ASA ءاطخأ فاشكتسأ لوح ةينف ةظالم IPsec و IKE Debugs (الوضوع العدواني IKEv1) واحالصإو

المحتويات

المقدمة

يصف هذا المستند تصحيح الأخطاء على جهاز الأمان القابل للتكيف (ASA) من Cisco عند إستخدام كل من الوضع العدواني والمفتاح المشترك مسبقا (PSK). تتم أيضا مناقشة ترجمة بعض سطور تصحيح الأخطاء إلى التكوين. توصي Cisco بأن تكون لديك معرفة أساسية ب IPsec وتبادل مفتاح الإنترنت (IKE).

لا يناقش هذا المستند حركة مرور البيانات بعد إنشاء النفق.

مسألة أساسية

تكون عمليات تصحيح أخطاء IKE و IPsec مشفرة في بعض الأحيان، ولكن يمكنك إستخدامها من أجل فهم المشاكل المتعلقة بإنشاء نفق VPN ل IPsec.

سيناريو

عادة ما يتم إستخدام الوضع القوي في حالة وجود شبكة VPN سهلة (EzVPN) مع برنامج (عميل Cisco VPN) وعملاء الأجهزة (جهاز الأمان القابل للتكيف Cisco ASA 5505 أو Cisco IOS® موجهات البرامج)، ولكن فقط عند إستخدام مفتاح مشترك مسبقا. على عكس الوضع الرئيسي، يتكون الوضع المتميز من ثلاث رسائل.

يأتي تصحيح الأخطاء من ASA الذي يشغل الإصدار 8.3.2 من البرنامج ويعمل كخادم EzVPN. عميل EzVPN هو عميل برنامج.

أوامر debug المستخدمة

هذه هي أوامر تصحيح الأخطاء المستخدمة في هذا المستند:

```
debug crypto isakmp 127
debug crypto ipsec 127
```

تكوين ASA

يقصد أن يكون تكوين ASA في هذا المثال أساسيا بشكل صارم؛ ولا يتم إستخدام أية خوادم خارجية.

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.48.67.14 255.255.254.0

crypto ipsec transform-set TRA esp-aes esp-sha-hmac

crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000

crypto dynamic-map DYN 10 set transform-set TRA
crypto dynamic-map DYN 10 set reverse-route

crypto map MAP 65000 ipsec-isakmp dynamic DYN
crypto map MAP interface outside
crypto isakmp enable outside

crypto isakmp policy 10
 authentication pre-share
 encryption aes
 hash sha
 group 2
 lifetime 86400

username cisco password  cisco
username cisco attributes
vpn-framed-ip-address 192.168.1.100 255.255.255.0

tunnel-group EZ type remote-access
tunnel-group EZ general-attributes
 default-group-policy EZ
tunnel-group EZ ipsec-attributes
 ***** pre-shared-key

group-policy EZ internal
group-policy EZ attributes
 password-storage enable
 dns-server value 192.168.1.99
 vpn-tunnel-protocol ikev1
 split-tunnel-policy tunnelall
 split-tunnel-network-list value split
default-domain value jyoungta-labdomain.cisco.com
```

تصحيح الأخطاء

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

وصف رسالة الخادم	تصحيح الأخطاء	وصف رسالة العميل
	49711:28:30.28908/24/12Sev=info/6IKE/0x630003b محاولة إنشاء اتصال مع 64.102.156.88. 49811:28:30.29708/24/12sev=debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D5619780D7BE3E5 :R_Cookie=00000000000CurState AM_INITIALEvent: EV_INITIATOR 49911:28:30.29708/24/12Sev=info/4IKE/0x6300001 بدء تفاوض المرحلة الأولى من IKE 50011:28:30.29708/24/12sev=debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D5619780D7BE3E5 :R_Cookie=00000000000CurState AM_SND_MSG1event: EV_GEN_DHKEY 5011:28:30.30408/24/12Sev=debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D5619780D7BE3E5 :R_Cookie=00000000000CurState AM_SND_MSG1event: EV_BLD_MSG 50211:28:30.30408/24/12sev=debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D5619780D7BE3E5 :R_Cookie=00000000000CurState .AM_SND_MSG1event: EV_START_RETRY_TMR 50311:28:30.30408/24/12sev=debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D5619780D7BE3E5 :R_Cookie=00000000000CurState AM_SND_MSG1event: EV_SND_MSG	يبدأ الوضع العدائي. التركيب AM1. وتتضمن هذه العملية ما يلي: - ISAKMP HDR. - جهاز الأمان (SA) الذي يحتوي على جميع حمولات التحويل والمقترحات التي يدعمها العميل - حمولة تبادل المفاتيح - معرف بادئ المرحلة 1 - Nonce
	50411:28:30.30408/24/12Sev=info/4IKE/0x6300013 إرسال >>> ISAKMP OAK AG (SA، KE، NON، ID(Xauth)، ((VID(DPD)، VID(Frag)، VID(NAT-T)، VID(Unity إلى 64.102.156.88	إرسال AM1.
	<========== رسالة عدوانية 1 (AM1) ==========	
إستلام AM1 من العميل.	أغسطس 24 11:31:03 [IKEv1]IP = IKE_Decode، 64.102.156.87 استلم رسالة (msgid=0) مع الحمولات: + HDR + SA (1) (KE (4) + NONCE (10) + ID (5) + ID (13 + المورد (13) + المورد (13) + المورد (13) + المورد (13) + لا شيء (0) + الطول الإجمالي 9 : 8	50611:28:30.3 308/24/12Sev =debug/7IKE/0 x6300076 NAV Trace- >SA:I_Cookie= D56197780D7 BE3E5 R_Cookie=000 0000000000C :urState AM_WAIT_MS G2Event: EV_NO_EVEN T	انتظار إستجابة الخادم.
معالجة AM1. مقارنة الاقتراحات	24 أغسطس 11:31:03 [تصحيح أخطاء = IKEv1]IP 64.102.156.87، معالجة حمولة SA 24 أغسطس 11:31:03 [تصحيح أخطاء = IKEv1]IP	

والتحويلات المستلمة مع تلك التي تم تكوينها بالفعل للتطابقات.
التكوين ذي الصلة:
تم تمكين ISAKMP على الواجهة، وتم تعريف سياسة واحدة على الأقل تطابق ما أرسله العميل:
`crypto isakmp enable outside`
`crypto isakmp policy 10`
`authentication pre share`
`encryption aes`
`hash sha`
`group 2`
`lifetime 86400`
مجموعة النفق المطابقة لاسم الهوية الموجود:
`tunnel-group EZ type remote-access`
`tunnel-group EZ general-attributes`
`default-group-policy EZ`
`tunnel-group -EZ ipsec attributes`
`pre-shared-key cisco`
	64.102.156.87، معالجة حمولة الوصلة
	24 أغسطس 11:31:03 [تصحيح أخطاء = IKEv1]IP
	64.102.156.87، معالجة حمولة ISA_KE
	24 أغسطس 11:31:03 [تصحيح أخطاء = IKEv1]IP
	64.102.156.87، معالجة الحمولة مرة واحدة
	24 أغسطس 11:31:03 [تصحيح أخطاء = IKEv1]IP
	64.102.156.87، حمولة معرف المعالجة
	24 أغسطس 11:31:03 [تصحيح أخطاء = IKEv1]IP
	64.102.156.87، معالجة حمولة VID
	24 أغسطس 11:31:03 [تصحيح أخطاء = IKEv1]IP
	64.102.156.87، تم تلقي الإصدار السادس من XAUTH
	24 أغسطس 11:31:03 [تصحيح أخطاء = IKEv1]IP
	64.102.156.87، معالجة حمولة VID
	24 أغسطس 11:31:03 [تصحيح أخطاء = IKEv1]IP
	64.102.156.87، تم إستلام DPD VID
	24 أغسطس 11:31:03 [تصحيح أخطاء = IKEv1]IP
	64.102.156.87، معالجة حمولة VID
	24 أغسطس 11:31:03 [تصحيح أخطاء = IKEv1]IP
	64.102.156.87، تم إستلام قيمة التجزئة VID
	أغسطس 24 11:31:03 [تصحيح أخطاء = IKEv1]IP
	64.102.156.87، قام نظير IKE بتضمين علامات قدرة تجزئة IKE: الوضع الرئيسي:وضع TrueAggressive:False
	24 أغسطس 11:31:03 [تصحيح أخطاء = IKEv1]IP
	64.102.156.87، معالجة حمولة VID
	24 أغسطس 11:31:03 [تصحيح أخطاء = IKEv1]IP
	64.102.156.87، تم تلقي NAT-Traversal من VID 02
	24 أغسطس 11:31:03 [تصحيح أخطاء = IKEv1]IP
	64.102.156.87، معالجة حمولة VID
	24 أغسطس 11:31:03 [تصحيح أخطاء = IKEv1]IP
	64.102.156.87، تم تلقي Cisco Unity Client VID
	في 24 أغسطس 11:31:03 [IKEv1]IP = 64.102.156.87، تم تنزيل الاتصال على IPsec tunnel_group
	24 أغسطس 11:31:03 [تصحيح أخطاء IKEv1]المجموعة = ipSec، IP = 64.102.156.87، معالجة حمولة IKE SA
	24 أغسطس 11:31:03 [IKEv1]فشل المرحلة 1:أنواع السمات غير المطابقة لوصف مجموعة الفئات:RCV d: المجموعة 2CFG d: المجموعة 5
	24 أغسطس 11:31:03 [IKEv1]فشل المرحلة 1:أنواع السمات غير المطابقة لوصف مجموعة الفئات:RCV d: المجموعة 2CFG d: المجموعة 5
	24 أغسطس 11:31:03 [IKEv1]فشل المرحلة 1:أنواع السمات غير المطابقة لوصف مجموعة الفئات:RCV d: المجموعة 2CFG d: المجموعة 5
	24 أغسطس 11:31:03 [IKEv1]فشل المرحلة 1:أنواع السمات غير المطابقة لوصف مجموعة الفئات:RCV d: المجموعة 2CFG d: المجموعة 5
	24 أغسطس 11:31:03 [IKEv1]فشل المرحلة 1:أنواع السمات غير المطابقة لوصف مجموعة الفئات:RCV d: المجموعة 2CFG d: المجموعة 5
	24 أغسطس 11:31:03 [IKEv1]فشل المرحلة 1:أنواع السمات غير المطابقة لوصف مجموعة الفئات:RCV d: المجموعة 2CFG d: المجموعة 5
	24 أغسطس 11:31:03 [IKEv1]فشل المرحلة 1:أنواع السمات	

	غير المطابقة لوصف مجموعة الفئات:d RCV: المجموعة 2CFG d: المجموعة 5 24 أغسطس 11:31:03 [IKEv1]فشل المرحلة 1:أنواع السمات غير المطابقة لوصف مجموعة الفئات:d RCV: المجموعة 2CFG d: المجموعة 5 24 أغسطس 11:31:03 [IKEv1]فشل المرحلة 1:أنواع السمات غير المطابقة لوصف مجموعة الفئات:d RCV: المجموعة 2CFG d: المجموعة 5 24 أغسطس 11:31:03 [IKEv1]فشل المرحلة 1:أنواع السمات غير المطابقة لوصف مجموعة الفئات:d RCV: المجموعة 2CFG d: المجموعة 5 24 أغسطس 11:31:03 [IKEv1]فشل المرحلة 1:أنواع السمات غير المطابقة لوصف مجموعة الفئات:d RCV: المجموعة 2CFG d: المجموعة 5 24 أغسطس 11:31:03 [IKEv1]فشل المرحلة 1:أنواع السمات غير المطابقة لوصف مجموعة الفئات:d RCV: المجموعة 2CFG d: المجموعة 5 24 أغسطس 11:31:03 [IKEv1]فشل المرحلة 1:أنواع السمات غير المطابقة لوصف مجموعة الفئات:d RCV: المجموعة 2CFG d: المجموعة 5 24 أغسطس 11:31:03 [IKEv1]فشل المرحلة 1:أنواع السمات غير المطابقة لوصف مجموعة الفئات:d RCV: المجموعة 2CFG d: المجموعة 5 24 أغسطس 11:31:03 [IKEv1]فشل المرحلة 1:أنواع السمات غير المطابقة لوصف مجموعة الفئات:d RCV: المجموعة 2CFG d: المجموعة 5 24 أغسطس 11:31:03 [IKEv1]فشل المرحلة 1:أنواع السمات غير المطابقة لوصف مجموعة الفئات:d RCV: المجموعة 2CFG d: المجموعة 5 24 أغسطس 11:31:03 [تصحيح أخطاء IKEv1]المجموعة = IP = 64.102.156.87 ،ipsEc، مقترح 1 # IKE SA، تحويل رقم 5AcceptedMatch Global IKE إدخال # 1	
	24 أغسطس 11:31:03 [تصحيح أخطاء IKEv1]المجموعة = IP = 64.102.156.87 ،ipSec، إنشاء حمولة ISAKMP SA 24 أغسطس 11:31:03 [تصحيح أخطاء IKEv1]المجموعة = IP = 64.102.156.87 ،ipsEc، إنشاء حمولة الكبل 24 أغسطس 11:31:03 [تصحيح أخطاء IKEv1]المجموعة = IP = 64.102.156.87 ،ipSec، إنشاء حمولة مرة واحدة أغسطس 24 11:31:03 [تصحيح أخطاء IKEv1]المجموعة = IP = 64.102.156.87 ،ipSec، يتم الآن إنشاء مفاتيح للمسؤول... 24 أغسطس 11:31:03 [تصحيح أخطاء IKEv1]المجموعة = IP = 64.102.156.87 ،ipSec، إنشاء حمولة المعرف 24 أغسطس 11:31:03 [تصحيح أخطاء IKEv1]المجموعة = IP = 64.102.156.87 ،ipSec، إنشاء حمولة التجزئة 24 أغسطس 11:31:03 [تصحيح أخطاء IKEv1]المجموعة = IP = 64.102.156.87 ،ipSec، تجزئة الحوسبة ل ISAKMP أغسطس 24 11:31:03 [تصحيح أخطاء IKEv1]المجموعة = IP = 64.102.156.87 ،ipSec، إنشاء حمولة Cisco Unity VID 24 أغسطس 11:31:03 [تصحيح أخطاء IKEv1]المجموعة = IP = 64.102.156.87 ،ipSec، إنشاء حمولة VID في الإصدار 6 24 أغسطس 11:31:03 [تصحيح أخطاء IKEv1]المجموعة = IP = 64.102.156.87 ،ipsEc، إنشاء حمولة نطاق الحماية (DPD)	التركيب AM2. وتتضمن هذه العملية ما يلي: - السياسات المختارة - -Diffie Hellman (DH) - معرف المستجيب -auth - حمولة اكتشاف ترجمة عنوان الشبكة (NAT)

	24 أغسطس 11:31:03 [تصحيح أخطاء IKEv1]المجموعة = 64.102.156.87، IP = ipSec، إنشاء حمولة NAT-Traversal VID الإصدار 02 24 أغسطس 11:31:03 [تصحيح أخطاء IKEv1]المجموعة = 64.102.156.87، IP = ipSec، إنشاء حمولة NAT-Discovery 24 أغسطس 11:31:03 [تصحيح أخطاء IKEv1]المجموعة = 64.102.156.87، IP = ipSec، تجزئة اكتشاف NAT للحوسبة 24 أغسطس 11:31:03 [تصحيح أخطاء IKEv1]المجموعة = 64.102.156.87، IP = ipSec، إنشاء حمولة NAT-Discovery 24 أغسطس 11:31:03 [تصحيح أخطاء IKEv1]المجموعة = 64.102.156.87، IP = ipSec، تجزئة اكتشاف NAT للحوسبة 24 أغسطس 11:31:03 [تصحيح أخطاء IKEv1]المجموعة = 64.102.156.87، IP = ipSec، إنشاء تجزؤ VID + حمولة القدرات الموسعة 24 أغسطس 11:31:03 [تصحيح أخطاء IKEv1]المجموعة = 64.102.156.87، IP = ipSec، إنشاء حمولة VID 24 أغسطس 11:31:03 [تصحيح أخطاء IKEv1]المجموعة = 64.102.156.87، IP = ipSec، إرسال Altiga/Cisco VPN3000/Cisco ASA GW VID	
إرسال AM2.	24 أغسطس 11:31:03 [IKEv1]IP = 64.102.156.87، IKE_Decode Send Message (msgid=0) مع الحمولات: HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + HASH (8) + المورد (13) + المورد (13) + المورد (13) + ((13) NAT-D (130) + NAT-D +) + المورد (13) + البائع (13) + لا شيء (0) الطول الإجمالي : 444	
	========== رسالة عدوانية 2 (AM2) <==========	
	50711:28:30.40208/24/12Sev=info/5IKE/0x630002F حزمة ISAKMP المستلمة: النظير = 64.102.156.8 50811:28:30.40308/24/12Sev=info/4IKE/0x6300014 إستلام <<< ISAKMP OAK AG (SA، KE، NON، ID، HASH، VID(Unity)، VID(Xauth)، VID(DPD)، VID(NAT-T)، NAT-D(؟)، VID(FRAG)، VID من 64.102.156.88 51011:28:30.41208/24/12sev=debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D5619780D7BE3E5 :R_Cookie=1B301D2DE710EDA0CurState AM_WAIT_MSG2Event: EV_RCVD_MSG	إستلمت AM2.
	5111:28:30.41208/24/12Sev=info/5IKE/0x6300001 النظير هو نظير متوافق مع Cisco-Unity 51211:28:30.41208/24/12Sev=info/5IKE/0x6300001 يدعم النظير Xauth 51311:28:30.41208/24/12Sev=info/5IKE/0x6300001 يدعم النظير DPD 51411:28:30.41208/24/12Sev=info/5IKE/0x6300001 دعم النظير ل NAT-T 51511:28:30.41208/24/12Sev=info/5IKE/0x6300001 يدعم النظير حمولات تجزئة IKE 51611:28:30.41208/24/12sev=debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D5619780D7BE3E5 :R_Cookie=1B301D2DE710EDA0CurState AM_WAIT_MSG2Event: EV_GEN_SKEYID 51711:28:30.4208/24/12Sev=debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D5619780D7BE3E5	العملية 2 AM.

	:R_Cookie=1B301D2DE710EDA0CurState AM_WAIT_MSG2Event: EV_AUTHENTICATE_PEER 51811:28:30.4208/24/12sev=debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D5619780D7BE3E5 :R_Cookie=1B301D2DE710EDA0CurState AM_WAIT_MSG2Event: EV_ADJUST_PORT 51911:28:30.4208/24/12Sev=debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D5619780D7BE3E5 :R_Cookie=1B301D2DE710EDA0CurState AM_WAIT_MSG2Event: EV_CRYPTO_ACTIVE	
	52011:28:30.4208/24/12Sev=debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D5619780D7BE3E5 :R_Cookie=1B301D2DE710EDA0CurState [AM_SND_MSG3Event: EV_BLD_MSG 5211:28:30.4208/24/12Sev=debug/8IKE/0x6300001 تم بدء نسخ معرف مورد IOS 52211:28:30.4208/24/12Sev=info/6IKE/0x6300001 تم نسخ معرف مورد IOS بنجاح	التركيب AM3. تتضمن هذه العملية مصادقة العميل. وفي هذه المرحلة، تم بالفعل تبادل جميع البيانات ذات الصلة بالتشفير.
	52311:28:30.42308/24/12sev=debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D5619780D7BE3E5 :R_Cookie=1B301D2DE710EDA0CurState AM_SND_MSG3Event: EV_SND_MSG 52411:28:30.42308/24/12Sev=info/4IKE/0x6300013 إرسال >>> ISAKMP OAK AG *(تجزئة، إعلام:،NAT-D، NAT-D، STATUS_INITIAL_CONTACT VID(؟)، VID(وحدة)) إلى 64.102.156.88	إرسال AM3.
	<========== رسالة عدوانية 3 (AM3) ==========	
إستلام AM3 من العميل.	24 أغسطس 11:31:03 [،64.102.156.87 = IPIKEv1] IKE_Decode تم إستلام رسالة (msgid=0) مع الحمولات : HDR + HASH (8) + NOTIFY (11) + NAT-D (130) + NAT-D (130) + المورد (13) + المورد (13) + لا شيء (0) الطول الإجمالي 168 :	
العملية AM 3. تأكيد إستخدام إجتياز NAT (NAT-T)). كلا الجانبين جاهزان الآن لبدء تشفير حركة المرور.	24 أغسطس 11:31:03 [تصحيح أخطاء IKEv1]المجموعة = IP = 64.102.156.87، ipSec، معالجة حمولة التجزئة 24 أغسطس 11:31:03 [تصحيح أخطاء IKEv1]المجموعة = IP = 64.102.156.87، ipSec، تجزئة الحوسبة ل ISAKMP 24 أغسطس 11:31:03 [تصحيح أخطاء IKEv1]المجموعة = IP = 64.102.156.87، ipSec، معالجة حمولة الإعلام 24 أغسطس 11:31:03 [تصحيح أخطاء IKEv1]المجموعة = IP = 64.102.156.87، ipSec، معالجة حمولة اكتشاف nat 24 أغسطس 11:31:03 [تصحيح أخطاء IKEv1]المجموعة = IP = 64.102.156.87، ipSec، تجزئة اكتشاف NAT للحوسبة 24 أغسطس 11:31:03 [تصحيح أخطاء IKEv1]المجموعة = IP = 64.102.156.87، ipSec، معالجة حمولة اكتشاف nat 24 أغسطس 11:31:03 [تصحيح أخطاء IKEv1]المجموعة = IP = 64.102.156.87، ipSec، تجزئة اكتشاف NAT للحوسبة 24 أغسطس 11:31:03 [تصحيح أخطاء IKEv1]المجموعة = IP = 64.102.156.87، ipSec، معالجة حمولة VID أغسطس 24 11:31:03 [تصحيح أخطاء IKEv1]المجموعة = IP = 64.102.156.87، ipSec، معالجة حمولة معرف المورد IOS/PIX (الإصدار 1.0.0، القدرات: 0000408) 24 أغسطس 11:31:03 [تصحيح أخطاء IKEv1]المجموعة =	

	ipSec، IP = 64.102.156.87، معالجة حمولة VID 24 أغسطس 11:31:03 [تصحيح أخطاء IKEv1]المجموعة = ipSec، IP = 64.102.156.87، تم إستلام Cisco Unity Client VID 24 أغسطس 11:31:03 [IKEv1]المجموعة = = ipSec، IP 64.102.156.87، الكشف التلقائي عن nat الحالة:Remote EndISbehind NAT DeviceThisend ليس خلف جهاز nat	
بدء المرحلة 1.5 (XAUTH)، وطلب بيانات اعتماد المستخدم.	24 أغسطس 11:31:03 [تصحيح أخطاء IKEv1]المجموعة = ipSec، IP = 64.102.156.87، إنشاء حمولة تجزئة فارغة 24 أغسطس 11:31:03 [تصحيح أخطاء IKEv1]المجموعة = ipSec، IP = 64.102.156.87، إنشاء حمولة تجزئة QM 24 أغسطس 11:31:03 [IKEv1]IP = 64.102.156.87، IKE_Decode Send Message (msgid=fb709d4d) مع الحمولات : 0) NONE (14) + ATTR (8) + HASH (HDR) الطول الإجمالي : 72	
	========== XAuth - طلب بيانات الاعتماد ==========>	
	53511:28:30.43008/24/12Sev=info/4IKE/0x6300014 إستلام <<</HASH، ATTR) * (isakmp OAK Trans من 64.102.156.88 53611:28:30.43108/24/12sev=decode/11IKE/0x630000 1 رأس ISAKMP ملف تعريف إرتباط البادئ:D56197780D7BE3E5 ملف تعريف إرتباط المستجيب:1B301D2DE710EDA0 الحمولة التالية:التجزئة الإصدار (10:(hex نوع التبادل:الحركة العلامات:(تشفير) MessageID(hex):FB709D4D الطول:76 تجزئة الحمولة الحمولة التالية: السمات محجوز: 00 طول الحمولة: 24 البيانات (باللغة السداسية العشرية): C779D5CBC5C75E3576C478A15A7CAB8A83A232D0 سمات الحمولة الحمولة التالية: لا شيء محجوز: 00 طول الحمولة: 20 النوع: ISAKMP_CFG_REQUEST محجوز: 00 المعرف: 0000 نوع Xauth: عام اسم مستخدم Xauth: (فارغ) كلمة مرور مستخدم Xauth: (فارغ) 53711:28:30.43108/24/12Sev=debug/7IKE/0x6300076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_INITIALEvent: EV_RCVD_MSG	تلقي طلب مصادقة. تظهر الحمولة التي تم فك تشفيرها حقلي اسم المستخدم وكلمة المرور الفارغتين.
	53811:28:30.43108/24/12sev=debug/7IKE/0x6300076 NAV Trace->TM:MsgID=FB709D4DCurState:	بدء المرحلة 1. 5 (Xauth). بدء مؤقت

	TM_PCS_XAUTH_REQEvent: EV_INIT_XAUTH 53911:28:30.43108/24/12 SEV=debug/7IKE/0x6300076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_PCS_XAUTH_REQEvent: .EV_START_RETRY_TMR 54011:28:30.43208/24/12sev=debug/7IKE/0x6300076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_WAIT_4USEREvent: EV_NO_EVENT 11:28:36.41508/24/12Sev=debug/7IKE/0x6300076 541 NAV Trace->TM:MsgID=FB709D4DCurState: TM_WAIT_4USEREvent: EV_RCVD_USER_INPUT	إعادة المحاولة بينما ينتظر إدخال المستخدم. عند نفاد مؤقت إعادة المحاولة، يتم قطع الاتصال تلقائيا.
	54211:28:36.41508/24/12Sev=debug/7IKE/0x6300076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_WAIT_4USEREvent: EV_SND_MSG 54311:28:36.41508/24/12Sev=info/4IKE/0x6300013 إرسال >>> ISAKMP OAK Trans *(HASH، ATTR) إلى 64.102.156.88 54411:28:36.41508/24/12Sev=decode/11IKE/0x63000 01 رأس ISAKMP ملف تعريف إرتباط البادئ:D56197780D7BE3E5 ملف تعريف إرتباط المستجيب:1B301D2DE710EDA0 الحمولة التالية:التجزئة الإصدار (10:(hex نوع التبادل:الحركة العلامات:(تشفير) MessageID(hex):FB709D4D الطول:85 تجزئة الحمولة الحمولة التالية: السمات محجوز: 00 طول الحمولة: 24 البيانات (باللغة السداسية العشرية): 1A3645155BE9A81CB80FCDB5F7F24E03FF8239F5 سمات الحمولة الحمولة التالية: لا شيء محجوز: 00 طول الحمولة: 33 النوع: ISAKMP_CFG_REPLY محجوز: 00 المعرف: 0000 نوع Xauth: عام اسم مستخدم Xauth: (لا يتم عرض البيانات) كلمة مرور مستخدم Xauth: (لا يتم عرض البيانات)	بمجرد إستلام إدخال المستخدم، قم بإرسال بيانات اعتماد المستخدم إلى الخادم. تظهر الحمولة التي تم فك تشفيرها حقلي اسم المستخدم وكلمة المرور المعبئين (ولكن المخفيين). طلب تكوين وضع الإرسال (سمات مختلفة).
	<========== xauth - مسوغات المستخدم ==========>	
إستلام بيانات اعتماد المستخدم.	أغسطس 24 11:31:09 [IKEv1]IP = 64.102.156.87، تلقى IKE_Decode رسالة (msgid=fb709d4d) مع الحمولات : HDR + تجزئة (8) + (14) ATTR) + لا شيء (0) مجموع الطول : 85 أغسطس 24 11:31:09 [تصحيح أخطاء IKEv1]المجموعة = process_attr، IP = 64.102.156.87، ipSec(): أدخل!	

معالجة مسوغات المستخدم. تحقق من بيانات الاعتماد، وقم بإنشاء حمولة تكوين الوضع. التكوين ذي الصلة: username cisco password cisco	أغسطس 24 11:31:09 [تصحيح أخطاء IKEv1]المجموعة = 64.102.156.87 ،IP = ipSec، سمات الرد على وضع المعالجة_CFG. أغسطس 24 11:31:09 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، IKEGetUserAttributes: DNS الأساسي = 192.168.1.99 أغسطس 24 11:31:09 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، IKEGetUserAttributes: DNS الثانوي = ممسوح أغسطس 24 11:31:09 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، IKEGetUserAttributes: WINS الأساسية = ممسوح أغسطس 24 11:31:09 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، IKEGetUserAttributes: WINS الثانوي = ممسوح أغسطس 24 11:31:09 [IKEv1 debug]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، IKEGetUserAttributes: قائمة تقسيم الاتصال النفقي = انقسام أغسطس 24 11:31:09 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، IKEGetUserAttributes: المجال الافتراضي = jyoungta-labdomain.cisco.com أغسطس 24 11:31:09 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، IKEGetUserAttributes: ضغط IP = معطل أغسطس 24 11:31:09 [IKEv1 debug]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، IKEGetUserAttributes: نهج تقسيم الاتصال النفقي = معطل أغسطس 24 11:31:09 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، IKEGetUserAttributes: إعداد وكيل المستعرض = عدم التعديل أغسطس 24 11:31:09 [IKEv1 debug]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، IKEGetUserAttributes: تجاوز وكيل المستعرض داخلي = تعطيل 24 أغسطس 11:31:09 [IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، تم التصديق على المستخدم (user1).	
إرسال نتيجة Xuath.	24 أغسطس 11:31:09 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، تكوين حمولة تجزئة فارغة 24 أغسطس 11:31:09 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، تكوين حمولة تجزئة QM 24 أغسطس 11:31:09 [IKEv1]IP = 64.102.156.87، IKE_Decode Send Message (msgid=5b6910ff) مع الحمولات : HDR + تجزئة (8) + 14) ATTR) + لا شيء (0) الطول الإجمالي : 64	
	XAuth ========== نتيجة التفويض ==========>	
إستلام نتائج المصادقة، ونتائج العملية.	54511:28:36.41608/24/12Sev=debug/7IKE/0x6300076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_XAUTHREQ_DONEEvent:	

	EV_XAUTHREQ_DONE 54611:28:36.41608/24/12Sev=debug/7IKE/0x6300076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_XAUTHREQ_DONEEvent: EV_NO_EVENT 54711:28:36.42408/24/12Sev=info/5IKE/0x630002F حزمة ISAKMP المستلمة: النظير = 64.102.156.88 54811:28:36.42408/24/12Sev=info/4IKE/0x6300014 إستلام <<</ATTR، HASH)* isakmp OAK Trans) من 64.102.156.88 54911:28:36.42508/24/12sev=decode/11IKE/0x630000 1 رأس ISAKMP ملف تعريف إرتباط البادئ:D56197780D7BE3E5 ملف تعريف إرتباط المستجيب:1B301D2DE710EDA0 الحمولة التالية:التجزئة الإصدار (10:(hex نوع التبادل:الحركة العلامات:(تشفير) معرف الرسالة (5B6910FF:(hex الطول:76 تجزئة الحمولة الحمولة التالية: السمات محجوز: 00 طول الحمولة: 24 البيانات (بالسداسي العشري): 7dCF47827164198731639BFB7595f694c9DDFE85 سمات الحمولة الحمولة التالية: لا شيء محجوز: 00 طول الحمولة: 12 النوع: ISAKMP_CFG_SET محجوز: 00 المعرف: 0000 حالة Xauth: pass 55011:28:36.42508/24/12Sev=debug/7IKE/0x6300076 NAV Trace->TM:MsgID=5B6910FFCurState: TM_INITIALEvent: EV_RCVD_MSG 5511:28:36.42508/24/12Sev=debug/7IKE/0x6300076 NAV Trace->TM:MsgID=5B6910FFCurState: TM_PCS_XAUTH_SETEvent: EV_INIT_XAUTH 55211:28:36.42508/24/12Sev=debug/7IKE/0x6300076 NAV Trace->TM:MsgID=5B6910FFCurState: TM_PCS_XAUTH_SETEvent: EV_CHK_AUTH_RESULT	
	55311:28:36.42508/24/12Sev=info/4IKE/0x6300013 إرسال >>> ATTR، HASH)* ISAKMP OAK Trans) إلى 64.102.156.88	نتيجة ACK.
	<========== xauth - الإقرار ==========	
إستلام ACK ومعالجته، لا توجد إستجابة من الخادم.	24 أغسطس 11:31:09 [IKEv1]IP = 64.102.156.87، تلقى IKE_Decode الرسالة (msgid=5b6910ff) مع الحمولات : HDR + تجزئة (8) + (14 ATTR) + لا شيء (0) الطول الإجمالي : 60	

	أغسطس 24 11:31:09 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، process_attr(): أدخل! أغسطس 24 11:31:09 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، معالجة سمات ACK	
	55511:28:36.42608/24/12Sev=debug/7IKE/0x6300076 NAV Trace->TM:MsgID=5B6910FFCurState: :TM_XAUTH_DONEEvent EV_XAUTH_DO_SUC 55611:28:36.42608/24/12Sev=debug/7IKE/0x6300076 NAV Trace->TM:MsgID=5B6910FFCurState: TM_XAUTH_DONEEvent: EV_NO_EVENT 55711:28:36.42608/24/12Sev=debug/7IKE/0x6300076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_XAUTHREQ_DONEEvent: EV_TERM_REQUEST 55811:28:36.42608/24/12Sev=debug/7IKE/0x6300076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_FREEEvent: EV_REMOVE 55911:28:36.42608/24/12Sev=debug/7IKE/0x6300076 NAV Trace->TM:MsgID=FB709D4DCurState: TM_FREEEvent: EV_NO_EVENT 56011:28:36.42608/24/12Sev=debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D5619780D7BE3E5 :R_Cookie=1B301D2DE710EDA0CurState CMN_XAUTH_PROGEvent: EV_XAUTH_DONE_SUC 5611:28:38.40608/24/12Sev=debug/8IKE/0x630004C بدء مؤقت DPD ل IKE SA (i_Cookie=d56197780d7BE3E5 sa (R_Cookie=1B301D2DE710EDA0->الحالة = 1، -sa dpd.worry_freq(mSec) = 5000> 56211:28:38.40608/24/12Sev=debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D5619780D7BE3E5 :R_Cookie=1B301D2DE710EDA0CurState CMN_MODECFG_PROGEvent: EV_INIT_MODECFG 56311:28:38.40608/24/12Sev=debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D5619780D7BE3E5 :R_Cookie=1B301D2DE710EDA0CurState CMN_MODECFG_PROGEvent: EV_NO_EVENT 56411:28:38.40608/24/12Sev=debug/7IKE/0x6300076 NAV Trace->TM:MsgID=84B4B653CurState: TM_INITIALEvent: EV_INIT_MODECFG 56511:28:38.40808/24/12Sev=info/5IKE/0x630005E العميل يرسل طلب جدار حماية إلى مركز التركيز 56611:28:38.40908/24/12sev=debug/7IKE/0x6300076 NAV Trace->TM:MsgID=84B4B653CurState: :TM_SND_MODECFGREQEvent .EV_START_RETRY_TMR	قم بإنشاء طلب mode-config. تظهر الحمولة التي تم فك تشفيرها المعلمات المطلوبة من الخادم.
	56711:28:38.40908/24/12sev=debug/7IKE/0x6300076 NAV Trace->TM:MsgID=84B4B653CurState: TM_SND_MODECFGREQEvent: EV_SND_MSG 56811:28:38.40908/24/12Sev=info/4IKE/0x6300013 إرسال >>> ISAKMP OAK Trans *(HASH، ATTR) إلى	قم بإرسال طلب mode-config.

	64.102.156.88 56911:28:38.62708/24/12sev=decode/11IKE/0x630000 1 رأس ISAKMP ملف تعريف إرتباط البادئ:D56197780D7BE3E5 ملف تعريف إرتباط المستجيب:1B301D2DE710EDA0 الحمولة التالية:التجزئة الإصدار (10:(hex نوع التبادل:الحركة العلامات:(تشفير) MessageID(hex):84B4B653 الطول:183 تجزئة الحمولة الحمولة التالية: السمات محجوز: 00 طول الحمولة: 24 البيانات (بالسداسي العشري): 81BFBF6721A744A815D69A315EF4AAA571D6B687 سمات الحمولة الحمولة التالية: لا شيء محجوز: 00 طول الحمولة: 131 النوع: ISAKMP_CFG_REQUEST محجوز: 00 المعرف: 0000 عنوان IPv4: (فارغ) قناع شبكة IPv4: (فارغ) DNS ل IPv4: (فارغ) IPv4 NBNS (WINS): (فارغ) انتهاء صلاحية العنوان: (فارغ) امتداد Cisco: الشعار: (فارغ) امتداد Cisco: حفظ PWD: (فارغ) امتداد Cisco: اسم المجال الافتراضي: (فارغ) امتداد Cisco: تقسيم التضمين: (فارغ) امتداد Cisco: تقسيم اسم DNS: (فارغ) امتداد Cisco: عمل PFS: (فارغ) غير معروف: (فارغ) امتداد Cisco: خوادم النسخ الاحتياطي: (فارغة) امتداد Cisco: قطع اتصال إزالة البطاقة الذكية: (فارغ) إصدار التطبيق: Cisco Systems VPN Client 5.0.07.0290:WinNT امتداد Cisco: نوع جدار الحماية: (فارغ) امتداد Cisco: اسم مضيف DNS الديناميكي: -ATBASU LABBOX		
	mode-config request ==========> ==========		
استلم طلب mode-config.	24 أغسطس 11:31:11 [IKEv1]IP = 64.102.156.87، تلقى IKE_Decode رسالة (msgid=84b4b653) مع الحمولات: HDR + HASH (8) + ATTR (14) + NONE (0)) الطول الإجمالي : 183	57011:28:38.6 2808/24/12sev = debug/7IKE/0x 6300076	انتظار إستجابة الخادم.

	أغسطس 24 11:31:11 [تصحيح أخطاء IKEv1][المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، process_attr(): أدخل!	NAV Trace->TM:MsgID=84B4B653CurState: TM_WAIT_MODECFGREPLYEvent: EV_NO_EVENT	
طلب تكوين وضع العملية. يتم تكوين العديد من هذه القيم عادة في نهج المجموعة. ومع ذلك، فنظرا لأن الخادم في هذا المثال له تكوين أساسي للغاية، فلن تتمكن من رؤيتهم هنا.	24 أغسطس 11:31:11 [تصحيح أخطاء IKEv1][المجموعة = ipSec، اسم المستخدم = 64.102.156.87 ،user1، معالجة سمات طلب CFG أغسطس 24 11:31:11 [تصحيح أخطاء IKEv1][المجموعة = ipSec، اسم المستخدم = 64.102.156.87، IP = user1، mode_cfg: تم تلقي طلب عنوان IPv4! أغسطس 24 11:31:11 [تصحيح أخطاء IKEv1][المجموعة = ipSec، اسم المستخدم = 64.102.156.87، IP = user1، mode_cfg: تم تلقي طلب لقناع شبكة IPv4! أغسطس 24 11:31:11 [تصحيح أخطاء IKEv1][المجموعة = ipSec، اسم المستخدم = 64.102.156.87، IP = user1، MODE_CFG: تم تلقي طلب عنوان خادم DNS! أغسطس 24 11:31:11 [تصحيح أخطاء IKEv1][المجموعة = ipSec، اسم المستخدم = 64.102.156.87، IP = user1، mode_cfg: تم تلقي طلب عنوان خادم WINS! 24 أغسطس 11:31:11 [IKEv1][المجموعة = ipSec، اسم المستخدم = 64.102.156.87 ،user1، سمة وضع المعاملة غير المدعومة التي تم تلقيها: 5 أغسطس 24 11:31:11 [تصحيح أخطاء IKEv1][المجموعة = ipSec، اسم المستخدم = 64.102.156.87، IP = user1، mode_cfg: تم تلقي طلب الشعار! أغسطس 24 11:31:11 [تصحيح أخطاء IKEv1][المجموعة = ipSec، اسم المستخدم = 64.102.156.87، IP = user1، mode_cfg: تم تلقي طلب حفظ إعداد PW! أغسطس 24 11:31:11 [IKEv1 debug][المجموعة = ipSec، اسم المستخدم = mode_cfg، IP = 64.102.156.87، user1: تم تلقي طلب لاسم المجال الافتراضي! أغسطس 24 11:31:11 [تصحيح أخطاء IKEv1][المجموعة = ipSec، اسم المستخدم = 64.102.156.87، IP = user1، mode_cfg: تم تلقي طلب لقائمة النفق المقسم! أغسطس 24 11:31:11 [تصحيح أخطاء IKEv1][المجموعة = ipSec، اسم المستخدم = 64.102.156.87، IP = user1، mode_cfg: تم تلقي طلب DNS المقسمة! أغسطس 24 11:31:11 [IKEv1 debug][المجموعة = ipSec، اسم المستخدم = 64.102.156.87، IP = user1، MODE_CFG: تم تلقي طلب إعداد PFS! أغسطس 24 11:31:11 [تصحيح أخطاء IKEv1][المجموعة = ipSec، اسم المستخدم = 64.102.156.87، IP = user1، MODE_CFG: تم تلقي طلب إعداد وكيل مستعرض العميل! أغسطس 24 11:31:11 [تصحيح أخطاء IKEv1][المجموعة = ipSec، اسم المستخدم = 64.102.156.87، IP = user1، MODE_CFG: تم تلقي طلب لإجراء نسخ إحتياطي لقائمة نظير ip-sec! أغسطس 24 11:31:11 [IKEv1 debug][المجموعة = ipSec،		

	اسم المستخدم = user1، IP = 64.102.156.87، MODE_CFG: تم تلقي طلب إعداد قطع اتصال إزالة البطاقة الذكية للعميل! أغسطس 24 11:31:11 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، MODE_CFG: تم إستلام طلب إصدار التطبيق! 24 أغسطس 11:31:11 [IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، نوع العميل: إصدار تطبيق WinNTCclient: 5.0.07.0290 أغسطس 24 11:31:11 [IKEv1 debug]المجموعة = ipSec، اسم المستخدم = mode_cfg، IP = 64.102.156.87، user1: تم تلقي طلب ل FWTYPE! أغسطس 24 11:31:11 [IKEv1 debug]المجموعة = ipSec، اسم المستخدم = mode_cfg، IP = 64.102.156.87، user1: تم تلقي طلب اسم مضيف DHCP ل DDNS هو: atbasu-labbox!	
قم بإنشاء إستجابة mode-config باستخدام جميع القيم التي تم تكوينها. التكوين ذي الصلة: ملاحظة في هذه الحالة، يتم تعيين IP للمستخدم دائما. username cisco attributes **vpn-framed-ip-address 192.168.1.100 255.255.255.0** group-policy EZ internal group-policy EZ attributes password-storage enabledns-server value 192.168.1.129 vpn-tunnel-protocol ikev1 split-tunnel-policy tunnelall split-tunnel-network-list value split	أغسطس 24 11:31:11 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، تم الحصول على عنوان 192.168.1.100) IP) قبل بدء وضع CFG (تم تمكين XAuth) 24 أغسطس 11:31:11 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، إرسال قناع الشبكة الفرعية (255.255.255.0) إلى عميل بعيد 24 أغسطس 11:31:11 [IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، عنوان IP خاص تم تعيينه للمستخدم البعيد 192.168.1.100 24 أغسطس 11:31:11 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، تكوين حمولة تجزئة فارغة أغسطس 24 11:31:11 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، construct_cfg_set: المجال الافتراضي = jyoungta-labdomain.cisco.com أغسطس 24 11:31:11 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، إرسال سمات وكيل مستعرض العميل! أغسطس 24 11:31:11 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، تم تعيين وكيل المستعرض على "عدم التعديل". لن يتم تضمين بيانات وكيل المستعرض في الرد mode-cfg أغسطس 24 11:31:11 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، إرسال تمكين فصل إزالة البطاقة الذكية من Cisco!! 24 أغسطس 11:31:11 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، تكوين حمولة تجزئة QM	

-default domain value -jyoungta labdomain.cisco.com			
قم بإرسال الاستجابة mode-config.	24 أغسطس 11:31:11 [IKEv1]IP = 64.102.156.87، IKE_Decode Send Message (msgid=84b4b653) مع الحمولات : HDR + التجزئة (8) + 0) NONE (14) (ATTR) الطول الإجمالي : 215		
	mode-config response ========== ==========>		
إستلام قيم معلمات mode-config من الخادم.	5711:28:38.63808/24/12Sev=info/5IKE/0x630002F حزمة ISAKMP المستلمة: النظير = 64.102.156.88 57211:28:38.63808/24/12Sev=info/4IKE/0x6300014 إستلام <<<\ATTR، HASH)* isakmp OAK Trans) من 64.102.156.88 57311:28:38.63908/24/12sev=decode/11IKE/0x6300001 رأس ISAKMP ملف تعريف إرتباط البادئ:D56197780D7BE3E5 ملف تعريف إرتباط المستجيب:1B301D2DE710EDA0 الحمولة التالية:التجزئة الإصدار (10:(hex نوع التبادل:الحركة العلامات:(تشفير) MessageID(hex):84B4B653 الطول:220 تجزئة الحمولة الحمولة التالية: السمات محجوز: 00 طول الحمولة: 24 البيانات (بالسداسي العشري): 6DE2E70ACF6B1858846BC62E590C00A66745D14D سمات الحمولة الحمولة التالية: لا شيء محجوز: 00 طول الحمولة: 163 النوع: ISAKMP_CFG_REPLY محجوز: 00 المعرف: 0000 عنوان IPv4: 192.168.1.100 قناع شبكة IPv4: 255.255.255.0 IPv4 DNS: 192.168.1.99 امتداد Cisco: حفظ PWD: لا امتداد Cisco: اسم المجال الافتراضي: jyoungta-labdomain.cisco.com امتداد Cisco: Do PFS: لا إصدار التطبيق: Cisco Systems، Inc ASA5505، الإصدار 8.4(4)1 الذي تم إنشاؤه بواسطة البنائين في THU 14-JUN-12 11:20 امتداد Cisco: قطع اتصال إزالة البطاقة الذكية: نعم		
معلمات العملية، ثم قم بتكوين نفسه وفقا لذلك.	57411:28:38.63908/24/12sev=	أغسطس 24 11:31:13 [فك ترميز IKEv1]IP = 64.102.156.87، المستجيب IKE الذي يبدأ QM: معرف msg = 0e83792e	يتم إكمال المرحلة 1 على الخادم. بدء

عملية الوضع السريع (QM).	أغسطس 24 11:31:13 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، معالجة الوضع السريع التأخير، CERT/Trans Exch/RM DSID قيد التقدم 24 أغسطس 11:31:13 [IKEv1]المجموعة = ipSec، اسم المستخدم = = IP ،user1 64.102.156.87، ARP مجاني يتم إرساله ل 192.168.1.100 24 أغسطس 11:31:13 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، إستئناف معالجة الوضع السريع، اكتمل CERT/Trans Exch/RM DSID 24 أغسطس 11:31:13 [IKEv1]المجموعة = ipSec، اسم المستخدم = = IP ،user1 64.102.156.87، اكتملت المرحلة 1	debug/7IKE/0x 6300076 NAV Trace-> TM:MsgID=8 4B4B653CurSt :ate TM_WAIT_MO DECFGREPL YEvent: EV_RCVD_MS G 57511:28:38.6 3908/24/12sev = معلومات/5IKE/0 x6300010 MODE_CFG_ REPLY: السمة = internal_IPV4_ address:، القيمة = 192.168.1.100 57611:28:38.6 3908/24/12Se v=info/5IKE/0x 6300010 MODE_CFG_ REPLY: السمة = internal_IPv4_ netmask:، القيمة = 255.255.255.0 57711:28:38.6 3908/24/12sev = معلومات/5IKE/0 x6300010 MODE_CFG_ REPLY: السمة = internal_IPv4_ dns(1):، القيمة = 192.168.1.99 57811:28:38.6 3908/24/12sev =info/5IKE/0x6 30000d MODE_CFG_ REPLY: السمة =	

	modecfg_unity _savepwd:، القيمة = 0x00000 57911:28:38.6 3908/24/12Se v=info/5IKE/0x 630000E MODE_CFG_ REPLY: السمة = modecfg_unity _defdomain:، value = -jjuventa labdomain.cisc o.com 58011:28:38.6 3908/24/12sev = معلومات/0/5IKE x630000d mode_cfg_repl y: السمة = modecfg_unity _pfs:، القيمة = 0x000000 5811:28:38.63 908/24/12Sev =info/5IKE/0x6 30000E MODE_CFG_ REPLY: السمة = application_ver sion، القيمة = Cisco Systems، Inc ASA5505، الإصدار 8.4(4)1 الذي تم إنشاؤه بواسطة البناؤون في ثو 14-يونيو-12 11:20 58211:28:38.6 3908/24/12sev = معلومات/0/5IKE x630000d MODE_CFG_ REPLY: السمة =		

	modecfg_unity _smartcard_re move_disconn ect: ، value = 0x000001 58311:28:38.6 3908/24/12sev = معلومات/5IKE/0 x630000d MODE_CFG_ REPLY: السمة = تم تلقيها واستخدام -NAT T رقم المنفذ، القيمة = 0x00001194 58411:28:39.3 6708/24/12sev = debug/9IKE/0x 6300093 قيمة المعلمة INI EnableDNSRe 1 هي direction 58511:28:39.3 6708/24/12sev = debug/7IKE/0x 6300076 NAV Trace- >TM:MsgID=8 4B4B653CurSt :ate TM_MODECF G_DONEEven t: EV_MODECF G_DONE_SU C		
إنشاء DPD وإرساله للعميل.	24 أغسطس 11:31:13 [64.102.156.87 = IP[IKEv1، النوع Keep-Live لهذا الاتصال: DPD أغسطس 24 11:31:13 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = 64.102.156.87 = IP ،user1، بدء مؤقت إعادة مفاتيح P1: 82080 ثانية. 24 أغسطس 11:31:13 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = 64.102.156.87 = IP ،user1، إرسال رسالة الإعلام 24 أغسطس 11:31:13 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = 64.102.156.87 = IP ،user1، تكوين حمولة تجزئة فارغة 24 أغسطس 11:31:13 [تصحيح أخطاء IKEv1]المجموعة =		

	ipSec، اسم المستخدم = user1، IP = 64.102.156.87، تكوين حمولة تجزئة QM 24 أغسطس 11:31:13 [IKEv1]IP = 64.102.156.87، IKE_Decode Send Message (msgid=be8f7821) مع الحمولات : 0) NONE + Notify (11) + HASH (8) + HDR) الطول الإجمالي : 92	
	========== اكتشاف النظير الميت (DPD) <==========	
	58811:28:39.79508/24/12sev=debug/7IKE/0x6300015 lcl=0x0501A8C0، mask=0x00FFFFFF، intf_data&colon؛ bcast=0xFF01A8C0، bcast_vra=0xFF07070A 58911:28:39.79508/24/12sev=debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D5619780D7BE3E5 :R_Cookie=1B301D2DE710EDA0CurState CMN_MODECFG_PROGEvent: EV_INIT_P2 59011:28:39.79508/24/12Sev=info/4IKE/0x6300056 تم تلقي طلب أساسي من برنامج التشغيل: IP المحلي = 192.168.1.100، IP = 64.102.156.88، GW IP عن بعد = 0.0.0 5911:28:39.79508/24/12Sev=debug/7IKE/0x6300076 NAV Trace->SA:I_Cookie=D5619780D7BE3E5 :R_Cookie=1B301D2DE710EDA0CurState CMN_ACTIVEEvent: EV_NO_EVENT 59211:28:39.79508/24/12Sev=debug/7IKE/0x6300076 NAV Trace->QM:MsgID=0E83792ECurState: QM_INITIALEvent: EV_Initiator 59311:28:39.79508/24/12Sev=debug/7IKE/0x6300076 NAV Trace->QM:MsgID=0E83792ECurState: QM_BLD_MSG1Event: EV_CHK_PFS 59411:28:39.79608/24/12Sev=debug/7IKE/0x6300076 NAV Trace->QM:MsgID=0E83792ECurState: QM_BLD_MSG1event: EV_BLD_MSG 59511:28:39.79608/24/12Sev=debug/7IKE/0x6300076 NAV Trace->QM:MsgID=0E83792ECurState: .QM_SND_MSG1Event: EV_START_RETRY_TMR	بدء تطبيق جودة الخدمة (QM)، المرحلة الثانية. التركيب QM1. وتتضمن هذه العملية ما يلي: - تجزئة - مع كافة مقترحات المرحلة الثانية التي يدعمها العميل ونوع النفق والتشفير - Nonce - معرف العميل - معرفات الوكيل
	59611:28:39.79608/24/12Sev=debug/7IKE/0x6300076 NAV Trace->QM:MsgID=0E83792ECurState: QM_SND_MSG1event: EV_SND_MSG 59711:28:39.79608/24/12Sev=info/4IKE/0x6300013 إرسال >>> Isakmp OAK QM *(تجزئة، SA، غير، معرف، معرف) إلى 64.102.156.88	إرسال QM1.
	<========== رسالة الوضع السريع 1 (QM1) ==========	
إستقبال QM1.	24 أغسطس 11:31:13 [IKEv1]IP = 64.102.156.87، IKE_Decode استلم الرسالة (msgid=e83792e) مع الحمولات : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + 0) NONE (5) + ID) الطول الإجمالي: 1026	
معالجة QM1. التكوين ذي الصلة: crypto dynamic-map	24 أغسطس 11:31:13 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، معالجة حمولة التجزئة 24 أغسطس 11:31:13 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87،	

DYN 10 set -transform set TRA	معالجة حمولة SA 24 أغسطس 11:31:13 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، معالجة الحمولة مرة واحدة 24 أغسطس 11:31:13 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، معالجة حمولة معرف أغسطس 24 11:31:13 [IKEv1 Decode] المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، ID_IPv4_ADDR تم إستلام المعرف 192.168.1.100 24 أغسطس 11:31:13 [IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، تم إستلام بيانات مضيف الوكيل البعيد في حمولة المعرف:العنوان 192.168.1.100، البروتوكول 0، المنفذ 0 24 أغسطس 11:31:13 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، معالجة حمولة معرف أغسطس 24 11:31:13 [فك تشفير IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، ID_IPv4_ADDR_SUBNET ID الذي تم إستلامه—0.0.0.0.0 أغسطس 24 11:31:13 [IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، بيانات الشبكة الفرعية لوكيل IP المحلي في حمولة المعرف:العنوان 0.0.0.0، القناع 0.0.0.0، البروتوكول 0، المنفذ 0 24 أغسطس 11:31:13 [IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، QM يتم إعادة تكوينها القديمة نظرا لعدم العثور عليها بواسطة ADDR أغسطس 24 11:31:13 [IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، التحقق من خريطة التشفير الثابتة، التحقق من الخريطة = 10 ،out-map... 24 أغسطس 11:31:13 [IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، التحقق الثابت من خريطة التشفير بالمرور: إدخال خريطة التشفير غير مكتمل! أغسطس 24 11:31:13 [IKEv1 debug]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، تحديد أوضاع النقل عبر بروتوكول UDP-Encapsulated-Tunnel و-UDP Encapsulated-Transport التي تم تعريفها بواسطة محول NAT أغسطس 24 11:31:13 [IKEv1 debug]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، تحديد أوضاع النقل عبر بروتوكول UDP-Encapsulated-Tunnel و-UDP Encapsulated-Transport التي تم تعريفها بواسطة محول NAT أغسطس 24 11:31:13 [IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، نظير IKE البعيد الذي تم تكوينه لخريطة التشفير: out-dyn-map 24 أغسطس 11:31:13 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، معالجة حمولة IPSec SA	
التركيب QM2. التكوين ذي	أغسطس 24 11:31:13 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، مقترح	

الصلة: tunnel-group EZ type **remote-!** **access** *tunnel type)* *ra = tunnel* *type remote-* *(access* crypto ipsec -transform set TRA **esp--aes esp sha-hmac** crypto ipsec -security association **lifetime seconds 28800** crypto ipsec -security association lifetime kilobytes 4608000 **crypto dynamic-map DYN 10 set -transform set TRA** crypto map MAP 65000 ipsec-isakmp dynamic DYN crypto map MAP interface outside	12 # IPSec sa، تحويل # 1AcceptedMatch Global IPSec SA الإدخال # 10 24 أغسطس 11:31:13 [IKEv1]المجموعة = ipSec، اسم المستخدم = IKE، 64.102.156.87 = IP، user1: طلب SPI! IPSec: تم إنشاء SA جنيني جديد عند 0xCFDFFC90، SCB: 0xCFDFFB58، الإتجاه: الوارد SPI: 0x9E18ACB2 معرف جلسة العمل: 0x00138000 num ل VPIF: 0x000004 نوع النفق: RA البروتوكول: ESP العمر الافتراضي: 240 ثانية أغسطس 24 11:31:13 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = 64.102.156.87 = IP، user1، حصلت IKE على SPI من المحرك الرئيسي: SPI = 0x9e18acb2 أغسطس 24 11:31:13 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = 64.102.156.87 = IP، user1، تكوين وضع سريع 24 أغسطس 11:31:13 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = 64.102.156.87 = IP، user1، تكوين حمولة تجزئة فارغة 24 أغسطس 11:31:13 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = 64.102.156.87 = IP، user1، إنشاء حمولة IPSec SA 24 أغسطس 11:31:13 [IKEv1]المجموعة = ipSec، اسم المستخدم = 64.102.156.87 = IP، user1، تجاوز مدة إعادة حساب IPSec الخاصة ببادئ التشغيل من 2147483 إلى 86400 ثانية 24 أغسطس 11:31:13 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = 64.102.156.87 = IP، user1، إنشاء حمولة IPSec مرة واحدة 24 أغسطس 11:31:13 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = 64.102.156.87 = IP، user1، إنشاء معرف الوكيل 24 أغسطس 11:31:13 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = 64.102.156.87 = IP، user1، معرف وكيل الإرسال: المضيف البعيد: 192.168.1.100 البروتوكول 0 0Port الشبكة الفرعية المحلية:0.0.0.0 0.0.0.0mask بروتوكول 0port 0 24 أغسطس 11:31:13 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = 64.102.156.87 = IP، user1، إرسال إعلام العمر الافتراضي للمستجيب إلى البادئ 24 أغسطس 11:31:13 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = 64.102.156.87 = IP، user1، تكوين حمولة تجزئة QM	
إرسال QM2.	أغسطس 24 11:31:13 [IKEv1 Decode] المجموعة = ipSec، اسم المستخدم = 64.102.156.87 = IP، user1، مستجيب IKE يرسل QM PKT الثاني: معرف msg = 0e83792e 24 أغسطس 11:31:13 [IKEv1]IP = 64.102.156.87، IKE_Decode Send Message (msgid=e83792e) مع الحمولات : HDR + HASH (8) + SA (1) + NONCE (10) + NOTIFY (11) + NONE (0) + ID (5) + ID (5) الطول: 184	

	========== رسالة الوضع السريع 2 (QM2) <==========	
	60811:28:39.96208/24/12Sev=info/4IKE/0x6300014 إستلام <<< ISAKMP OAK QM *(تجزئة، SA، غير، معرف، معرف، إعلام:status_resp_lifetime) من 64.102.156.88	إستقبال QM2.
	60911:28:39.96408/24/12sev=decode/11IKE/0x6300001 رأس ISAKMP ملف تعريف إرتباط البادئ:D56197780D7BE3E5 ملف تعريف إرتباط المستجيب:1B301D2DE710EDA0 الحمولة التالية:التجزئة الإصدار (10:(hex نوع Exchange:صيغة سريعة العلامات:(تشفير) MessageID(hex):E83792E الطول:188 تجزئة الحمولة الحمولة التالية: اقتران الأمان محجوز: 00 طول الحمولة: 24 البيانات (باللغة السداسية العشرية): CABF38A62C9B88D1691E81F3857d6189534B2EC0 اقتران أمان الحمولة الحمولة التالية: Nonce محجوز: 00 طول الحمولة: 52 DOI: IPsec الحالة: (SIT_IDENTITY_ONLY) مقترح الحمولة الحمولة التالية: لا شيء محجوز: 00 طول الحمولة: 40 المقترح رقم: 1 معرف البروتوكول: PROTO_IPsec_ESP حجم SPI: 4 # من التحويلات: 1 SPI: 9E18ACB2 تحويل الحمولة الحمولة التالية: لا شيء محجوز: 00 طول الحمولة: 28 التحويل #: 1 Transform-id: ESP_3DES محجوز 2: 0000 نوع الحياة: ثوان مدة البقاء (سداسي عشر): 0020c49b وضع التضمين: نفق UDP خوارزمية المصادقة: SHA1 الحمولة Nonce الحمولة التالية: التعريف	معالجة QM2. تعرض الحمولة التي تم فك تشفيرها العروض المختارة.

	محجوز: 00 طول الحمولة: 24 البيانات (بالسداسي العشري): 3A079B75DA512473706F235EA3FCA61F1D15D4CD تعريف الحمولة الحمولة التالية: التعريف محجوز: 00 طول الحمولة: 12 نوع المعرف: عنوان IPv4 معرف البروتوكول (UDP/TCP، وما إلى ذلك): 0 المنفذ: 0 ID Data&colon؛ 192.168.1.100 تعريف الحمولة الحمولة التالية: الإعلام محجوز: 00 طول الحمولة: 16 نوع المعرف: الشبكة الفرعية ل IPv4 معرف البروتوكول (UDP/TCP، وما إلى ذلك): 0 المنفذ: 0 ID Data&colon؛ 0.0.0.0/0.0.0.0 إعلام الحمولة الحمولة التالية: لا شيء محجوز: 00 طول الحمولة: 28 DOI: IPsec معرف البروتوكول: PROTO_IPsec_ESP حجم SPI: 4 نوع الإخطار: status_resp_lifetime SPI: 9E18ACB2 Data&colon؛ نوع الحياة: ثوان مدة البقاء (ست عشري): 00015180	
	61011:28:39.96508/24/12Sev=debug/7IKE/0x6300076 NAV Trace->QM:MsgID=0E83792ECurState: QM_WAIT_MSG2Event: EV_RCVD_MSG 6111:28:39.96508/24/12Sev=info/5IKE/0x6300045 يحتوي إعلام مدة بقاء المستجيب على قيمة 86400 ثانية 61211:28:39.96508/24/12Sev=debug/7IKE/0x6300076 NAV Trace->QM:MsgID=0E83792ECurState: QM_WAIT_MSG2Event: EV_CHK_PFS 61311:28:39.96508/24/12Sev=debug/7IKE/0x6300076	معالجة QM2.
	NAV Trace->QM:MsgID=0E83792ECurState: QM_BLD_MSG3Event: EV_BLD_MSG 61411:28:39.96508/24/12Sev=debug/7IKE/0x6300076 رأس ISAKMP ملف تعريف إرتباط البادئ:D56197780D7BE3E5 ملف تعريف إرتباط المستجيب:1B301D2DE710EDA0 الحمولة التالية:التجزئة الإصدار (10:(hex نوع Exchange:صيغة سريعة العلامات:(تشفير) MessageID(hex):E83792E الطول:52	التركيب QM3. الحمولة التي تم فك تشفيرها ل QM3 الموضحة هنا. تتضمن هذه العملية التجزئة.

	تجزئة الحمولة الحمولة التالية: لا شيء محجوز: 00 طول الحمولة: 24 البيانات (بالسداسي العشري): CDDC20D91EB4B568C826D6A5770A5CF020141236	
	61511:28:39.96508/24/12Sev=debug/7IKE/0x6300076 NAV Trace->QM:MsgID=0E83792ECurState: QM_SND_MSG3Event: EV_SND_MSG 61611:28:39.96508/24/12Sev=info/4IKE/0x6300013 الإرسال >>> HASH)* Isakmp OAK QM) إلى 64.102.156.88	إرسال QM3. العميل جاهز الآن للتشفير وفك التشفير.
	<========== رسالة الوضع السريع 3 (QM3) ==========	
إستقبال QM3.	24 أغسطس 11:31:13 [64.102.156.87 = IP][IKEv1، تلقى IKE_Decode الرسالة (msgid=e83792e) مع الحمولات : HDR + تجزئة (8) + لا شيء (0) إجمالي الطول : 52	

معالجة QM3. قم بإنشاء فهارس معلمات الأمان الواردة والصادرة (SPIs). إضافة مسار ثابت للمضيف. التكوين ذي الصلة:
 	
`crypto ipsec -transform set TRA esp- -aes esp sha-hmac`
`crypto ipsec -security association lifetime seconds 28800`
`crypto ipsec -security association lifetime kilobytes 4608000`
`crypto dynamic-map DYN 10 set -transform set TRA`
`crypto dynamic-map DYN 10 **set -reverse route**`
	24 أغسطس 11:31:13 [تصحيح أخطاء IKEv1][المجموعة = ipSec، اسم المستخدم = 64.102.156.87 ،user1، معالجة حمولة التجزئة
	24 أغسطس 11:31:13 [تصحيح أخطاء IKEv1][المجموعة = ipsEc، اسم المستخدم = 64.102.156.87 ،user1، تحميل جميع شبكات IPsec SAs
	أغسطس 24 11:31:13 [تصحيح أخطاء IKEv1][المجموعة = ipSec، اسم المستخدم = 64.102.156.87 ،user1، إنشاء مفتاح الوضع السريع!
	أغسطس 24 11:31:13 [تصحيح أخطاء IKEv1][المجموعة = ipSec، اسم المستخدم = 64.102.156.87 ،user1، قاعدة تشفير NP للبحث عن قاعدة تشفير التشفير خارج-10 dyn-map غير المعروفة لقوائم التحكم في الوصول (ACL) المطابقة: تم إرجاعها
	cs_id=cc107410؛ قاعدة=000000
	أغسطس 24 11:31:13 [تصحيح أخطاء IKEv1][المجموعة = ipSec، اسم المستخدم = 64.102.156.87 ،user1، إنشاء مفتاح الوضع السريع!
	IPSec: تم إنشاء SA جنيني جديد عند 0xccc9ed60،
	SCB: 0xCF7F59E0،
	الإتجاه: الصادر
	SPI: 0xC05290a
	معرف جلسة العمل: 0x00138000
	num ل VPIF: 0x000004
	نوع النفق: RA
	البروتوكول: ESP
	العمر الافتراضي: 240 ثانية
	IPSec: اكتمل تحديث OBSA للمضيف، SPI 0xC055290A
	IPSec: إنشاء سياق VPN الصادر، SPI 0xC055290A
	العلامات: 0x0000025
	SA: 0xccc9ed60
	SPI: 0xC05290a
	MTU: 1500 بايت
	VCID: 0x000000
	النظير: 0x000000	

SCB: 0xA5922B6B
القناة: 0xc82afb60
IPSec: سياق VPN الصادر المكتمل، SPI 0xC055290A
معالج VPN: 0x0015909c
IPSec: قاعدة تشفير صادرة جديدة، SPI 0xC055290A
عنوان SRC: 0.0.0.0
قناع SRC: 0.0.0.0
DST: 192.168.1.100
قناع DST: 255.255.255.255
منافذ SRC
أعلى: 0
أقل: صفر
التجاهل
منافذ DST
أعلى: 0
أقل: صفر
التجاهل
البروتوكول: 0
إستخدام البروتوكول: خطأ
SPI: 0x000000
إستخدام SPI: خطأ
IPSec: قاعدة التشفير الصادر المكتملة، SPI 0xC055290A
معرف القاعدة: 0xcb47a710
IPSec: قاعدة السماح الصادرة الجديدة، SPI 0xC055290A
Src addr: 64.102.156.88
قناع SRC: 255.255.255.255
DST: 64.102.156.87
قناع DST: 255.255.255.255
منافذ SRC
أعلى: 4500
أقل: 4500
أوبس: يساوي
منافذ DST
أعلى: 58506
أدنى: 58506
أوبس: يساوي
البروتوكول: 17
إستخدام البروتوكول: صحيح
SPI: 0x000000
إستخدام SPI: خطأ
IPSec: قاعدة السماح الصادرة المكتملة، SPI 0xC055290A
معرف القاعدة: 0xcdf3cfa0
أغسطس 24 11:31:13 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، قاعدة تشفير NP للبحث عن قاعدة تشفير التشفير خارج-10 dyn-map غير المعروفة لقوائم التحكم في الوصول (ACL) المطابقة: تم إرجاعها
cs_id=cc107410؛ قاعدة=000000
أغسطس 24 11:31:13 [IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، اكتمال تفاوض الأمان للمستخدم (user1)Responder، SPI الوارد = 0x9e18acb2، Outbound SPI = 0xc05290a

	24 أغسطس 11:31:13 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = IKE ،user1، IP = 64.102.156.87 حصلت على KEY_ADD msg ل SA: SPI = 0xc055290a IPSec: اكتمل تحديث IBSA المضيف، SPI 0x9E18ACB2 IPSec: إنشاء سياق VPN الوارد، SPI 0x9E18ACB2 العلامات: 0x0000026 SA: 0xcfdffc90 SPI: 0x9E18ACB2 وحدة الحد الأقصى للنقل (0 :(MTU بايت VCID: 0x000000 النظير: 0x0015909c SCB: 0xA5672481 القناة: 0xc82afb60 IPSec: سياق VPN الوارد المكتمل، SPI 0x9E18ACB2 معالج VPN: 0x0016219c IPSec: تحديث سياق VPN الصادر SPI ،0x0015909C 0xC055290A العلامات: 0x0000025 SA: 0xccc9ed60 SPI: 0xC05290a MTU: 1500 بايت VCID: 0x000000 النظير: 0x0016219c SCB: 0xA5922B6B القناة: 0xc82afb60 IPSec: سياق VPN الصادر المكتمل، SPI 0xC055290A معالج VPN: 0x0015909c IPSec: قاعدة داخلية صادرة مكتملة، SPI 0xC055290A معرف القاعدة: 0xcb47a710 IPSec: قاعدة SPD الخارجية المكتملة، SPI 0xC055290A معرف القاعدة: 0xcdf3cfa0 IPSec: قاعدة تدفق النفق الوارد الجديدة، SPI 0x9E18ACB2 Src addr: 192.168.1.100 قناع SRC: 255.255.255.255 DST: 0.0.0.0 قناع DST: 0.0.0 منافذ SRC أعلى: 0 أقل: صفر التجاهل منافذ DST أعلى: 0 أقل: صفر التجاهل البروتوكول: 0 إستخدام البروتوكول: خطأ SPI: 0x000000 إستخدام SPI: خطأ IPSec: قاعدة تدفق النفق الوارد المكتملة، SPI 0x9E18ACB2 معرف القاعدة: 0xcdf15270 IPSec: قاعدة فك تشفير واردة جديدة، SPI 0x9E18ACB2 Src addr: 64.102.156.87 قناع SRC: 255.255.255.255	

	DST ADDR: 64.102.156.88 قناع DST: 255.255.255.255 منافذ SRC أعلى: 58506 أدنى: 58506 أوبس: يساوي منافذ DST أعلى: 4500 أقل: 4500 أوبس: يساوي البروتوكول: 17 إستخدام البروتوكول: صحيح SPI: 0x000000 إستخدام SPI: خطأ IPSec: قاعدة فك الترميز الداخلية المكتملة، SPI 0x9E18ACB2 معرف القاعدة: 0xce03c2f8 IPSec: قاعدة السماح الواردة الجديدة، SPI 0x9E18ACB2 Src addr: 64.102.156.87 قناع SRC: 255.255.255.255 DST ADDR: 64.102.156.88 قناع DST: 255.255.255.255 منافذ SRC أعلى: 58506 أدنى: 58506 أوبس: يساوي منافذ DST أعلى: 4500 أقل: 4500 أوبس: يساوي البروتوكول: 17 إستخدام البروتوكول: صحيح SPI: 0x000000 إستخدام SPI: خطأ IPSec: قاعدة السماح الواردة المكتملة، SPI 0x9E18ACB2 معرف القاعدة: 0xcf6f58c0 أغسطس 24 11:31:13 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، Pitcher: تم تلقي KEY_UPDATE، spi 0x9e18acb2 24 أغسطس 11:31:13 [تصحيح أخطاء IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، بدء مؤقت إعادة مفاتيح P2: 82080 ثانية. 24 أغسطس 11:31:13 [IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، إضافة مسار ثابت لعنوان العميل: 192.168.1.100	
اكتملت المرحلة الثانية. يقوم كلا الطرفين بالتشفير وفك التشفير الآن.	24 أغسطس 11:31:13 [IKEv1]المجموعة = ipSec، اسم المستخدم = user1، IP = 64.102.156.87، المرحلة 2 المكتملة (msgid=0e83792e)	
بالنسبة لعملاء الأجهزة، يتم تلقي رسالة أخرى حيث	24 أغسطس 11:31:13 [IKEv1]: IP = 10.48.66.23، IKE_Decode تم إستلام الرسالة (msgid=91facca9) مع الحمولات : HDR + التجزئة (8) + (11) Notify) + لا شيء (0) إجمالي الطول : 184	

يرسل العميل معلومات حول نفسه. إذا بحثت بعناية، فيجب عليك العثور على اسم المضيف لعميل EzVPN والبرنامج الذي يتم تشغيله على العميل وموقع البرنامج واسمه	24 أغسطس 11:31:13 [تصحيح أخطاء IKEv1]: المجموعة = EZ، اسم المستخدم = 10.48.66.23 ،cisco، معالجة حمولة التجزئة 24 أغسطس 11:31:13 [تصحيح أخطاء IKEv1]: المجموعة = EZ، اسم المستخدم = 10.48.66.23 ،cisco، معالجة حمل الإعلام 24 أغسطس 11:31:13 [فك تشفير IKEv1]: واصف قديم - الفهرس 1 24 أغسطس 11:31:13 [فك ترميز IKEv1]: 0000: 000000 7534000B 62736e73 2d383731 u4..**bsns-871**.... 0010: **-** 20383731 6973636f 32000943 2d332e75 **3**.u2..**cisco 871** 0020: 32513675 3934331 46484B30 7535000B u5..FHK094412Q6u 0030: 36000932 32383538 39353638 7539009 ..228589568u9..6 0040: 2B666C61 32753300 3136331 31343532 145216312u3.+**fla** 0050: 70736572 61647669 3837302d 73683a63 **sh:c870-advipser** 0060: 76696365 736B392D 6D7A2E31 32342D32 **vicesk9-mz.124-2** 0070: 302E5435 2E62696E **0.T5.bin** 24 أغسطس 11:31:13 [تصحيح أخطاء IKEv1]: المجموعة = EZ، اسم المستخدم = 10.48.66.23 ،Cisco، معالجة تجزئة PSK أغسطس 24 11:31:13 [IKEv1]: المجموعة = EZ، اسم المستخدم = 192.168.1.100 ،Cisco، حجم تجزئة PSK غير متناسق أغسطس 24 11:31:13 [تصحيح أخطاء IKEv1]: المجموعة = EZ، اسم المستخدم = 10.48.66.23 ،Cisco، فشل التحقق من تجزئة PSK!	

التحقق من النفق

ISAKMP

المخرجات من **الأمر sh cry isa sa det** هو:

```
Active SA: 1
(Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey
Total IKE SA: 1

IKE Peer: 10.48.66.23 1
Type : user Role : responder
Rekey : no State : AM_ACTIVE
Encrypt : aes Hash : SHA
```

```
Auth : preshared Lifetime: 86400
                    Lifetime Remaining: 86387
.AM_ACTIVE - aggressive mode is active
```

IPsec

ونظرا لاستخدام بروتوكول رسائل التحكم في الإنترنت (ICMP) لتشغيل النفق، فلم يتم تشغيل سوى رسالة IPsec واحدة فقط. البروتوكول 1 هو ICMP. لاحظ أن قيم SPI تختلف عن تلك التي تم التفاوض عليها في تصحيح الأخطاء. هذا، في الواقع، نفس النفق بعد المرحلة 2 مفتاح.

الإخراج من الأمر **sh crypto ipSec sa** هو:

```
                                        interface: outside
                    Crypto map tag: DYN, seq num: 10, local addr: 10.48.67.14

                      (local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0
                (remote ident (addr/mask/prot/port): (192.168.1.100/255.255.255.255/0/0
                                    current_peer: 10.48.66.23, username: cisco
                                      dynamic allocated peer ip: 192.168.1.100

                                pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5#
                                pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5#
                                    pkts compressed: 0, #pkts decompressed: 0#
               pkts not compressed: 5, #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: 0#

             local crypto endpt.: 10.48.67.14/0, remote crypto endpt.: 10.48.66.23/0
                                path mtu 1500, ipsec overhead 74, media mtu 1500
                                        current outbound spi: C4B9A77C
                                        current inbound spi : EA2B6B15

                                                     :inbound esp sas
                                           (spi: 0xEA2B6B15 (3928714005
                                transform: esp-aes esp-sha-hmac no compression
                                            { ,in use settings ={RA, Tunnel
                                 slot: 0, conn_id: 425984, crypto-map: DYN
                                sa timing: remaining key lifetime (sec): 28714
                                                    IV size: 16 bytes
                                          replay detection support: Y
                                                  :Anti replay bitmap
                                                0x00000000 0x0000003F
                                                     :outbound esp sas
                                           (spi: 0xC4B9A77C (3300501372
                                transform: esp-aes esp-sha-hmac no compression
                                            { ,in use settings ={RA, Tunnel
                                 slot: 0, conn_id: 425984, crypto-map: DYN
                                sa timing: remaining key lifetime (sec): 28714
                                                    IV size: 16 bytes
                                          replay detection support: Y
                                                  :Anti replay bitmap
                                                0x00000000 0x00000001
```

معلومات ذات صلة

- مقالة على موقع IPsec
- أستكشاف أخطاء IPsec وإصلاحها: فهم أوامر تصحيح الأخطاء واستخدامها

- 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).