفير هذه الحمولة، ويتم تحليل محتوياتها كحمولات إضافية.

ملخص شهادة الخادم التي تم إستردادها:
DACE1C274785F28BA11D64453096BAE294A3172E
EAP :IKEv2-PLAT-5:**نجاح في رد اتصال AAA**
IKEv2-PROTO-3: إستجابة مستلمة من مصدق
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MSGid = 000003 CurState: R_PROC_EAP_RESP
حدث: EV_REV_EAP AUTH
6) :IKEv2-PROTO-5): الإجراء: action_null
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MSGid = 000003 CurState: R_BLD_EAP_REQ
حدث: EV_REV_EAP_req
6) :IKEv2-PROTO-2) إرسال طلب EAP
رسالة XML المنشأة أدناه
<?xml version="1.0" encoding="UTF-8"?>
<config-auth client="vpn" **type="complete"**>
<version who="sg">9.0(2)8</version>
<session-id>32768</session-id>
<session-token>18wA0TtGmDxPKPQCJywC7fB7EWLCEgz-
ZtjYpAyXx2yJH0H3G3H8t5xpBOx3Ixag</session-token>
<auth id="success">
<message id="0" param1="" param2=""></message>
</auth>

6) :IKEv2-PROTO-3): حزمة بناء للتشفير؛ المحتويات هي:
حمولة **EAP** التالية: لا شيء، محجوز: 0x0، الطول: 4239
الرمز: الطلب: المعرف: 3، الطول: 4235
نوع: غير معروف - 254
بيانات EAP: 4230 بايت

IKEv2-PROTO-3: Tx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id: 0x3
[IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: FC696330E6B94D7F
IKEv2-PROTO-4: IKEv2 HDR ispi: 58AFF71141BA436B - RSPI:
FC696330E6B94D7F
IKEv2-PROTO-4: الحمولة التالية: ENCR، الإصدار: 2.0
IKEv2-Proto-4: نوع Exchange: IKE_AUTH، العلامات: **Responder MSG-RESPONSE**
IKEv2-PROTO-4: معرف الرسالة: 0x3، الطول: 4300
الحمولة التالية: EAP، محجوزة: 0x0، الطول: 4272
بيانات مشفرة&colon؛4268 بايت
6) :IKEv2-Proto-5): تجزئة الحزمة، تجزئة وحدة الحد الأقصى للنقل (544 :(MTU، **عدد الأجزاء**
معرف الجزء: 2
IKEv2-PLAT-4: Sent PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc69630e6b94d7f
mid=0000000030003030b
IKEv2-PLAT-4: Sent PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc69630e6b94d7f
mid=0000000030003030b
IKEv2-PLAT-4: Sent PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc69630e6b94d7f
mid=0000000030003030b
IKEv2-PLAT-4: Sent PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc69630e6b94d7f
mid=0000000030003030b
IKEv2-PLAT-4: Sent PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171

InitSPI=0x58aff71141ba436b RespSPI=0xfc69630e6b94d7f mid=0000000030003030b
IKEv2-PLAT-4: Sent PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b RespSPI=0xfc69630e6b94d7f mid=0000000030003030b
IKEv2-PLAT-4: Sent PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b RespSPI=0xfc69630e6b94d7f mid=0000000030003030b
IKEv2-PLAT-4: Sent PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b RespSPI=0xfc69630e6b94d7f mid=0000000030003030b
IKEv2-PLAT-4: Sent PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b RespSPI=0xfc69630e6b94d7f mid=0000000030003030b
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 000003 CurState: R_BLD_EAP_REQ .event: EV_START_TMR
6) :IKEv2-PROTO-3): بدء عداد الوقت لانتظار رسالة مصادقة المستخدم (120 ثانية)
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B _SPI=FC696330E6B94D7F (R) MSGid = 000003 CurState: R_WAIT_EAP_RESP
حدث: EV_NO_EVENT
****
التاريخ: 2013/04/23 م
الوقت: 16:25:07
النوع : المعلومات
المصدر:

الوصف: **ملف التعريف الحالي: AnyConnect-ikev2.xml**
تم تلقي إعدادات تكوين جلسة عمل VPN:
الحفاظ على التثبيت: ممكن
إعداد الوكيل: عدم التعديل
الخادم الوكيل: بلا
URL PAC للوكيل: لا شيء
إستثناءات الوكيل: بلا
تمكين تأمين الوكيل:
فصل إستثناء: تم تعطيل تفضيل الوصول إلى شبكة LAN المحلية
تقسيم التضمين: معطل
تقسيم DNS: معطل
حرف بدل الشبكة المحلية (LAN): تم تعطيل تفضيل الوصول إلى شبكة LAN المحلية
قواعد جدار الحماية: لا شيء
عنوان العميل: 10.2.2.1
قناع العميل: 255.0.0.0
عنوان IPv6 للعميل: غير معروف
قناع IPv6 للعميل: غير معروف
وحدة الحد الأقصى للنقل (MTU): 1406
أي كي البقاء على قيد الحياة 20 ثانية
IKE DPD: 30 ثانية
مهلة جلسة العمل: 0 ثانية
مهلة قطع الاتصال: 1800 ثانية
مهلة الخمول: 1800 ثانية
الخادم: غير معروف
مضيف MUS: غير معروف
رسالة مستخدم DAP: بلا

حالة العزل: معطل
دائما على VPN: غير معطل
مدة التأجير: 0 ثانية
المجال الافتراضي: غير معروف
الصفحة الرئيسية: غير معروف
تم تمكين قطع الاتصال لإزالة البطاقة الذكية:
إستجابة الترخيص: غير معروف
****

يرسل العميل حزمة البادئ بحمولة EAP.
تحتوي حزمة EAP على:

1. **الرمز: الاستجابة** - يتم إرسال هذا الرمز بواسطة النظير إلى المصدق إستجابة لطلب EAP.
2. **المعرف: 3** - يساعد المعرف في مطابقة استجابات EAP مع الطلبات. هنا القيمة 3، والتي تشير إلى أن هذا هو إستجابة للطلب الذي تم إرساله مسبقا من قبل ASA (المصدق). يتلقى ASA الآن حزمة الاستجابة من العميل، الذي يحتوي على نوع "config-auth" من "ack"؛ وتعترف هذه الاستجابة برسالة EAP "complete" التي تم إرسالها من قبل ASA .
3. **الطول: 173** - يتضمن طول حزمة EAP الرمز ومعرف البيانات وطولها وبيانات EAP.
4. **بيانات EAP**.

يقوم ASA بمعالجة هذه الحزمة. يعرض الأمر تم تبادل EAP بنجاح. ال ASA يتهيأون لإرسال مجموعة الأنفاق التكوين في الحزمة التالية، والتي

IKEv2-PLAT-4: **RECV PKT** [IKE_AUTH] [192.168.1.1]:25171->[10.0.1]:4500 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f=0000000 004
IKEv2-PROTO-3: Rx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id: 0x4
[IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: FC696330E6B94D7F
IKEv2-PROTO-4: IKEv2 HDR ispi: 58AFF71141BA436B - RSPI: FC696330E6B94D7F
IKEv2-PROTO-4: الحمولة التالية: ENCR، الإصدار: 2.0
IKEv2-Proto-4: **نوع Exchange: IKE_AUTH، العلامات: البادئ**
IKEv2-PROTO-4: معرف الرسالة: 0x4، الطول: 252
6) :IKEv2-PROTO-5): يحتوي الطلب على MESS_ID 4، متوقع من 4 إلى 4

حزمة تم فك تشفيرها فعليا:بيانات: 177 بايت
حمولة **EAP** التالية: لا شيء، محجوز: 0x0، الطول: 177
الرمز: الرد: المعرف: 3، الطول: 173
نوع: غير معروف - 254
بيانات 168 :**EAP** بايت

الحزمة التي تم فك تشفيرها:البيانات:252 بايت
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
_SPI=FC696330E6B94D7F (R) MSGid = 000004 CurState: R_WAIT_EAP_RESP
الحدث: EV_REV_AUTH
6) :IKEv2-PROTO-3): إيقاف المؤقت لانتظار رسالة المصادقة
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
_SPI=FC696330E6B94D7F (R) MSGid = 000004 CurState: R_WAIT_EAP_RESP
الحدث: EV_REV_EAP_RESP

تم طلبه مسبقا من قبل العميل في حمولة IDi. ال ASA يستلم حزمة الاستجابة من العميل، والذي يحتوي على نوع 'config-auth' من 'ack'. هذا الاستجابة تعترف ب EAP الرسالة 'Complete' التي تم إرسالها بواسطة ASA سابقا.

IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 000004 CurState: R_PROC_EAP_RESP حدث: EV_PROC_MSSP G
IKEv2-Proto-2: (6) **معالجة إستجابة EAP**
تم تلقي رسالة XML أدناه من العميل
<؟"xml version="1.0" encoding="UTF-8؟>
<"config-auth client="vpn" **type="ack**>
<device-id>win</device-id>
<version who="vpn">3.0.1047</version>
<config-auth/>

التكوين ذي الصلة:

```
tunnel-group ASA-IKEV2
    type remote-access
tunnel-group ASA-IKEV2
    general-attributes
 address-pool webvpn1
authorization-server-
                group
 LOCAL default-group-
                policy
 ASA-IKEV2
tunnel-group ASA-IKEV2
    webvpn-attributes
group-alias ASA-IKEV2
    enable
```

IKEv2-PLAT-3: (6) إعداد بروتوكول aggrAuthHDL على 0x2000
IKEv2-PLAT-3: (6) **tg_name set إلى: ASA-IKEV2**
IKEv2-PLAT-3: (6) **تم تعيين نوع بروتوكول إدارة الشبكة الخاصة بالتون على: RA**
IKEv2-PLAT-1: **المصادقة ناجحة:EAP**
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 000004 CurState: R_PROC_EAP_RESP حدث: EV_REV_EAP نجاح_نجاح
IKEv2-PROTO-2: (6): إرسال رسالة حالة EAP
IKEv2-PROTO-3: (6): حزمة بناء للتشفير؛ المحتويات هي:
حمولة **EAP** التالية: لا شيء، محجوز: 0x0، الطول: 8
الرمز: النجاح: المعرف: 3، الطول: 4

IKEv2-PROTO-3: Tx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id: 0x4
[IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: FC696330E6B94D7F
IKEv2-PROTO-4: IKEv2 HDR ispi: 58AFF71141BA436B - RSPI: FC696330E6B94D7F
IKEv2-PROTO-4: الحمولة التالية: ENCR، الإصدار: 2.0
IKEv2-Proto-4: نوع التبادل: IKE_AUTH، العلامات: Responder MSG-RESPONSE
IKEv2-PROTO-4: معرف الرسالة: 0x4، الطول: 76
الحمولة التالية ل ENCR: EAP، محجوزة: 0x0، الطول: 48
بيانات مشفرة&colon؛44 بايت

IKEv2-PLAT-4: **PKT المرسل [**10.0.0.1]:4500->[192.168.1.1]:25171] **IKE_AUTH]**
itSPI=0x58aff71141ba436b RespSPI=0xfc69630e6b94d7f=0000000000000b 004
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 000004 CurState: R_PROC_EAP_RESP event: EV_START_TMR.
IKEv2-PROTO-3: (6): بدء المؤقت لانتظار رسالة المصادقة (30 ثانية)
IKEv2-Proto-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 0000004 CurState: **r_WAIT_EAP_AUTH_VERIFY** حدث:_NO_EVENT

1. **الرمز: النجاح** - هذا الرمز هو مرسلة من المصدق إلى النظير بعد إكمال EAP أسلوب المصادقة. هذا تشير إلى أن النظير لديه تمت المصادقة بنجاح على مصادق.
2. **المعرف: 3** - يساعد المعرف في مطابقة استجابات EAP مع الطلبات. هنا القيمة هي 3، أي تشير إلى أن هذا رد على الطلب الذي سبق وأرسلته ASA (مصدق).

المجموعة الثالثة
من الحزم في التبادل
ناجح، وتبادل EAP
ناجحة.

3. **الطول: 4** - طول
EAP
تتضمن الحزمة الرمز،
المعرف،
الطول وبيانات EAP.

4. **بيانات EAP**.

بما أن تبادل EAP ناجح، يرسل العميل حزمة بادئ IKE_AUTH بحمولة المصادقة. يتم إنشاء حمولة المصادقة من المفتاح السري المشترك.

IKEv2-PLAT-4: Recv PKT [IKE_AUTH] [192.168.1.1]:25171->[10.0.1]:4500
InitSPI=0x58aff71141ba436b RespSPI=0xfc69630e6b94d7f
mid=0000000000000000000000b000000b0b 5
IKEv2-PROTO-3: Rx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id: 0x5
[IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: FC696330E6B94D7F
IKEv2-PROTO-4: IKEv2 HDR ispi: 58AFF71141BA436B - RSPI:
FC696330E6B94D7F
IKEv2-PROTO-4: الحمولة التالية: ENCR، الإصدار: 2.0
IKEv2-PROTO-4: نوع التبادل: IKE_AUTH، **العلامات: البادئ**
IKEv2-PROTO-4: معرف الرسالة: 0x5، الطول: 92
6) :IKEv2-PROTO-5): يحتوي الطلب على 5 MESS_ID؛ من المتوقع أن يتراوح من 5 إلى 5

حزمة تم فك تشفيرها فعليا:البيانات:28 بايت
حمولة **المصادقة** التالية: لا شيء، محجوز: 0x0، الطول: 28
طريقة المصادقة PSK، محجوزة: 0x0، محجوزة 0x0
بيانات المصادقة: 20 بايت

عند تحديد مصادقة EAP أو ضمني من قبل ملف تعريف العميل و لا يحتوي ملف التعريف على عنصر <IKEIdentity>، يرسل العميل حمولة ID_GROUP IDi مع السلسلة الثابتة *$AnyConnectClient$*. يعالج ASA هذه الرسالة.

الحزمة التي تم فك تشفيرها:البيانات: 92 بايت
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MSGid = 0000005 CurState:
R_WAIT_EAP_AUTH_VERIFY حدث: EV_RECV أوث
6) :IKEv2-PROTO-3): إيقاف المؤقت لانتظار رسالة المصادقة
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MSGid = 000005 CurState: R_VERIFY_AUTH
الحدث: EV_GET_EAP_Key
6) :IKEv2-PROTO-2): إرسال مصادقة للتحقق من النظير بعد تبادل EAP
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MSGid = 000005 CurState: R_VERIFY_AUTH
الحدث: EV_VERIFY_AUTH
6) :IKEv2-PROTO-3): **التحقق من بيانات المصادقة**
6) :IKEv2-PROTO-3): **أستخدم المفتاح المشترك مسبقا للمعرف *$AnyConnectClient$*، المفتاح len 20**
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MSGid = 000005 CurState: R_VERIFY_AUTH
الحدث: EV_GET_CONFIG_MODE
IKEv2-PLAT-3: وضع التكوين في قائمة الانتظار
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F (R) MSGid = 000005 CurState: R_VERIFY_AUTH
الحدث: EV_NO_EVENT
Ev2-PLAT-3: PSH: client=AnyConnect client-version=3.0.1047 client-os=Windows
=client-os-version
IKEv2-PLAT-3: اكتمل الرد على وضع التكوين

التكوين ذي الصلة:

```
crypto dynamic-map
dynmap 1000
set ikev2 ipsec-
proposal 3des
crypto map crymap
10000
ipsec-isakmp dynamic
dynmap
crypto map crymap
interface
outside
```

IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 000005 CurState: R_VERIFY_AUTH الحدث: EV_OK_GET_CONFIG
6) :IKEv2-PROTO-3): امتلاك بيانات وضع التكوين للإرسال
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 000005 CurState: R_VERIFY_AUTH الحدث: EV_CHK4_IC
6) :IKEv2-PROTO-3) معالجة جهة الاتصال الأولية
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 000005 CurState: R_VERIFY_AUTH الحدث: EV_CHK_REDIRECT
6) :IKEv2-PROTO-5): تم بالفعل إعادة توجيه التحقق لجلسة العمل هذه، وتجاوزها
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 000005 CurState: R_VERIFY_AUTH الحدث: EV_PROC_SA_TS
6) :IKEv2-PROTO-2): **معالجة رسالة المصادقة**
IKEv2-PLAT-1: **خريطة التشفير: خريطة خريطة المنطقة 1000. محدد معدل باستخدام IP المع**
IKEv2-PLAT-3: **خريطة التشفير: مطابقة في خريطة ديناميكية سلسلة 1000**
IKEv2-PLAT-3: تعطيل PFS لاتصال RA
6) :IKEv2-PROTO-3):
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 000005 CurState: R_VERIFY_AUTH الحدث: EV_NO_EVENT
IKEv2-PLAT-2: تم تلقي رد اتصال SPI ل SPI الخاص ب 0x30b848a4 SPI، خطأ FALSE
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 000005 CurState: R_VERIFY_AUTH الحدث: EV_OK_RED_IPSEC RESP
6) :IKEv2-PROTO-2): **معالجة رسالة المصادقة**
IKEv2-Proto-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 000005 CurState: **R_BLD_AUTH** الحدث: EV_MY_AUTH الأسلوب
6) :IKEv2-PROTO-3): **احصل على طريقة المصادقة الخاصة بي**
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 000005 CurState: R_BLD_AUTH الحدث: EV_GET_PRESHR_KEY
6) :IKEv2-PROTO-3): **الحصول على مفتاح النظير المضغوط ل *$AnyConnectClient$***
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 000005 CurState: R_BLD_AUTH الحدث: EV_GEN_AUTH
6) :IKEv2-PROTO-3): **إنشاء بيانات المصادقة الخاصة بي**
6) :IKEv2-PROTO-3): **إستخدام المفتاح المشترك مسبقا لمعرف hostname=ASA-IKEV2، مفتاح len 20**
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 000005 CurState: R_BLD_AUTH الحدث: EV_CHK4_SIGN
6) :IKEv2-PROTO-3): احصل على طريقة المصادقة الخاصة بي
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 000005 CurState: R_BLD_AUTH الحدث: EV_OK_AUTH_AUGEN
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 000005 CurState: R_BLD_EAP_AUTH_VERIFY حدث: EV_GEN أوث
6) :IKEv2-PROTO-3): إنشاء بيانات المصادقة الخاصة بي

يقوم ASA بإنشاء رسالة إستجابة IKE_AUTH مع حمولات SA و TSi و TSr. تحتوي حزمة المستجيب IKE_AUTH على:

1. **رأس** - ISAKMP SPI/الإصدار/العلاما ت.
2. **حمولة المصادقة** - باستخدام طريقة المصادقة المختارة.
3. **cfg** - CFG_REQUEST/ CFG_REPLY يسمح لنقطة نهاية IKE بطلب المعلومات من النظير. إذا لم يكن طول إحدى السمات في حمولة تكوين CFG_REQUEST صفرا، فسيتم اعتبارها اقتراحا لتلك

السمة. قد ترجع حمولة تكوين CFG_REPLY تلك القيمة أو قيمة جديدة. كما يمكن أن يضيف سمات جديدة ولا يتضمن بعض السمات المطلوبة. يتجاهل أصحاب الطلبات السمات المرتجعة التي لا يتعرفون عليها. يرد ASA على العميل باستخدام علامات تكوين النفق في حزمة CFG_REPLY.

4. **SAr2** - يقوم SAr2 ببدء SA، والذي يشبه مجموعة تحويل المرحلة 2 في IKEv1.
5. **TSi** و**TSr** - يحتوي محدد حركة مرور البادئ والمستجيب، على التوالي، على عنوان المصدر والوجهة للبادئ والمستجيب لإعادة توجيه حركة المرور المشفرة واستقبالها. يحدد نطاق العناوين أن كل حركة المرور إلى ذلك النطاق ومنه يتم إنشاء قنوات لها. إذا كان العرض مقبولا للمستجيب، فإنه يرسل حمولات TS متطابقة.

حمولة **ENCR**: يتم فك تشفير هذه الحمولة، ويتم تحليل محتوياتها كحمولات إضافية.

6) :IKEv2-PROTO-3): إستخدام المفتاح المشترك مسبقا لمعرف hostname=ASA-IKEV2، مفتاح len 20
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 000005 CurState: R_BLD_EAP_AUTH_VERIFY حدث: EV_SEND أوث
6) :IKEv2-PROTO-2): **إرسال المصادقة للتحقق من النظير بعد تبادل EAP**
IKEv2-PROTO-3: مقترح 1 :ESP، حجم 4 :SPI (تفاوض IPSec)، عدد عمليات التحويل: 3
إيه إس إس-سي إتش 96
IKEv2-PROTO-5: إنشاء Notify Payload: ESP_TFC_NO_SUPPORTIKEv2-PROTO-5
إنشاء 6) :Notify Payload: NON_FIRST_FRASIKEv2-PROTO-3): إنشاء حزمة للتشفير؛ المحتويات هي:
حمولة **المصادقة** التالية: CFG، محجوزة: 0x0، الطول: 28
طريقة المصادقة PSK، محجوزة: 0x0، محجوزة 0x0
بيانات المصادقة والقولون، 20 بايت
الحمولة التالية **ل** SA :**CFG**، محجوزة: 0x0، الطول: 4196
نوع **CFG_REPLY** :cfg، محجوز: 0x0، محجوز: 0x0

نوع الجهاز: عنوان IP4 داخلي، الطول: 4

01 01 01 01
النوع Attrib: قناع الشبكة الداخلي ل IP4، الطول: 4

00 00 00 00
نوع Attrib: انتهاء صلاحية العنوان الداخلي، الطول: 4

00 00 00 00
نوع التطبيق: إصدار التطبيق، الطول: 16

41 53 41 20 31 30 30 31 00 31 36 31 29 36 28 37 2e
نوع attrib: غير معروف - 28704، الطول: 4

00 00 00 00
نوع attrib: غير معروف - 28705، الطول: 4

00 00 07 08
نوع attrib: غير معروف - 28706، الطول: 4

00 00 07 08
نوع attrib: غير معروف - 28707، الطول: 1

01
نوع attrib: غير معروف - 28709، الطول: 4

00 000 1e
نوع attrib: غير معروف - 28710، الطول: 4

00 00 00 14
نوع attrib: غير معروف - 28684، الطول: 1

01
نوع attrib: غير معروف - 28711، الطول: 2

057 اس
نوع attrib: غير معروف - 28679، الطول: 1

00
نوع attrib: غير معروف - 28683، الطول: 4

80 مليا 001
نوع attrib: غير معروف - 28725، الطول: 1

00
نوع attrib: غير معروف - 28726، الطول: 1

00
نوع attrib: غير معروف - 28727، الطول: 4056

3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31
2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54
3f 3e 3c 63 6f 6e 66 69 67 2d 61 75 22 38 22 20 ثنائي الأبعاد 46
6c 69 65 6e 74 3d 22 76 6 e 22 20 63 20 68 74
6f 6d 70 6c 65 74 65 22 3e 63 22 65 74 65 6c 70 عمق 22 79 74
3c 76 65 72 73 69 6f 6e 20 77 68 6f 3d 22 73 67
3e 31 30 30 2e 37 28 36 29 31 36 3c 2f 76 22
6f 6e 3c 73 65 73 69 6f 6e 2d 69 73 72 65
3e 38 31 39 32 3c 2f 73 65 73 69 6f 6e 64 69
<snip>
6F 66 69 6c 65 2d 6d 61 6e 69 665 73 74 3e 72
3c 2f 63 6f 6e 66 69 67 3e 3c 2f 63 6e 66 69
67 ديسيبل 61 75 74 68 00 3e
نوع attrib: غير معروف - 28729، الطول: 1

00
حمولة **SA** التالية: TSi، محجوزة: 0x0، الطول: 44
IKEv2-PROTO-4: المقترح الأخير: 0x0، محجوز: 0x0، الطول: 40
المقترح: 1، معرف البروتوكول: ESP، حجم SPI: 4، #trans: 3
IKEv2-PROTO-4: آخر تحويل: 0x3، محجوز: 0x0: الطول: 12
النوع: 1، محجوز: 0x0، المعرف: AES-CBC
IKEv2-PROTO-4: آخر تحويل: 0x3، محجوز: 0x0: الطول: 8
النوع: 3، محجوز: 0x0، المعرف: SHA96
IKEv2-PROTO-4: آخر تحويل: 0x0، محجوز: 0x0: الطول: 8
النوع: 5، محجوز: 0x0، المعرف:

الحمولة التالية ل TSr :**TSi**، محجوزة: 0x0، الطول: 24
num of TSs: 1، محجوز 0x0، محجوز 0x0
نوع TS: TS_IPv4_ADDR_RANGE، معرف الإصدار: 0، الطول: 16
منفذ البدء: 0 ومنفذ النهاية: 65535
بداية العنوان: 10.2.2.1، نهاية العنوان: 10.2.2.1
الحمولة التالية ل NOTIFY :**TSr**، محجوز: 0x0، الطول: 24
num of TSs: 1، محجوز 0x0، محجوز 0x0
نوع TS: TS_IPv4_ADDR_RANGE، معرف الإصدار: 0، الطول: 16
منفذ البدء: 0 ومنفذ النهاية: 65535
بداية العنوان: 0.0.0.0، نهاية العنوان: 255.255.255.255
IKEv2-PROTO-3: Tx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id: 0x5
[IKEv2-PROTO-3: HDR[i:58AFF71141BA436B - r: FC696330E6B94D7F

IKEv2-PROTO-4: IKEv2 HDR ispi: 58AFF71141BA436B - RSPI: FC696330E6B94D7F
IKEv2-PROTO-4: الحمولة التالية: ENCR، الإصدار: 2.0
IKEv2-Proto-4: **نوع Exchange: IKE_AUTH، العلامات: المستجيب msg-response**
IKEv2-PROTO-4: معرف الرسالة: 0x5، الطول: 4396
حمولة **ENCR** التالية: المصادقة، محجوزة: 0x0، الطول: 4368
بيانات مشفرة&4364 ،colon بايت

يرسل ASA رسالة إستجابة ike_AUTH هذه، والتي يتم تجزئتها إلى تسع حزم. اكتمل تبادل IKE_AUTH.

6) :IKEv2-Proto-5): تجزئة الحزمة، تجزئة وحدة الحد الأقصى للنقل (MTU): 544، **عدد الأجزاء**
معرف الجزء: 3
IKEv2-PLAT-4: Sent PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b RespSPI=0xfc69630e6b94d7f mid=0000000000500005
IKEv2-PLAT-4: Sent PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b RespSPI=0xfc69630e6b94d7f mid=0000000000500005
IKEv2-PLAT-4: Sent PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b RespSPI=0xfc69630e6b94d7f mid=0000000000500005
IKEv2-PLAT-4: Sent PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b RespSPI=0xfc69630e6b94d7f mid=0000000000500005
IKEv2-PLAT-4: Sent PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b RespSPI=0xfc69630e6b94d7f mid=0000000000500005
IKEv2-PLAT-4: Sent PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b RespSPI=0xfc69630e6b94d7f mid=0000000000500005
IKEv2-PLAT-4: Sent PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b RespSPI=0xfc69630e6b94d7f mid=0000000000500005
IKEv2-PLAT-4: Sent PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b RespSPI=0xfc69630e6b94d7f mid=0000000000500005
IKEv2-PLAT-4: Sent PKT [IKE_AUTH] [10.0.0.1]:4500->[192.168.1.1]:25171 InitSPI=0x58aff71141ba436b RespSPI=0xfc69630e6b94d7f mid=0000000000500005
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 000005 CurState: AUTH_DID حدث: EV_OK
6) :IKEv2-PROTO-5): الإجراء: action_null
IKEv2-Proto-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 000005 CurState: **AUTH_DONE**: حدث: EV_PKI_SSH_SSH إغلاق
****
التاريخ: 2013/04/23 م
الوقت: 16:25:07
النوع : المعلومات
المصدر:

الوصف: الوظيفة: ikev2_log
الملف: .\ikev2_anyconnect_osal.cpp
السطر: 2730
تم إنشاء اتصال IPsec.

****
التاريخ: 2013/04/23 م
الوقت: 16:25:07
النوع : المعلومات
المصدر:

الوصف: تسجيل جلسة عمل IPsec:
التشفير: AES-CBC
PRF: SHA1
HMAC: SHA96
طريقة المصادقة المحلية: PSK
طريقة المصادقة عن بعد: PSK
معرف التسلسل: 0
حجم المفتاح: 192
مجموعة DH: 1
الوقت الرئيسي: 4294967 ثانية
العنوان المحلي: 192.168.1.1
العنوان البعيد: 10.0.0.1
المنفذ المحلي: 4500
المنفذ البعيد: 4500
معرف جلسة العمل: 1
****
التاريخ: 2013/04/23 م
الوقت: 16:25:07
النوع : المعلومات
المصدر: أكفبنوي

الوصف: **ملف التعريف الذي تم تكوينه على البوابة الآمنة هو: AnyConnect-ikev2.xml**
****
التاريخ: 2013/04/23 م
الوقت: 16:25:07
النوع : المعلومات
المصدر: أكفبنوي

الوصف: تم إرسال معلومات نوع الرسالة إلى المستخدم:
يتم الآن إنشاء جلسة عمل VPN...
****
—انتهاء تبادل IKE_AUTH—
****
التاريخ: 2013/04/23 م
الوقت: 16:25:07
النوع : المعلومات
المصدر: AcvpnDownloadLoader

الوصف: الوظيفة: ProfileMgr::loadProfile
الملف: ..\API\ProfileMgr.cpp
السطر: 148
ملفات التعريف المحملة:
C:\Documents and Settings\AllUsers\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\Anyconnect-ikev2.xml
****
****
التاريخ: 2013/04/23 م

الوقت: 16:25:07
النوع : المعلومات
المصدر: AcvpnDownloadLoader

الوصف: إعدادات التفضيل الحالية:
ServiceDisable: خطأ
CertificateStoreOverride: خطأ
مخزن الشهادات: الكل
ShowPreConnectMessage: خطأ
AutoConnectOnStart: خطأ
MinimizeOnConnect: صحيح
LocalLanAccess: خطأ
إعادة الاتصال التلقائي: صواب
AutoReconnectBehavior: DisconnectOnSuspend
UseStartBeforeLogon: false
التحديث التلقائي: صحيح
RSASecurIdiIntegration: تلقائي
WindowsLogonEnforcement: SingleLocalLogon
WindowsVPNEestment: LocalUsersOnly
إعدادات الوكيل: أصلية
AllowLocalProxyConnections: true
PPPExclusion: تعطيل
PPPExclusionServerIP:
AutomaticVPNPolicy: false
TrustedNetworkPolicy: قطع الاتصال
NetworkPolicy غير موثوق: الاتصال
TrustedDNSDomans:
TrustedDnssErver:
AlwaysOn: خطأ
ConnectFailurePolicy: مغلق
AllowCaptivePortalRemediation: خطأ
CaptivePortalRemediationTimeout: 5
ApplyLastVPNLocalResourceRules: false
AllowVPNDisconnect: صحيح
EnableScripting: خطأ
TerminateScriptOnNextEvent: خطأ
EnablePostSBLOnConnectScript: صحيح
AutomaticCertSelection: صحيح
RetainVpnOnLogoff: خطأ
UserEnforcement: SameUserOnly
EnableAutomaticServerSelection: خطأ
AutoServerSelection: 20 تحسين
AutoServerSelectionSuspendTime: 4
مهلة المصادقة: 12
SafeWordSofTokenIntegration: خطأ
AllowIPsecOverSSL: خطأ
ClearSmartcardPin: صحيح
****

التاريخ: 2013/04/23 م
الوقت: 16:25:07
النوع : المعلومات
المصدر: أكفبنوي

الوصف: تم إرسال معلومات نوع الرسالة إلى المستخدم:
إنشاء شبكة خاصة ظاهرية (VPN) - نظام الفحص...
****

التاريخ: 2013/04/23 م
الوقت: 16:25:07
النوع : المعلومات
المصدر: أكفبنوي

الوصف: تم إرسال معلومات نوع الرسالة إلى المستخدم:
إنشاء VPN - تنشيط محول VPN...
****

التاريخ: 2013/04/23 م
الوقت: 16:25:07
النوع : المعلومات
المصدر:

الوصف: الوظيفة: CVirtualAdapter::DoRegistryRepair
الملف: .\WindowsVirtualAdapter.cpp
السطر: 1869
تم العثور على مفتاح التحكم في :VA
SYSTEM\CurrentControlSet\ENUM\ROOT\NET\0000\Control
****

التاريخ: 2013/04/23 م
الوقت: 16:25:07
النوع : المعلومات
المصدر:

الوصف: **تم اكتشاف واجهة شبكة جديدة.**
****

التاريخ: 2013/04/23 م
الوقت: 16:25:07
النوع : المعلومات
المصدر:

الوصف: الوظيفة: CRouteMgr::LogInterfaces
الملف: .\RouteMgr.cpp
السطر: 2076
تم إستدعاء الدالة: LogInterfaces
رمز الإرجاع: 0 (0x0000000)
الوصف: قائمة واجهة عنوان IP:
10.2.2.1
192.168.1.1
****

التاريخ: 2013/04/23 م
الوقت: 16:25:08
النوع : المعلومات
المصدر:

الوصف: تكوين المضيف:
العنوان العام: 192.168.1.1
القناع العام: 255.255.255.0
العنوان الخاص: 10.2.2.1
القناع الخاص: 255.0.0.0

عنوان IPv6 الخاص: غير متوفر
قناع IPv6 الخاص: غير متوفر
النظراء عن بعد: 10.0.0.1 (منفذ TCP رقم 443، منفذ UDP رقم 500)، 10.0.0.1 (منفذ UDP رقم 4500)
الشبكات الخاصة: لا شيء
الشبكات العامة: لا شيء
وضع النفق: نعم
****

يتم إدخال الاتصال في قاعدة بيانات اقتران الأمان (SA)، ويتم تسجيل الحالة. كما يقوم ASA بتنفيذ بعض عمليات التحقق مثل حالات بطاقة الوصول المشترك (CAC)، ووجود حالات SA المكررة، وتعيين قيم مثل اكتشاف النظير الميت (DPD) وما إلى ذلك.

IKEv2-Proto-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 000005 CurState: AUTH_DID حدث: **EV_INSERT_IKE**
IKEv2-PROTO-2: (6): **تم إنشاء SA؛ إدراج SA في قاعدة البيانات**
IKEv2-PLAT-3:
حالة الاتصال: النظير الفائق: 192.168.1.1:25171، *$AnyConnectClient :*$phase1_id*
IKEv2-Proto-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 000005 CurState: AUTH_DONE حدث: **EV_REGISTER_SESSION_SESSION**
IKEv2-PLAT-3: (6) **اسم المستخدم معين إلى: ANU**
IKEv2-PLAT-3:
حالة الاتصال:... النظير **المسجل**: 192.168.1.1:25171، **$AnyConnectClient* :*$phase1_id***
IKEv2-PROTO-3: (6): تهيئة DPD، تم تكوينها لمدة 10 ثوان
IKEv2-PLAT-3: (6) قاعدة معلومات الإدارة_index مضبوطة على: 4501
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 000005 CurState: AUTH_DONE حدث: EV_GEN_LOAD_IPSEC
IKEv2-PROTO-3: (6): تحميل المواد الأساسية ل IPsec
IKEv2-PLAT-3: خريطة التشفير: مطابقة في الخريطة الديناميكية الرقم 1000
IKEv2-PLAT-3: (6) **الحد الأقصى لوقت DPD سيكون: 30**
IKEv2-PLAT-3: (6) **الحد الأقصى لوقت DPD سيكون: 30**
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 000005 CurState: AUTH_DONE الحدث EV_START_ACCT
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 000005 CurState: AUTH_DID حدث: EV_CHECK_DUPE
IKEv2-Proto-3: (6): **التحقق من تكرار SA**
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 000005 CurState: AUTH_DONE حدث: EV_CHK4_ROLE
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 000005 CurState: Ready Event: EV_R_UPDATE_CAC_STATS
IKEv2-PLAT-5: تم تنشيط طلب IKEV2 SA الجديد
IKEv2-PLAT-5: عدد حالات تناقص التفاوض المقبل
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 0000005 CurState: حدث جاهز: R_OK/
IKEv2-PROTO-3: (6): بدء الموقت لحذف سياق التفاوض
IKEv2-PROTO-5: (6): SM Trace-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MSGid = 0000005 CurState: Ready Event: EV_NO_EVENT
IKEv2-PLAT-2: تم إستلام PFKEY إضافة sa ل SPI 0x77EE5348، خطأ FALSE
IKEv2-PLAT-2: تم تلقي تحديث SA ل PFKEY ل SPI 0x30b848a4، خطأ FALSE
****

التاريخ: 2013/04/23 م
الوقت: 16:25:08
النوع : المعلومات
المصدر:

الوصف: **تم إنشاء اتصال VPN ويمكن الآن تمرير البيانات.**
****

التاريخ: 2013/04/23 م
الوقت: 16:25:08
النوع : المعلومات
المصدر: أكفبنوي

الوصف: تم إرسال معلومات نوع الرسالة إلى المستخدم:
إنشاء شبكة VPN - تكوين النظام...
****

التاريخ: 2013/04/23 م
الوقت: 16:25:08
النوع : المعلومات
المصدر: أكفبنوي

الوصف: تم إرسال معلومات نوع الرسالة إلى المستخدم:
يتم الآن إنشاء شبكة VPN...
****

التاريخ: 2013/04/23 م
الوقت: 16:25:37
النوع : المعلومات
المصدر:

الملف: .\IPsecProtocol.cpp
السطر: 945
تم إنشاء نفق IPsec
****

التحقق من النفق

AnyConnect

عينة إنتاج من **العرض vpn-sessiondb تفصيل** anyConnect أمر:

```
Session Type: AnyConnect Detailed

            Username     : Anu                    Index        : 2
  Assigned IP  : 10.2.2.1               Public IP    : 192.168.1.1
              Protocol     : IKEv2 IPsecOverNatT AnyConnect-Parent
                                    License      : AnyConnect Premium
Encryption   : AES192 AES256          Hashing      : none SHA1 SHA1
         Bytes Tx     : 0                      Bytes Rx     : 11192
           Pkts Tx      : 0                      Pkts Rx      : 171
             Pkts Tx Drop : 0                      Pkts Rx Drop : 0
      Group Policy : ASA-IKEV2             Tunnel Group : ASA-IKEV2
```

```
                                        Login Time   : 22:06:24 UTC Mon Apr 22 2013
                                            Duration     : 0h:02m:26s
                                            Inactivity   : 0h:00m:00s
                                               NAC Result   : Unknown
                          VLAN Mapping : N/A                    VLAN         : none

                                                     IKEv2 Tunnels: 1
                                                IPsecOverNatT Tunnels: 1
                                              AnyConnect-Parent Tunnels: 1

                                                       :AnyConnect-Parent
                                                  Tunnel ID    : 2.1
                                               Public IP    : 192.168.1.1
                  Encryption   : none                  Auth Mode    : userPassword
                    Idle Time Out: 30 Minutes            Idle TO Left : 27 Minutes
                                               Client Type  : AnyConnect
                                                   Client Ver   : 3.0.1047
                                                                  :IKEv2
                                                  Tunnel ID    : 2.2
                          UDP Src Port : 25171                UDP Dst Port : 4500
                                              Rem Auth Mode: userPassword
                                             Loc Auth Mode: rsaCertificate
                          Encryption   : AES192                Hashing      : SHA1
                 Rekey Int (T): 86400 Seconds         Rekey Left(T): 86254 Seconds
                             PRF          : SHA1                  D/H Group    : 1
                                                               :  Filter Name
                                                 Client OS    : Windows
                                                               :IPsecOverNatT
                                                  Tunnel ID    : 2.3
                                        Local Addr   : 0.0.0.0/0.0.0.0/0/0
                                    Remote Addr  : 10.2.2.1/255.255.255.255/0/0
                          Encryption   : AES256                Hashing      : SHA1
                                                 Encapsulation: Tunnel
                    Rekey Int (T): 28800 Seconds         Rekey Left(T): 28654 Seconds
                  Rekey Int (D): 4608000 K-Bytes       Rekey Left(D): 4607990 K-Bytes
                       Idle Time Out: 30 Minutes            Idle TO Left : 29 Minutes
                            Bytes Tx     : 0                    Bytes Rx     : 11192
                              Pkts Tx      : 0                    Pkts Rx      : 171
                                                                    :NAC
                         Reval Int (T): 0 Seconds             Reval Left(T): 0 Seconds
                       SQ Int (T)   : 0 Seconds             EoU Age(T)   : 146 Seconds
                                   :Hold Left (T): 0 Seconds             Posture Token
                                                                : Redirect URL
```

ISAKMP

نموذج الإخراج من الأمر **show crypto ikev2 sa**:

```
                                        ASA-IKEV2#  show crypto ikev2 sa

                                                       :IKEv2 SAs

                                    Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1

            Tunnel-id                Local                Remote     Status         Role
             READY    RESPONDER      192.168.1.1/25171         10.0.0.1/4500    55182129
Encr: AES-CBC, keysize: 192, Hash: SHA96, DH Grp:1, Auth sign: RSA, Auth verify: EAP
                                                  Life/Active Time: 86400/112 sec
                                Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
                                     remote selector 10.2.2.1/0 - 10.2.2.1/65535
                                          ESP spi in/out: 0x30b848a4/0x77ee5348
```

نموذج الإخراج من الأمر **show crypto ikev2 sa detail** هو:

```
ASA-IKEV2# show crypto ikev2 sa detail

:IKEv2 SAs

Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id                Local                Remote     Status         Role
READY    RESPONDER      192.168.1.1/25171        10.0.0.1/4500    55182129
Encr: AES-CBC, keysize: 192, Hash: SHA96, DH Grp:1, Auth sign: RSA, Auth verify: EAP
Life/Active Time: 86400/98 sec
Session-id: 2
Status Description: Negotiation done
Local spi: FC696330E6B94D7F       Remote spi: 58AFF71141BA436B
Local id: hostname=ASA-IKEV2
*$Remote id: *$AnyConnectClient
Local req mess id: 0             Remote req mess id: 9
Local next mess id: 0           Remote next mess id: 9
Local req queued: 0              Remote req queued: 9      Local window:
1                   Remote window: 1
DPD configured for 10 seconds, retry 2
NAT-T is detected  outside
Assigned host addr: 10.2.2.1
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
remote selector 10.2.2.1/0 - 10.2.2.1/65535
ESP spi in/out: 0x30b848a4/0x77ee5348
AH spi in/out: 0x0/0x0
CPI in/out: 0x0/0x0
Encr: AES-CBC, keysize: 256, esp_hmac: SHA96
ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

IPsec

نموذج الإخراج من الأمر **show crypto ipSec sa** هو:

```
ASA-IKEV2# show crypto ipsec sa
interface: outside
Crypto map tag: dynmap, seq num: 1000, local addr: 10.0.0.1

(local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0
(remote ident (addr/mask/prot/port): (10.2.2.1/255.255.255.255/0/0
current_peer: 192.168.1.1, username: Anu
dynamic allocated peer ip: 10.2.2.1

pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0#
pkts decaps: 163, #pkts decrypt: 108, #pkts verify: 108#
pkts compressed: 0, #pkts decompressed: 0#
pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0#
pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0#
PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0#
send errors: 0, #recv errors: 55#

local crypto endpt.: 10.0.0.1/4500, remote crypto endpt.: 192.168.1.1/25171
path mtu 1488, ipsec overhead 82, media mtu 1500
current outbound spi: 77EE5348
current inbound spi : 30B848A4

:inbound esp sas
```

```
                                (spi: 0x30B848A4 (817383588
        transform: esp-aes-256 esp-sha-hmac no compression
            { ,in use settings ={RA, Tunnel,  NAT-T-Encaps
                slot: 0, conn_id: 8192, crypto-map: dynmap
            sa timing: remaining key lifetime (sec): 28685
                                        IV size: 16 bytes
                                replay detection support: Y
                                        :Anti replay bitmap
                                    0xFFAD6BED 0x7ABFD5BF
                                                :outbound esp sas
                                 (spi: 0x77EE5348 (2012107592
        transform: esp-aes-256 esp-sha-hmac no compression
            { ,in use settings ={RA, Tunnel,  NAT-T-Encaps
                slot: 0, conn_id: 8192, crypto-map: dynmap
            sa timing: remaining key lifetime (sec): 28685
                                        IV size: 16 bytes
                                replay detection support: Y
                                        :Anti replay bitmap
                                    0x00000000 0x00000001
```

معلومات ذات صلة

- المعيار RFC 4306، بروتوكول تبادل مفتاح الإنترنت (IKEv2)
- المعيار RFC 3748، بروتوكول المصادقة المتوسع (EAP)
- المعيار RFC 5996، بروتوكول تبادل مفتاح الإنترنت الإصدار 2 (IKEv2)
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).