أستكشاف أخطاء IOS IKEv2 وإصلاحها لشبكة VPN من موقع إلى موقع باستخدام PSKs

المحتويات

المقدمة

يصف هذا المستند تصحيح أخطاء مفتاح الإنترنت الإصدار 2 (IKEv2) على Cisco IOS® عند إستخدام مفتاح غير مشترك (PSK).

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 IOS 15.1(1)T 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 قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

معلومات أساسية

يوفر هذا المستند معلومات حول كيفية ترجمة بعض خطوط تصحيح الأخطاء في تكوين ما.

مسألة أساسية

يختلف تبادل الحزم في IKEv2 جذريا عن تبادل الحزم في IKEv1. في IKEv1 كان هناك تبادل محدد بشكل واضح يتألف من ست (6) حزم مع تبادل في المرحلة الثانية فيما في المرحلة 1 يتكون من ثلاث (3) حزم؛ تبادل IKEv2 متغير. لمزيد من المعلومات حول الفروق وشرح بعد، تبادل الحزم، ارجع مرة أخرى إلى تصحيح أخطاء مستوى البروتوكول وIKEv2 في تبادل الحزم.

تكوين المُوجّه

يسرد هذا القسم التكوينات المستخدمة في هذا المستند.

الموجه 1

```
interface Loopback0
 ip address 192.168.1.1 255.255.255.0
!
interface Tunnel0
 ip address 172.16.0.101 255.255.255.0
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel destination 10.0.0.2
 tunnel protection ipsec profile phse2-prof
!
interface Ethernet0/0
 ip address 10.0.0.1 255.255.255.0

crypto ikev2 proposal PHASE1-prop
 encryption 3des aes-cbc-128
 integrity sha1
 group 2
!
crypto ikev2 policy site-pol
 proposal PHASE1-prop
!
crypto ikev2 keyring KEYRNG
 peer peer1
  address 10.0.0.2 255.255.255.0
  hostname host1
  pre-shared-key local cisco
  pre-shared-key remote cisco
```

```
 !
crypto ikev2 profile IKEV2-SETUP
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local KEYRNG
 lifetime 120
!
crypto ipsec transform-set TS esp-3des esp-sha-hmac
!
crypto ipsec profile phse2-prof
 set transform-set TS
 set ikev2-profile IKEV2-SETUP
!
ip route 0.0.0.0 0.0.0.0 10.0.0.2
ip route 192.168.2.1 255.255.255.255 Tunnel0
```

المجوم 2

```
crypto ikev2 proposal PHASE1-prop
 encryption 3des aes-cbc-128
 integrity sha1
 group 2
!
crypto ikev2 keyring KEYRNG
 peer peer2
  address 10.0.0.1 255.255.255.0
  hostname host2
  pre-shared-key local cisco
  pre-shared-key remote cisco
 !
crypto ikev2 profile IKEV2-SETUP
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local KEYRNG
 lifetime 120
!
crypto ipsec transform-set TS esp-3des esp-sha-hmac
!
!
crypto ipsec profile phse2-prof
 set transform-set TS
 set ikev2-profile IKEV2-SETUP
!
interface Loopback0
 ip address 192.168.2.1 255.255.255.0
!
interface Ethernet0/0
 ip address 10.0.0.2 255.255.255.0
!
interface Tunnel0
 ip address 172.16.0.102 255.255.255.0
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel destination 10.0.0.1
 tunnel protection ipsec profile phse2-prof
!
```

```
ip route 0.0.0.0 0.0.0.0 10.0.0.1
ip route 192.168.1.1 255.255.255.255 Tunnel0
```

استكشاف الأخطاء وإصلاحها

الموجه أخطاء تصحيح

يتم استخدام أوامر تصحيح الأخطاء هذه في هذا المستند:

```
deb crypto ikev2 packet
deb crypto ikev2 internal
```

وصف رسالة الموجه 1 (البادئ)	تصحيح الأخطاء	وصف رسالة الموجه 2 (المستجيب)
يستلم الموجه 1 حزمة طابق قائمة للوصول في التحكم إلى التشفير ل peer ASA 10.0.0.2. بدء إنشاء SA	*نوفمبر 11 20:28:34.003: IKEv2:الحصول على حزمة من المرسل *11 نوفمبر 20:28:34.003: IKEv2:معالجة عنصر خارج قائمة انتظار pak *نوفمبر 11 19:30:34.811: IKEv2: الحصول على المفتاح المضغوط من الخال العنوان 10.0.0.2 *نوفمبر 11:30:34.811: IKEv2:إضافة مرحلة اقتراح 1-prop إلى سياسة مجموعة الأدوات *11 نوفمبر 19:30:34.811: IKEv2:(1): إختيار IKE Profile IKEv2-Setup *بتاريخ 11 نوفمبر 19:30:34.811: تم قبول طلب IKEv2:New IKEV2 *11 نوفمبر 19:30:34.811: IKEv2:زيادة عدد مرات التفاوض الصادرة بمعدل واحد	
أول زوج من الرسائل هو تبادل IKE_SA_INIT. تتفاوض هذه الرسائل على خوارزميات التشفير، الاتصال مدع المتبادل، وتوقم تبادل Diffie-Hellman. التكوين ذي	*نوفمبر 11 19:30:34.811:(معرف IKEv2:(معرف SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=000000000000000 (I) MSGid = 0000000 CurState State: المخلوع وضع حدث: EV_INIT_SA *نوفمبر 11 19:30:34.811: (معرف IKEv2:(معرف SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=000000000000000000000000 CurState: I_BLD_init حدث: EV_GET_IKE_POLICY *نوفمبر 11 19:30:34.811: (معرف IKEv2:(معرف SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=000000000000000 (I) MSGid = 0000000 CurStateLd: I_BLD: MLLLLLL_MLD_init event:EV_SET_POLICY *نوفمبر 11 19:30:34.811: IKEv2:(معرف SA = 1):إعداد	

الصلة: لوكوتورب التشفير CRYPTO ikev2 المقترح المرحلة 1-prop encryption 3des aes- cbc-128 Integrity SHA1 المجموعة 2crypto ikev2 keyRing Peer1 عنوان 10.0.0.2 255.255.255.255.0 hostname host1 مفتاح مشترك مسبقا محلي cisco مشترك مسبقا مفتاح بعيد Cisco	السياسات التي تم تكوينها *نوفمبر 11 19:30:34.811: (معرف IKEv2:(معرف SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000000000 CurState: I_BLD_INIT event: EV_CHK_AUTH4PKI *نوفمبر 11 19:30:34.811: (معرف IKEv2:(معرف SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=00000000000000 (I) MSGid = 0000000 CurStateLd: I_BLD: MLLLLLL_MLD_init event:EV_GEN_DH_KEY *نوفمبر 11 19:30:34.811: (معرف IKEv2:(معرف SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000000000 CurState: I_BLD_init event: EV_NO_EVENT *نوفمبر 11 19:30:34.811: (معرف IKEv2:(معرف SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000000000 CurState: I_BLD_init event: EV_OK_RECD_DH_PUBKEY_RESP *نوفمبر 11 19:30:34.811: IKEv2:(معرف SA = 1):الإجراء: Action_NULL *نوفمبر 11 19:30:34.811: (معرف IKEv2:(معرف SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000000000 CurState: I_BLD_init event: EV_GET_CONFIG_MODE *نوفمبر 11 19:30:34.811: بدء IKEv2:IKEv2 - لا توجد بيانات تكوين لإرسالها في بروتوكول IKE_SA_INIT *نوفمبر 11:30:34.811: لا توجد بيانات تكوين لإرسالها إلى مجموعة الأدوات: *نوفمبر 11 19:30:34.811: (معرف IKEv2:(معرف SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000000000 CurState: I_BLD_init حدث: EV_BLD_MSG *نوفمبر 11 19:30:34.811: IKEv2:إنشاء حمولة محددة للمورد: الحذف بسبب *نوفمبر 11 19:30:34.811: IKEv2:إنشاء حمولة محددة للمورد: (مخصص) *نوفمبر 11 19:30:34.811: IKEv2:Construct Notify Payload: NAT_DETECTION_SOURCE_IP *نوفمبر 11 19:30:34.811: IKEv2:Construct Notify Payload: NAT_DETECTION_DESTINATION_IP	

حزمة IKE_INIT_SA إنشاء البادئ.
يحتوي على: رأس ISAKMP (SPI/الإصدار/العلامات) و SAi1 (خوارزمية التشفير التي يستخدمها بادئ IKE) و KEi
	*في 11 نوفمبر 19:30:34.811: IKEv2:(معرف المدخلة = 1):الحمولة التالية: SA، الإصدار 2.0 نوع Exchange: IKE_SA_INIT، العلامات: معرف رسالة البادئ: 0، الطول: 344
	محتويات الحمولة:
	حمولة SA التالية: KE، محجوزة: 0x0، الطول: 56
	  المقترح الأخير: 0x0، محجوز: 0x0، الطول: 52
	  المقترح: 1، معرف البروتوكول: IKE، حجم SPI: 0، #trans: 5 آخر تحويل: 0x3، محجوز: 0x0: الطول: 8	

(قيمة المفتاح العام DH الخاصة بالبادئ) و N (البادئ Nonce).	النوع: 1، محجوز: 0x0، المعرف: 3DES آخر تحويل: 0x3، محجوز: 0x0: الطول: 12 النوع: 1، محجوز: 0x0، المعرف: AES-CBC آخر تحويل: 0x3، محجوز: 0x0: الطول: 8 النوع: 2، محجوز: 0x0، المعرف: SHA1 آخر تحويل: 0x3، محجوز: 0x0: الطول: 8 النوع: 3، محجوز: 0x0، المعرف: SHA96 آخر تحويل: 0x0، محجوز: 0x0: الطول: 8 النوع: 4، محجوز: 0x0، المعرف: DH_GROUP_1024_MODP/Group 2 الحمولة التالية ل KE:N، محجوز: 0x0، الطول: 136 مجموعة DH: 2، محجوز: 0x0 الحمولة التالية: VID، محجوزة: 0x0، الطول: 24 حمولة VID التالية: VID، محجوز: 0x0، الطول: 23 الحمولة التالية ل VID: NOTIFY، محجوز: 0x0، الطول: 21 NOTIFY(nat_DETECTION_SOURCE_IP) الحمولة التالية: NOTIFY، محجوز: 0x0، الطول: 28 معرف بروتوكول الأمان: IKE، حجم SPI: 0، النوع: NAT_DETECTION_SOURCE_IP NOTIFY(nat_DETECTION_DESTINATION_IP) الحمولة التالية: لا شيء، محجوز: 0x0، الطول: 28 معرف بروتوكول الأمان: IKE، حجم SPI: 0، النوع: NAT_DETECTION_DESTINATION_IP	
—قام البادئ بإرسال IKE_INIT_SA —>		
	*نوفمبر 11 19:30:34.814: IKEv2:الحصول على حزمة من المرسل *11 نوفمبر 19:30:34.814: IKEv2:معالجة عنصر خارج قائمة انتظار pak *بتاريخ 11 نوفمبر 19:30:34.814: تم قبول طلب IKEv2:New IKEV2 *11 نوفمبر 19:30:34.814: IKEv2:زيادة عدد عمليات التفاوض الواردة بمعدل واحد	يتلقى المستجيب IKE_INIT_SA.
	*نوفمبر 11 19:30:34.814: IKEv2:الحمولة التالية: SA، الإصدار 2.0 نوع Exchange: IKE_SA_INIT، العلامات: معرف رسالة البادئ: 0، الطول: 344 محتويات الحمولة: حمولة SA التالية: KE، محجوزة: 0x0، الطول: 56 المقترح الأخير: 0x0، محجوز: 0x0، الطول: 52 المقترح: 1، معرف البروتوكول: IKE، حجم SPI: 0، #trans: 5 آخر تحويل: 0x3، محجوز: 0x0: الطول: 8 النوع: 1، محجوز: 0x0، المعرف: 3DES آخر تحويل: 0x3، محجوز: 0x0: الطول: 12 النوع: 1، محجوز: 0x0، المعرف: AES-CBC	يقوم المستجيب ببدء إنشاء S لهذا النظير.

	آخر تحويل: 0x3، محجوز: 0x0: الطول: 8 النوع: 2، محجوز: 0x0، المعرف: SHA1 آخر تحويل: 0x3، محجوز: 0x0: الطول: 8 النوع: 3، محجوز: 0x0، المعرف: SHA96 آخر تحويل: 0x0، محجوز: 0x0: الطول: 8 النوع: 4، محجوز: 0x0، المعرف: DH_GROUP_1024_MODP/Group 2 حمولة KE التالية: N، محجوزة: 0x0، الطول: 136 مجموعة DH: 2، محجوز: 0x0 الحمولة التالية: VID، محجوزة: 0x0، الطول: 24 *نوفمبر 11 19:30:34.814: الحمولة الخاصة بالمورد IKEv2:Parse: الحمولة التالية من Cisco-DELETE-Reason VID: VID، محجوز: 0x0، الطول: 23 *نوفمبر 11 19:30:34.814: الحمولة الخاصة بالمورد IKEv2:Parse: (مخصصة) الحمولة التالية: إعلام، محجوز: 0x0، الطول: 21 *نوفمبر 11 19:30:34.814: IKEv2:Parse إعلام الحمولة: NAT_DETECTION_SOURCE_IP Notify(NAT_DETECTION_SOURCE_IP) الحمولة التالية: إعلام، محجوز: 0x0، طول: 28 معرف بروتوكول الأمان: IKE، حجم SPI: 0، النوع: NAT_DETECTION_SOURCE_IP *نوفمبر 11 19:30:34.814: IKEv2:Parse إعلام الحمولة: NAT_DETECTION_DESTINATION_IP Notify(NAT_DETECTION_DESTINATION_IP) الحمولة التالية: لا شيء، محجوز: 0x0، الطول: 28 معرف بروتوكول الأمان: IKE، حجم SPI: 0، النوع: NAT_DETECTION_DESTINATION_IP	
	*نوفمبر 11 19:30:34.814:(معرف IKEv2:(معرف SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 0000000 CurStateStateStateStateState: حدث خام: حدث:_RECV_INIT *نوفمبر 11 19:30:34.814: (معرف IKEv2:(معرف SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 0000000 CurStateState: RState: R:Event EV_VERIFY_MSG *نوفمبر 11 19:30:34.814: (معرف IKEv2:(معرف SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 0000000 CurStateState: RState: R:Event EV_INSERT_SA *نوفمبر 11 19:30:34.814: (معرف IKEv2:(معرف SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 0000000	يقوم المستجيب بالتحقق من رسالة IKE_INI ومعالجتها: (1) إختيار مجموعة التشفير من تلك التي يقدمها البادئ (2) حساب مفت يرسل DH الخاص به، و(3) يقوم بحساب قيمة SKEYID والتي يمكن

	CurStateState: RState: R:Event جهن EV_GET_IKE_POLICY *ربمفون 11 19:30:34.814: IKEv2:ةفاضإ دادعإ يضارتفا تاودألا ةعومجم جهن ىلإ حارتقالل *ربمفون 11 19:30:34.814: (فرعم IKEv2:(فرعم SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 0000000 CurStateState: RState: R:Event EV_PROC_MSG *ربمفون 11 19:30:34.814: (فرعم IKEv2:(فرعم SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 0000000 CurState: ثدح R_INIT: EV_DETECT_NAT *ربمفون 11 19:30:34.814: IKEv2:(فرعم SA = 1):مالعإ ةيلمعلل nat فاشتكا *ربمفون 11 19:30:34.814: IKEv2:(فرعم SA = 1):يقوم جلاعم nat فاشتكاب src notify *ربمفون 11 19:30:34.814: IKEv2:(فرعم SA = 1):قباطت ناونعلا نع دعب *ربمفون 11 19:30:34.814: IKEv2:(فرعم SA = 1):فشك NAT مالعإ ةجلاعملل DST *ربمفون 11 19:30:34.814: IKEv2:(فرعم SA = 1):ناونعلا قباطم يلحملا *ربمفون 11 19:30:34.814: IKEv2:(فرعم SA = 1):مل متي روثعلا ىلع NAT *ربمفون 11 19:30:34.814: (فرعم IKEv2:(فرعم SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 0000000 CurState: ثدح R_INIT: ev_chk_config_mode *ربمفون 11 19:30:34.814:(IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 0000000 CurState: RState: R_BLD_IT IT: RTT ثدحلا: EV_SET_POLICY *11 ربمفون 19:30:34.814: IKEv2:(فرعم SA = 1):دادعإ تاسايسلا يتلا مت اهنيوكت *ربمفون 11 19:30:34.814:(IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 0000000 CurState: RState: R_BLD_IT IT: RTT ثدحلا: EV_CHK_AUTH4PKI *ربمفون 11 19:30:34.814:(IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 0000000 CurState: RState: R_BLD_IT IT: RTT ثدحلا: EV_PKI_SSH_OPEN *ربمفون 11 19:30:34.814: IKEv2:(فرعم SA = 1):حتف ةسلج PKI *ربمفون 11:30:34.815: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R)	قاقتشا ةفاك حيتافملا نم ل IKE_SA. متي ريفشت عيمج لئاسرلا يتلا يتأت دعب كلذ اهتقداصمو اهثتساب هذه سوؤر لئاسرلا. متي قاقتشا حيتافملا ةمدختسملا ريفشتلل ةيامحلاو نم لماكتلا نم SKEYID فرعتو مساب: SK_E (ريفشتلا) و SK_A (ةقداصملا) و SK_D متيو اهقاقتشا اهمادختساو قاقتشال داوملا نم ديزملا تيبثت حيتافملا ةصاخلا ب CHILD_SAs، متيو باسح SK_E و SK_A نالصفنم لك اهاجتا. يذ نيوكتلا ةلصلا: crypto ikev2 proposal phase1-prop encryption 3des aes-cbc-128 integrity1 عومجم 2 crypto ikev2 keyRing ريظن 2 ناونع 10.0.0.1 255.255.255.0

	MSGid = 00000000 CurState: RState: R_BLD_TRState IT Event:EV_GEN_DH_KEY
	*ربمفون 11 19:30:34.815: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 0000000 CurState: RState: R_BLD_IT IT: RT ثدحلا: EV_NO_EVENT
	*ربمفون 11:30:34.815: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 00000000 CurState: RState: R_BLD_TRState IT EVENT:EV_OK_RECD_DH_PUBKEY_RESP
	*ربمفون 11 19:30:34.815: IKEv2:(فرعم SA = 1):ءارجإلا: Action_NULL
	*ربمفون 11:30:34.815: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 00000000 CurState: RState: R_BLD_TRState IT Event:EV_GEN_DH_Secret
	*ربمفون 11 19:30:34.822: (فرعم IKEv2:(فرعم SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 0000000 CurState: RState: R_BLD_IT IT CBIثدحلا: EV_NO_EVENT
	*11 ربمفون 19:30:34.822: IKEv2:٪ مت حاتفم ىلع لوصحلا ناونعلاب هيلع طغضلا 10.0.0.1
	*ربمفون 11 19:30:34.822: IKEv2:ةفاضإ دادعإ يضارتفا تاودألا ةعومجم جهن ىلإ حارتقالل
	*11 ربمفون 19:30:34.822: IKEv2:(2): رايتخإ IKE Profile IKEv2-Setup
	*ربمفون 11 19:30:34.822: (فرعم IKEv2:(فرعم SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 0000000 CurState: RState: R_BLD_IT IT CBIثدحلا: EV_OK_RECD_DH_SECRET_RESP
	*ربمفون 11 19:30:34.822: IKEv2:(فرعم SA = 1):ءارجإلا: Action_NULL
	*ربمفون 11:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 0000000 CurState: R_BLD_PLIT Event: EV_GEN_SKEYID
	*11 ربمفون 19:30:34.822: IKEv2:(فرعم SA = 1):ءاشنإ skeyid
	*ربمفون 11 19:30:34.822: (فرعم IKEv2:(فرعم SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 0000000 CurState: RState: R_BLD_IT IT CBIثدحلا: EV_GET_CONFIG_MODE
	*ربمفون 11 19:30:34.822: بيجتسملا IKEv2:IKEv2 - دجوت ال تانايب نيوكت اهلاسرإل يف رادصإلا IKE_SA_INIT
	*ربمفون 11:30:34.822: دجوت ال تانايب نيوكت اهلاسرإل ىلإ
		`hostname host2`
		`pre-shared-key`
		`محلي cisco مشتر`
		`مسبق مفتاح بعي`
		`Cisco`

	مجموعة الأدوات: *نوفمبر 11 19:30:34.822: (معرف IKEv2:(معرف SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 0000000 CurState: RState: R_BLD_IT IT CBIحدث: EV_BLD_MSG *نوفمبر 11 19:30:34.822: IKEv2:إنشاء حمولة محددة للمورد: سبب الحذف *نوفمبر 11 19:30:34.822: IKEv2:إنشاء حمولة محددة للمورد: (مخصص) *نوفمبر 11 19:30:34.822: IKEv2:Construct Notify Payload: NAT_DETECTION_SOURCE_IP *نوفمبر 11 19:30:34.822: IKEv2:Construct Notify Payload: NAT_DETECTION_DESTINATION_IP *نوفمبر 11 19:30:34.822: IKEv2:Construct Notify Payload: HTTP_CERT_LOOKUP_SUPPORTED	
	*نوفمبر 11 19:30:34.822: IKEv2:(معرف SA = 1):الحمولة التالية: SA، الإصدار 2.0 نوع Exchange: IKE_SA_INIT، العلامات: معرف رسالة RESPONDER MSG-RESPONSE: 0، الطول: 449 محتويات الحمولة: حمولة SA التالية: KE، محجوزة: 0x0، الطول: 48 المقترح الأخير: 0x0، محجوز: 0x0، الطول: 44 المقترح: 1، معرف البروتوكول: IKE، حجم SPI: 0، #trans: 4 التحويل الأخير: 0x3، محجوز: 0x0: الطول: 12 النوع: 1، محجوز: 0x0، المعرف: AES-CBC آخر تحويل: 0x3، محجوز: 0x0: الطول: 8 النوع: 2، محجوز: 0x0، المعرف: SHA1 آخر تحويل: 0x3، محجوز: 0x0: الطول: 8 النوع: 3، محجوز: 0x0، المعرف: SHA96 آخر تحويل: 0x0، محجوز: 0x0: الطول: 8 النوع: 4، محجوز: 0x0، المعرف: DH_GROUP_1024_MODP/Group 2 الحمولة التالية ل KE:N، محجوز: 0x0، الطول: 136 مجموعة DH: 2، محجوز: 0x0 الحمولة التالية:VID، محجوزة: 0x0، الطول: 24 حمولة VID التالية: VID، محجوز: 0x0، الطول: 23 الحمولة التالية ل VID: NOTIFY، محجوز: 0x0، الطول: 21 NOTIFY(nat_DETECTION_SOURCE_IP) الحمولة التالية: NOTIFY، محجوز: 0x0، الطول: 28 معرف بروتوكول الأمان: IKE، حجم SPI: 0، النوع: NAT_DETECTION_SOURCE_IP NOTIFY(nat_DETECTION_DESTINATION_IP) الحمولة التالية: certreq، محجوز: 0x0، الطول: 28 معرف بروتوكول الأمان: IKE، حجم SPI: 0، النوع:	2 يقوم الموجه بإنشاء رسالة المستجيب ل IKE_SA_INIT exchange، وال يتم استقبال بواسطة ASA1 تحتوي هذه الحزمة على: ISAKMP Header(SPI/ version/flags) و SAr1(خوارزمية التشفير الت يختارها المستجيب ل IKE) و KEr(قي المفتاح العام DH الخاصة بالمستجيب) Responder Nonce.

	NAT_DETECTION_DESTINATION_IP الحمولة التالية ل CERTREQ: NOTIFY، زوجحم: 0x0، لوطلا: 105 تجزئة ترميز CERT و URL ل PKIX الحمولة التالية NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED): الب، زوجحم: 0x0، لوطلا: 8 معرف بروتوكول الأمان: IKE، مجح SPI: 0، عونلا: HTTP_CERT_LOOKUP_SUPPORTED		
	*نوفمبر 11 19:30:34.822: (معرف IKEv2:(معرف SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 000000 CurState: INIT_DONE event: EV_DONE *في 11 نوفمبر 19:30:34.822: IKEv2:(معرف SA = 1):تم تمكين Cisco DeleteReason Notify *نوفمبر 11 19:30:34.822: (معرف IKEv2:(معرف SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 000000 CurState: INIT_DONE event: EV_CHK4_ROLE *نوفمبر 11:30:34.822: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 0000000 CurState: INIT_DONE event: EV_START_TMR *نوفمبر 11 19:30:34.822: (معرف IKEv2:(معرف SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 0000000 CurState: RState: R_Wait_AUTH الحدث: EV_NO_EVENT *بتاريخ 11 نوفمبر 19:30:34.822: تم قبول طلب IKEv2:NewKev2 *11 نوفمبر 19:30:34.822: IKEv2:زيادة عدد مرات التفاوض الصادرة بمعدل واحد		يرسل الموجه رسالة المستجيب إل الموجه 1.
— IKE_INIT_SA المستجيب أرسل—>			
يستلم الموجه 1 استجابة حزمة IKE_SA_INIT من الموجه 2.	*نوفمبر 11:30:34.823: IKEv2:الحصول على حزمة من المرسل *نوفمبر 11:30:34.823: IKEv2:الحصول على حزمة من المرسل *11 نوفمبر 19:30:34.823: IKEv2:معالجة عنصر خارج	I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MsgID = 0000000 CurState: INIT_DONE Event:EV_START_TMR.	يقوم المستجيب بتشغيل المؤقت لعمل المصادقة.

	راظتنا ةمئاق pak		
يتحقق الموجه 1 من الاستجابة ويعالجها: (1) يتم حساب مفاتيح DH السري للبادئ، و(2) يتم إنشاء Skeyid للبادئ أيضا.	*نوفمبر 11 19:30:34.823: IKEv2:(معرف SA = 1):الحمولة التالية: SA، الإصدار: 2.0 ون Exchange: IKE_SA_INIT، العلامات: معرف رسالة MSG-RESPONSE الخاص بالمستجيب: 0، الطول: 449 محتويات الحمولة: حمولة SA التالية: KE، مجموح: 0x0، الطول: 48 المقترح الأخير: 0x0، مجموح: 0x0، الطول: 44 المقترح: 1، معرف البروتوكول: IKE، مجم SPI: 0، #trans: 4 التحويل الأخير: 0x3، مجموح: 0x0: الطول: 12 النوع: 1، مجموح: 0x0، المعرف: AES-CBC آخر تحويل: 0x3، مجموح: 0x0: الطول: 8 النوع: 2، مجموح: 0x0، المعرف: SHA1 آخر تحويل: 0x3، مجموح: 0x0: الطول: 8 النوع: 3، مجموح: 0x0، المعرف: SHA96 آخر تحويل: 0x0، مجموح: 0x0: الطول: 8 النوع: 4، مجموح: 0x0، المعرف: DH_GROUP_1024_MODP/Group 2 الحمولة التالية ل KE:N، مجموح: 0x0، الطول: 136 مجموعة DH: 2، مجموح: 0x0 الحمولة التالية:VID، مجموح: 0x0، الطول: 24 *نوفمبر 11 19:30:34.823: IKEv2:Parse Vendor Specific Payload: Cisco-DELETE-Reason VID Next Payload: VID، مجموح: 0x0، الطول: 23 *نوفمبر 11 19:30:34.823: IKEv2:تحليل الحمولة الخاصة: بالمورد: (مخصصة) الحمولة التالية: إعلام، مجموح: 0x0، الطول: 21 *نوفمبر 11 19:30:34.823: IKEv2:Parse إعلام الحمولة: NAT_DETECTION_SOURCE_IP Notify(NAT_DETECTION_SOURCE_IP) الحمولة التالية: إعلام، مجموح: 0x0، لوط: 28 معرف بروتوكول الأمان: IKE، مجم SPI: 0، النوع: NAT_DETECTION_SOURCE_IP *نوفمبر 11 19:30:34.824: IKEv2:Parse Notify Payload: NAT_DETECTION_DESTINATION_IP Notify(NAT_DETECTION_DESTINATION_IP) الحمولة التالية: CERTREQ، مجموح: 0x0، الطول: 28 معرف بروتوكول الأمان: IKE، مجم SPI: 0، النوع: NAT_DETECTION_DESTINATION_IP الحمولة التالية ل CERTREQ: NOTIFY، مجموح: 0x0، الطول:		

105
تجزئة ترميز CERT و URL ل PKIX

*نوفمبر 11 19:30:34.824: IKEv2:Parse Notify Payload: HTTP_CERT_LOOKUP_SUPPORTED NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED) الحمولة التالية: ال شيء، محجوز: 0x0، الطول: 8
معرف بروتوكول الأمان: IKE، حجم SPI: 0، النوع: HTTP_CERT_LOOKUP_SUPPORTED

*نوفمبر 11 19:30:34.824: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 0000000 CurState: I_WAIT_INIT الحدث: EV_RECV_INIT
*نوفمبر 11 19:30:34.824: IKEv2:(معرف SA = 1):معالجة رسالة IKE_SA_INIT
*نوفمبر 11 19:30:34.824: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 0000000 CurState: I_PROC_IT IT الحدث: EV_CHK4_NOTIFY
*نوفمبر 11 19:30:34.824: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 0000000 CurState: I_PROC_IT IT الحدث: EV_VERIFY_MSG
*نوفمبر 11 19:30:34.824: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 0000000 CurState: I_PROC_IT IT الحدث: EV_PROC_MSG
*نوفمبر 11 19:30:34.824: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 0000000 CurState: I_PROC_IT IT الحدث: EV_DETECT_NAT
*نوفمبر 11 19:30:34.824: IKEv2:(معرف SA = 1):إعلام اكتشاف nat للعملية
*نوفمبر 11 19:30:34.824: IKEv2:(معرف SA = 1):يقوم معالج nat باكتشاف src notify
*نوفمبر 11 19:30:34.824: IKEv2:(معرف SA = 1):تطابق العنوان عن بعد
*نوفمبر 11:30:34.824: IKEv2:(معرف SA = 1):كشف NAT للمعالجة إعلام DST
*نوفمبر 11 19:30:34.824: IKEv2:(معرف SA = 1):العنوان المحلي مطابق
*نوفمبر 11 19:30:34.824: IKEv2:(معرف SA = 1):لم يتم العثور على NAT
*نوفمبر 11 19:30:34.824: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I)

	MSGid = 0000000 CurState: I_PROC_IT IT الحدث: EV_CHK_NAT_T *نوفمبر 11 19:30:34.824: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 0000000 CurState: I_PROC_IT IT الحدث: EV_CHK_CONFIG_MODE *نوفمبر 11 19:30:34.824: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 0000000 CurState StateState: INIT_DONE event:EV_GEN_DH_SECRET *نوفمبر 11 19:30:34.831: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 000000 CurState: INIT_DONE event: EV_NO_EVENT *نوفمبر 11 19:30:34.831: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 000000 CurState: INIT_DONE event: EV_OK_RECD_DH_SECRET_RESP *نوفمبر 11 19:30:34.831: IKEv2:(معرف SA = 1):إلغاء: Action_NULL *نوفمبر 11 19:30:34.831: (معرف IKEv2:(معرف SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 0000000 CurStateState: INIT_DONE event: EV_GEN_SKEYID *11 نوفمبر 19:30:34.831: IKEv2:(معرف SA = 1):إنشاء skeyid *نوفمبر 11 19:30:34.831: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 000000 CurState: INIT_DONE event: EV_DONE *في 11 نوفمبر 19:30:34.831: IKEv2:(معرف SA = 1):تم تمكين Cisco DeleteReason Notify *نوفمبر 11 19:30:34.831: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 000000 CurState: INIT_DONE event: EV_CHK4_ROLE *نوفمبر 11 19:30:34.831: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 0000000 CurState: I_BLD_AUAUAUTH الحدث: EV_GET_CONFIG_MODE *نوفمبر 11:30:34.831: IKEv2:إرسال بيانات التكوين إلى مجموعة الأدوات *نوفمبر 11 19:30:34.831: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 0000000 CurState: I_BLD_AUAUAUTH الحدث: EV_CHK_EAP	
لدابئ تابدل أدبي	*نوفمبر 11 19:30:34.831: (معرف IKEv2:(معرف SA = 1):SM	

ويقوم IKE_AUTH بإنشاء حمولة المصادقة. تحتوي على: IKE_AUTH حزمة رأس ISAKMP (SPI/ الإصدار/العلامات)، IDi (هوية البادئ)، حمولة المصادقة، SAi2 (بدء مجموعة ل مماثل-SA تحويل المرحلة 2 في IKEv1)، و TSi و TSr (محددات حركة مرور البادئ والمستجيب). إنها تحتوي على عناوين المصدر والوجهة للبادئ والمستجيب على التوالي لإعادة توجيه/استقبال حركة مرور مشفرة. 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. يتم إنشاء أول CHILD_SA لزوج PROXY_ID الذي يطابق حزمة المشغل. التكوين ذي الصلة: `crypto ipSec transform-set TS esp-3des esp-sha-hmac crypto ipSec profile phse2-prof set transform-set ts set ikev2-profile ikev2-setup`	Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 0000000 CurState: I_BLD_AUAUPState: State الحدث:EV_GEN_AUTH *نوفمبر 11 19:30:34.831: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 0000000 CurState: I_BLD_AUAUAUTH الحدث: EV_CHK_AUTH_TYPE *نوفمبر 11 19:30:34.831: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 0000000 CurState: I_BLD_AUAUAUTH الحدث: EV_OK_AUTH_GEN *نوفمبر 11 19:30:34.831: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 0000000 CurState: I_BLD_AUAUAUTH الحدث: EV_SEND_AUTH *نوفمبر 11 19:30:34.831: IKEv2:إنشاء حمولة خاصة بالمورد: Cisco-Granite *نوفمبر 11 19:30:34.831: IKEv2:Build Notify Payload: Initial_CONTACT *نوفمبر 11 19:30:34.831: IKEv2:Construct Notify Payload: SET_WINDOW_SIZE *نوفمبر 11 19:30:34.831: IKEv2:Build Notify Payload: ESP_TFC_NO_SUPPORT *نوفمبر 11 19:30:34.831: IKEv2:Build Notify Payload: non_FIRST_FRAGS محتويات الحمولة: حمولة VID التالية: IDi، محجوزة: 0x0، الطول: 20 الحمولة التالية من IDi:المصادقة، المحجوزة: 0x0، الطول: 12 نوع المعرف: عناوين IPv4، محجوز: 0x0 0x0 حمولة المصادقة التالية: CFG، محجوزة: 0x0، الطول: 28 طريقة المصادقة PSK، محجوزة: 0x0، محجوزة 0x0 الحمولة التالية ل CFG: SA، محجوزة: 0x0، الطول: 309 cfg نوع: cfg_request، محجوز: 0x0، محجوز: 0x0 *11 نوفمبر 19:30:34.831: الحمولة التالية: TSi، محجوزة: 0x0، الطول: 40 المقترح الأخير: 0x0، محجوز: 0x0، الطول: 36 المقترح: 1، معرف البروتوكول: ESP، حجم SPI: 4، #trans: 3 آخر تحويل: 0x3، محجوز: 0x0: الطول: 8 النوع: 1، محجوز: 0x0، المعرف: 3DES آخر تحويل: 0x3، محجوز: 0x0: الطول: 8 النوع: 3، محجوز: 0x0، المعرف: SHA96 آخر تحويل: 0x0، محجوز: 0x0: الطول: 8 النوع: 5، محجوز: 0x0، المعرف: عدم استخدام ESN الحمولة التالية ل TSi: TSr، محجوزة: 0x0، الطول: 24 num of TSs: 1، محجوز 0x0، محجوز 0x0	

	عون TS: TS_IPv4_ADDR_RANGE، فرعم 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: NOTIFY، محجوز: 0x0، الطول: 24 num of TSs: 1، محجوز 0x0، محجوز 0x0 عون TS: TS_IPv4_ADDR_RANGE، فرعم الإصدار: 0، الطول: 16 منفذ البدء: 0 ومنفذ النهاية: 65535 بداية العنوان: 0.0.0.0، نهاية العنوان: 255.255.255.255 NOTIFY(initial_contact) الحمولة التالية: NOTIFY، محجوز: 0x0، الطول: 8 فرعم بروتوكول الأمان: IKE، حجم SPI: 0، النوع: Initial_CONTACT NOTIFY(set_window_size) الحمولة التالية: NOTIFY، محجوز: 0x0، الطول: 12 فرعم بروتوكول الأمان: IKE، حجم spi: 0، النوع: SET_WINDOW_SIZE حمولة NOTIFY(ESP_TFC_NO_SUPPORT) التالية: إعلام، محجوز: 0x0، الطول: 8 فرعم بروتوكول الأمان: IKE، حجم SPI: 0، النوع: ESP_TFC_NO_SUPPORT الحمولة التالية ل NOTIFY(non_first_frags): لا شيء، محجوز: 0x0، الطول: 8 فرعم بروتوكول الأمان: IKE، حجم SPI: 0، النوع: NON_FIRST_FRAGS *نوفمبر 11 19:30:34.832: IKEv2:(فرعم الدخلة (SA) = 1):الحمولة التالية: ENCR، الإصدار: 2.0 نوع الاستبدال: IKE_AUTH، العلامات: فرعم رسالة البادئ: 1، الطول: 556 محتويات الحمولة: الحمولة التالية ل ENCR: VID، محجوز: 0x0، الطول: 528 *نوفمبر 11 19:30:34.833: (فرعم IKEv2:(فرعم SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 0000001 CurState: I_Wait_TM حدث المصادقة: EV_NO_EVENT	
<— إرسال البادئ IKE_AUTH —>		
	*نوفمبر 11:30:34.832: IKEv2:الحصول على حزمة من المرسل *11 نوفمبر 19:30:34.832: IKEv2:معالجة عنصر خارج قائمة انتظار pak *نوفمبر 11 19:30:34.832: IKEv2:(فرعم SA = 1):يحتوي 1 إلى 1 من متوقع؛ 1 MESS_ID على طلب الا *في 11 نوفمبر 19:30:34.832: IKEv2:(فرعم الدخلة = 1):الحمولة التالية: ENCR، الإصدار 2.0 نوع Exchange:	يستلم الموج 2 بيانات المصادقة المستلمة من الموجه 1 ويتحقق منها.

	IKE_AUTH، العلامات: معرف رسالة البادئ: 1، الطول: 556 محتويات الحمولة: *11 نوفمبر 19:30:34.832: IKEv2:تحليل الحمولة الخاصة بالمورد: (CUSTOM) الحمولة التالية: IDi، محجوزة: 0x0، الطول: 20 الحمولة التالية من IDi:المصادقة، المحجوزة: 0x0، الطول: 12 نوع المعرف: عنوان IPv4، محجوز: 0x0 0x0 حمولة المصادقة التالية: CFG، محجوزة: 0x0، الطول: 28 طريقة المصادقة PSK، محجوزة: 0x0، محجوزة 0x0 الحمولة التالية ل CFG: SA، محجوزة: 0x0، الطول: 309 cfg نوع: cfg_request، محجوز: 0x0، محجوز: 0x0 *بتاريخ 11 نوفمبر/تشرين الثاني 19:30:34.832: نوع الجهاز: IP4 DNS داخلي، الطول: 0 *بتاريخ 11 نوفمبر/تشرين الثاني 19:30:34.832: نوع الجهاز: IP4 DNS داخلي، الطول: 0 *بتاريخ 11 نوفمبر/تشرين الثاني 19:30:34.832: نوع الجهاز: اتصال داخلي عبر الشبكة (NBNS) عبر بروتوكول الإنترنت بسرعة 4 ميجابت، الطول: صفر *بتاريخ 11 نوفمبر/تشرين الثاني 19:30:34.832: نوع الجهاز: اتصال داخلي عبر الشبكة (NBNS) عبر بروتوكول الإنترنت بسرعة 4 ميجابت، الطول: صفر *11 نوفمبر 19:30:34.832: نوع الملف: شبكة IP4 الفرعية الداخلية، الطول: 0 *نوفمبر 11 19:30:34.832: نوع التطبيق: الإصدار، الطول: 257 نوع attrib: غير معروف - 28675، الطول: 0 *نوفمبر 11 19:30:34.832: نوع attrib: غير معروف - 28672، الطول: 0 *نوفمبر 11 19:30:34.832: نوع attrib: غير معروف - 28692، الطول: 0 *نوفمبر 11 19:30:34.832: نوع attrib: غير معروف - 28681، الطول: 0 *نوفمبر 11 19:30:34.832: نوع attrib: غير معروف - 28674، الطول: 0 *11 نوفمبر 19:30:34.832: الحمولة التالية:TSi، محجوزة: 0x0، الطول: 40 المقترح الأخير: 0x0، محجوز: 0x0، الطول: 36 المقترح: 1، معرف البروتوكول: ESP، حجم SPI: 4، #trans: 3 آخر تحويل: 0x3، محجوز: 0x0: الطول: 8 النوع: 1، محجوز: 0x0، المعرف: 3DES آخر تحويل: 0x3، محجوز: 0x0: الطول: 8 النوع: 3، محجوز: 0x0، المعرف: SHA96 آخر تحويل: 0x0، محجوز: 0x0: الطول: 8 النوع: 5، محجوز: 0x0، المعرف: عدم إستخدام ESN الحمولة التالية ل TSi: TSr، محجوزة: 0x0، الطول: 24	التكوين ذي الصلة: تشفير AES256 لبروتوك ESP لبروتوكول E IKEv2 IPsec تك ESP SH بروتوكول 1 MD5

	num of TSs: 1، مجحج زوج 0x0، مجحج زوج 0x0 عون TS: TS_IPv4_ADDR_RANGE، فرعم 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، مجحج زوج: 0x0، الطول: 24 num of TSs: 1، مجحج زوج 0x0، مجحج زوج 0x0 عون TS: TS_IPv4_ADDR_RANGE، فرعم الإصدار: 0، الطول: 16 منفذ البدء: 0 ومنفذ النهاية: 65535 بداية العنوان: 0.0.0.0، نهاية العنوان: 255.255.255.255	
	*11 ربمفون 19:30:34.832: (فرعم IKEv2:(فرعم SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 000001 CurState: R_Wait_AUTH الحدث: EV_RECV_AUTH *11 ربمفون 19:30:34.832: (فرعم IKEv2:(فرعم SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 000001 CurState: R_Wait_AUTH الحدث: EV_CHK_NAT_T *11 ربمفون 19:30:34.832: (فرعم IKEv2:(فرعم SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 000001 CurState: R_Wait_AUTH الحدث: EV_PROC_ID *11 ربمفون 19:30:34.832: IKEv2:(فرعم SA = 1):المعلمات الصحيحة المستلمة في فرعم العملية *11 ربمفون 19:30:34.832: (فرعم IKEv2:(فرعم SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 000001 CurState: R_Wait_AUTH الحدث: EV_CHK_IF_PEER_CERT_NEEDS_TO_GET_FOR_PROF_SEL *11 ربمفون 19:30:34.832: (فرعم IKEv2:(فرعم SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 000001 CurState: R_Wait_AUTH الحدث: EV_GET_POLICY_BY_PEERID *11 ربمفون 19:30:34.833: IKEv2:(1): إختيار IKE Profile IKEv2-Setup *11 ربمفون 19:30:34.833: IKEv2: الحصول على المفتاح المضغوط من خلال العنوان 10.0.0.1 *11 ربمفون 19:30:34.833: IKEv2: الحصول على المفتاح المضغوط من خلال العنوان 10.0.0.1 *11 ربمفون 19:30:34.833: IKEv2:إضافة إعداد افتراضي للاقتراح إلى نهج مجموعة الأدوات *11 ربمفون 19:30:34.833: IKEv2:(فرعم SA = 1):إستخدام ملف تعريف IKEv2 'IKEv2-Setup'	يقوم المهاجم 2 بإنشاء الاستجابة لحزمة IKE_AU التي استلمه من المهاجم 1. تحتوي حزمة الاستجابة هذه على: ISAKMP Header(SPI/ version/flags) و IDr(فرعم المستجيب) وحمولة المصادقة و SAr2(بدء SA- similar of the phase 2 transfe set exchange IKEv1) و TSi و TSr(Initiator و Responder Tra Selters). إنها تحتوي على عناوين المصدر والوجهة للبادئ والمستجيب على التوالي لإعادة توجيه/إستقبا حركة مرور مشفرة. يحدد نطاق العناوين أن كل حركة

	*ربمفون 11 19:30:34.833: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 000001 CurState: R_Wait_AUTH ثدحلا: EV_SET_POLICY *ربمفون 11 19:30:34.833: IKEv2:(فرعم SA = 1):دادعإ اهنيوكت مت يتلا تاسايسلا *ربمفون 11 19:30:34.833: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 000001 CurState: R_Wait_AUTH ثدحلا: EV_VERIFY_POLICY_BY_PEERID *ربمفون 11 19:30:34.833: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 000001 CurState: R_Wait_AUTH ثدحلا: EV_CHK_AUTH4EAP *ربمفون 11 19:30:34.833: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 000001 CurState: R_Wait_AUTH ثدحلا: EV_CHK_POLREQEAP *ربمفون 11 19:30:34.833: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 000001 CurState: R_VERIFY_AUTH ثدحلا: EV_CHK_AUTH_TYPE *ربمفون 11 19:30:34.833: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 000001 CurState: R_VERIFY_AUTH ثدحلا: EV_GET_PRESHR_KEY *ربمفون 11 19:30:34.833: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 000001 CurState: R_VERIFY_AUTH ثدحلا: EV_VERIFY_AUTH *ربمفون 11 19:30:34.833: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 000001 CurState: R_VERIFY_AUTH ثدحلا: EV_CHK4_IC *ربمفون 11 19:30:34.833: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 000001 CurState: R_VERIFY_AUTH ثدحلا: EV_CHK_REDIRECT *ربمفون 11 19:30:34.833: IKEv2:(فرعم SA = 1):سيل كانه ةجاح ىلإ ققحتلا نم ةداعإ ،هيجوتلا امم يدؤي ىلإ هيطخت *ربمفون 11 19:30:34.833: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 000001 CurState: R_VERIFY_AUTH ثدحلا: EV_NOTIFY_AUTH_DONE *خيراتب 11 ربمفون 19:30:34.833: مل متي نيوكت ضيوفت	كلذ نم رورملا هيلإو قاطنلا ءاشنإ متي هذه .اهل تاونق تاملعملا ةقباطم تاملعملل الت تم اهيقلت مت ASA1.

مجموعة IKEv2:AAA
*في 11 نوفمبر 19:30:34.833: لم يتم تكوين تفويض
مستخدم IKEv2:AAA
*نوفمبر 11 19:30:34.833: (IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R)
MSGid = 000001 CurState: R_VERIFY_AUTH الحدث:
EV_CHK_CONFIG_MODE
*نوفمبر 11 19:30:34.833: (IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R)
MSGid = 000001 CurState: R_VERIFY_AUTH الحدث:
EV_SET_RECD_CONFIG_MODE
*نوفمبر 11 19:30:34.833: IKEv2:بيانات التكوين
المستلمة من مجموعة الأدوات:
*نوفمبر 11 19:30:34.833: (IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R)
MSGid = 000001 CurState: R_VERIFY_AUTH الحدث:
EV_PROC_SA_TS
*نوفمبر 11 19:30:34.833: (IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R)
MSGid = 000001 CurState: R_VERIFY_AUTH الحدث:
EV_GET_CONFIG_MODE
*نوفمبر 11 19:30:34.833: IKEv2:الرد في تكوين أخطأ
*نوفمبر 11:30:34.833: لا توجد بيانات تكوين للإرسال إلى
مجموعة الأدوات:
*نوفمبر 11:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R)
MSGid = 000001 CurState: R_BLD_AUTH الحدث:
EV_MY_AUTH_METHOD
*نوفمبر 11:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R)
MSGid = 000001 CurState: R_BLD_AUTH الحدث:
EV_GET_PRESHR_KEY
*نوفمبر 11:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R)
MSGid = 000001 CurState: R_BLD_AUTH الحدث:
EV_GEN_AUTH
*نوفمبر 11:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R)
MSGid = 000001 CurState: R_BLD_AUTH الحدث:
EV_CHK4_SIGN
*نوفمبر 11:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R)
MSGid = 000001 CurState: R_BLD_AUTH الحدث:
EV_OK_AUTH_GEN
*نوفمبر 11:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA:

	I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 000001 CurState: R_BLD_AUTH الحدث: EV_SEND_AUTH *نوفمبر 11 19:30:34.833: IKEv2:إنشاء حمولة خاصة بالمورد: Cisco-Granite *نوفمبر 11 19:30:34.833: IKEv2:Construct Notify Payload: SET_WINDOW_SIZE *نوفمبر 11 19:30:34.833: IKEv2:Build Notify Payload: ESP_TFC_NO_SUPPORT *نوفمبر 11 19:30:34.833: IKEv2:Build Notify Payload: non_FIRST_FRAGS	
	*نوفمبر 11 19:30:34.833: IKEv2:(معرف المدخل (SA) = 1):الحمولة التالية: ENCR، الإصدار 2.0 Exchange type: IKE_AUTH، العلامات: معرف رسالة MSG-RESPONSE الخاص بالمستجيب: 1، الطول: 252 محتويات الحمولة: حمولة ENCR التالية: VID، محجوزة: 0x0، الطول: 224 *نوفمبر 11 19:30:34.833: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 000001 CurState: AUTH_DONE event: EV_موافق *نوفمبر 11 19:30:34.833: IKEv2:(معرف SA = 1):الإجراء: Action_NULL *نوفمبر 11 19:30:34.833: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 000001 CurState: AUTH_DONE event: EV_PKI_SSH_CLOSE *نوفمبر 11 19:30:34.833: IKEv2:(معرف SA = 1):إغلاق جلسة PKI *نوفمبر 11 19:30:34.833: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 000001 CurState: AUTH_DONE event: EV_UPDATE_CAC_STATS *نوفمبر 11 19:30:34.833: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 000001 CurState: AUTH_DONE event:EV_INSERT_IKE *نوفمبر 11 19:30:34.834: IKEv2:Store MIB index ikev2 1، النظام الأساسي 60 *نوفمبر 11 19:30:34.834: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 000001 CurState: AUTH_DONE: حدث: EV_GEN_LOAD_IPsec *نوفمبر 11 19:30:34.834: IKEv2:(معرف SA = 1):تم وضع الطلب غير المتزامن في قائمة الانتظار	يرسل المستجيب الاستجابة ل IKE_AUTH.

	*نوفمبر 11 19:30:34.834: IKEv2:(معرف SA = 1): *نوفمبر 11 19:30:34.834: (معرف IKEv2:(معرف SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 000001 CurState: AUTH_DONE الحدث: EV_NO_EVENT		
<—أرسل المستجيب IKE_AUTH—			
يستلم البادئ إستجابة من المستجيب.	*نوفمبر 11 19:30:34.834: IKEv2:الحصول على حزمة من المرسل *11 نوفمبر 19:30:34.834: IKEv2:معالجة عنصر خارج قائمة انتظار pak	*نوفمبر 11 19:30:34.840: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 000001 CurState: AUTH_DONE event: EV_OK_RECD_LOAD_IPsec *نوفمبر 11 19:30:34.840: IKEv2:(معرف SA = 1):الإجراء: Action_NULL *نوفمبر 11 19:30:34.840: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 000001 CurState: AUTH_DONE event: EV_START_ACCT *نوفمبر 11 19:30:34.840: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 000001 CurState: AUTH_DONE event: EV_CHECK_DUPE *نوفمبر 11 19:30:34.840: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 000001 CurState: AUTH_DONE event: EV_CHK4_ROLE	موقي المستجيب بإدراج إدخال ف SAD.
يتحقق الموجه 1 من بيانات المصادقة	*نوفمبر 11 19:30:34.834: IKEv2:(معرف الخدمة (SA) =		

الموجودة في هذه الحزمة ويعالجها. يدخل مسجاح تخديد 1 هذا sa داخل هو حزين.	1):الحمولة التالية: ENCR، الإصدار: 2.0 نوع الاستبدال: IKE_AUTH، العلامات: معرف رسالة المستجيب MSG-RESPONSE: 1، الطول: 252 محتويات الحمولة: *نوفمبر 11 19:30:34.834: الحمولة الخاصة بالمورد IKEv2:Parse: (CUSTOM) الحمولة التالية: IDr، محجوزة: 0x0، الطول: 20 الحمولة التالية: المصادقة، المحجوزة: 0x0، الطول: 12 نوع المعرف: عنوان IPv4، محجوز: 0x0 0x0 الحمولة التالية للمصادقة: SA، محجوزة: 0x0، الطول: 28 طريقة المصادقة PSK، محجوزة: 0x0، محجوزة 0x0 حمولة SA التالية: TSi، محجوزة: 0x0، الطول: 40 المقترح الأخير: 0x0، محجوز: 0x0، الطول: 36 المقترح: 1، معرف البروتوكول: ESP، حجم SPI: 4، #trans: 3 آخر تحويل: 0x3، محجوز: 0x0: الطول: 8 النوع: 1، محجوز: 0x0، المعرف: 3DES آخر تحويل: 0x3، محجوز: 0x0: الطول: 8 النوع: 3، محجوز: 0x0، المعرف: SHA96 آخر تحويل: 0x0، محجوز: 0x0: الطول: 8 النوع: 5، محجوز: 0x0، المعرف: عدم إستخدام ESN الحمولة التالية ل TSi: TSr، 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 *نوفمبر 11 19:30:34.834: IKEv2:Parse إعلام الحمولة: SET_WINDOW_SIZE NOTIFY(SET_WINDOW_SIZE) الحمولة التالية: إعلام، محجوز: 0x0، طول: 12 معرف بروتوكول الأمان: IKE، حجم spi: 0، النوع: SET_WINDOW_SIZE *نوفمبر 11 19:30:34.834: IKEv2:Parse Notify Payload: ESP_TFC_NO_SUPPORT Notify(ESP_TFC_NO_SUPPORT) الحمولة التالية: Notify، محجوز: 0x0، طول: 8 معرف بروتوكول الأمان: IKE، حجم SPI: 0، النوع: ESP_TFC_NO_SUPPORT	

	*نوفمبر 11 19:30:34.834: IKEv2:Parse Notify Payload: NON_FIRST_FRAGS Notify(NON_FIRST_FRAGS) الحمولة التالية: ال شيء، محجوز: 0x0، الطول: 8 معرف بروتوكول الأمان: IKE، حجم SPI: 0، النوع: NON_FIRST_FRAGS *نوفمبر 11 19:30:34.834: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 000001 CurState: I_Wait_AUTH الحدث:EV_RECV_AUTH *نوفمبر 11 19:30:34.834: IKEv2:(معرف SA = 1):الإجراء: Action_NULL *نوفمبر 11 19:30:34.834: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 000001 CurState: I_PROC_AUTH_AUAUAUTH الحدث: EV_CHK4_NOTIFY *نوفمبر 11 19:30:34.834: (معرف IKEv2:(معرف SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 000001 CurState: I_PROC_AUI_AUI الحدث:EV_PROC_MSG *نوفمبر 11 19:30:34.834: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 000001 CurState: I_PROC_AUTH_AUAUAUTH الحدث: EV_CHK_IF_PEER_CERT_NEEDS_TO_GET_FOR_PROF_SEL *نوفمبر 11 19:30:34.834: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 000001 CurState: I_PROC_AUTH_AUAUAUTH الحدث: EV_GET_POLICY_BY_PEERID *تشرين الثاني 11:30:34.834: IKEv2:إضافة مشروع المرحلة 1-prop إلى سياسة مجموعة الأدوات *11 نوفمبر 19:30:34.834: IKEv2:(معرف SA = 1):إستخدام IKEv2 "إعداد IKEv2 ملف تعريف *نوفمبر 11 19:30:34.834: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 000001 CurState: I_PROC_AUTH_AUAUAUTH الحدث: EV_VERIFY_POLICY_BY_PEERID *نوفمبر 11 19:30:34.834: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 000001 CurState: I_PROC_AUTH_AUAUAUTH الحدث: EV_CHK_AUTH_TYPE *نوفمبر 11 19:30:34.834: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 000001 CurState: I_PROC_AUTH_AUAUAUTH الحدث: EV_GET_PRESHR_KEY	

*ربمفون 11:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 000001 CurState: I_PROC_AUC_AUA الحدث:EV_VERIFY_AUTH
*ربمفون 11 19:30:34.835: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 000001 CurState: I_PROC_AUTH الحدث: EV_CHK_EAP
*ربمفون 11:30:34.835: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 000001 CurState: I_PROC_AUC_AUA الحدث:EV_NOTIFY_AUTH_DONE
*ربمفون 11 خيراتب 19:30:34.835: لم يتم تكوين تفويض مجموعة IKEv2:AAA
*ربمفون 11 في 19:30:34.835: لم يتم تكوين تفويض مستخدم IKEv2:AAA
*ربمفون 11 19:30:34.835: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 000001 CurState: I_PROC_AUTH الحدث: EV_CHK_CONFIG_MODE
*ربمفون 11 19:30:34.835: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 000001 CurState: I_PROC_AUTH الحدث: EV_CHK4_IC
*ربمفون 11 19:30:34.835: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 000001 CurState: I_PROC_AUTH الحدث: EV_CHK_IKE_ONLY
*ربمفون 11 19:30:34.835: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 000001 CurState: I_PROC_AUTH الحدث: EV_PROC_SA_TS
*ربمفون 11 19:30:34.835: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 000001 CurState: AUTH_DONE event: EV_قفاوم
*ربمفون 11 19:30:34.835: IKEv2:(فرعم SA = 1):اإلجراء: Action_NULL
*ربمفون 11 19:30:34.835: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 000001 CurState: AUTH_DONE event: EV_PKI_SSH_CLOSE
*ربمفون 11 19:30:34.835: IKEv2:(فرعم SA = 1):إغالق جلسة PKI
*ربمفون 11 19:30:34.835: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I)

MSGid = 000001 CurState: AUTH_DONE event:
EV_UPDATE_CAC_STATS
*ربمفون 11 19:30:34.835: (IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I)
MSGid = 000001 CurState: AUTH_DONE event:
EV_INSERT_IKE
*ربمفون 11 19:30:34.835: IKEv2:Store MIB index ikev2 1،
60 يساسألا ماظنلا
*ربمفون 11 19:30:34.835: (IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I)
MSGid = 000001 CurState: AUTH_DONE event:
EV_GEN_LOAD_IPsec
*ربمفون 11 19:30:34.835: IKEv2:(مرعف SA = 1):عضو مت
راظنتالا ةمئاق يف المتزامن ريغ للطلب

*ربمفون 11 19:30:34.835: IKEv2:(مرعف SA = 1):
*ربمفون 11 19:30:34.835: (IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I)
MSGid = 000001 CurState: AUTH_DONE event:
EV_NO_EVENT
*بتاريخ 11 ربمفون 19:30:34.835: مت إستهلاك رسالة
IKEv2:KMI مقر 8. عارجإ يأ ذاختإ متي مل.
*بتاريخ 11 ربمفون 19:30:34.835: مت إستهلاك رسالة
IKEv2:KMI مقر 12. عارجإ يأ ذاختإ متي مل.
*ربمفون 11 19:30:34.835: IKEv2:ال دجوت بيانات لإرسالها
في مجموعة تكوين الوضع.
*ربمفون 11 19:30:34.841: IKEv2:إضافة مؤشر البداية
0x8000002 المرتبط ب SPI 0x9506D414 لجلسة العميل 8

*ربمفون 11 19:30:34.841: (IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I)
MSGid = 000001 CurState: AUTH_DONE event:
EV_OK_RECD_LOAD_IPsec
*ربمفون 11 19:30:34.841: IKEv2:(مرعف SA = 1):الإجراء:
Action_NULL
*ربمفون 11 19:30:34.841: (IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I)
MSGid = 000001 CurState: AUTH_DONE event:
EV_START_ACCT
*ربمفون 11 19:30:34.841: IKEv2:(مرعف SA = 1):المحاسبة
غير مطلوبة
*ربمفون 11 19:30:34.841: (IKEv2:(SA ID = 1):SM Trace-> SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I)
MSGid = 000001 CurState: AUTH_DONE event:
EV_CHECK_DUPE

	*ربمفون 11 19:30:34.841:(فرعم) IKEv2:(فرعم SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 000001 CurState: AUTH_DONE الحدث: EV_CHK4_ROLE		
النفق موجود في الحالة والبادئ showREADY.	*ربمفون 11 19:30:34.841:(فرعم) IKEv2:(فرعم SA = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 000001 CurState: READYE vent: EV_CHK_IKE_ONLY *ربمفون 11 19:30:34.841: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (I) MSGid = 000001 CurState: READY event:_F i_ok	*ربمفون 11 19:30:34.840: IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B r_SPI=F94020DD8CB4B9C4 (R) MSGid = 0000001 CurStateStateState: Ready الحدث: EV_R_OK *ربمفون 11 19:30:34.840: (IKEv2:(SA ID = 1):SM Trace-> SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4 (R) MSGid = 000001 CurState: READY event: EV:_ID no_event	النفق فوق المستجيب. يظهر نفق المستجيب ع قبل البادئ.

تصحيح أخطاء CHILD_SA

يتألف هذا التبادل من زوج من طلب/إستجابة واحدة وتمت الإشارة إليه كمرحلة 2 من التبادل في IKEv1. ويمكن البدء في هذه العملية من الخلال أي من طرفي IKE_SA بعد اكتمال عمليات التبادل الأولية.

وصف رسالة Child_SA للموجه 1	تصحيح الأخطاء	وصف رسالة Child_ للموجه 2
يبدأ الموجه 1 تبادل CHILD_SA. هذا هو طلب CREATE_CHILD_SA. عادة CHILD_SA تحتوي حزمة على: • SA HDR (نوع version.flags/exchange) • nonce ni (إختياري): إذا تم إنشاء CHILD_SA كجزء من التبادل الأولي، فيجب عدم إرسال حمولة KE (ثانية مرة واحدة)	*نوفمبر 11:31:35.873: IKEv2:الحصول على حزمة من المرسل *نوفمبر 11:31:35.873: IKEv2:معالجة عنصر خارج pak انتظار قائمة *نوفمبر 11 19:31:35.873: IKEv2:(معرف SA = 2):يحتوي الطلب على MESS_ID 3، متوقع 3 إلى 7 *نوفمبر 11 19:31:35.873: IKEv2:(معرف الخدمة = 2):الحمولة التالية: ENCR، الإصدار 2.0 نوع Exchange: CREATE_CHILD_SA، العلامات: معرف	

• حمولة SA • KEi (مفتاح إختياري): بلط يوتحي نأ نكمي CREATE_CHILD_SA إختياريا ىلع حمولة KE لدابتل DH إضافي لتمكين ضمانات أقوى لإعادة توجيه سرية CHILD_SA. إذا كان SA يتضمن عرض مجموعات DH مختلفة، يجب أن يكون KEi عنصرا من المجموعة التي يتوقع البادئ أن يقبلها المستجيب. في حالة تخمينه بشكل خاطئ، يفشل تبادل CREATE_CHILD_SA، ويتعين عليه إعادة المحاولة باستخدام KEi مختلف • N(إعلام الحمولة الاختيارية). يتم استخدام حمولة الإعلام لإرسال بيانات المعلومات، مثل حالات الخطأ وانتقالات الحالة، إلى نظير IKE. يمكن أن تظهر حمولة الإعلام في رسالة إستجابة (تحدد عادة سبب رفض طلب)، في Exchange للمعلومات (للإبلاغ عن خطأ ليس في طلب IKE)، أو في أي رسالة أخرى للإشارة إلى قدرات المرسل أو لتعديل معنى الطلب.إذا كان هذا التبادل CREATE_CHILD_SA يعيد تكوين SA موجود بخلاف IKE_SA،	رسالة البادئ: 3، الطول: 396 حمولة المحتويات: حمولة SA التالية: N، محجوزة: 0x0، الطول: 152 المقترح الأخير: 0x0، محجوز: 0x0، الطول: 148 المقترح: 1، معرف البروتوكول: IKE، حجم SPI: 8، #trans: 15 تحويل أخير: 0x3، محجوز: 0x0: الطول: 12 النوع: 1، محجوز: 0x0، المعرف: AES-CBC آخر تحويل: 0x3، محجوز: 0x0: الطول: 12 النوع: 1، محجوز: 0x0، المعرف: AES-CBC آخر تحويل: 0x3، محجوز: 0x0: الطول: 12 النوع: 1، محجوز: 0x0، المعرف: AES-CBC آخر تحويل: 0x3، محجوز: 0x0: الطول: 8 النوع: 2، محجوز: 0x0، المعرف: SHA512 آخر تحويل: 0x3، محجوز: 0x0: الطول: 8 النوع: 2، محجوز: 0x0، المعرف: SHA384 آخر تحويل: 0x3، محجوز: 0x0: الطول: 8 النوع: 2، محجوز: 0x0، المعرف: SHA256 آخر تحويل: 0x3، محجوز: 0x0: الطول: 8 النوع: 2، محجوز: 0x0، المعرف: SHA1 آخر تحويل: 0x3، محجوز: 0x0: الطول: 8 النوع: 2، محجوز: 0x0، المعرف: MD5 آخر تحويل: 0x3، محجوز: 0x0: الطول: 8 النوع: 3، محجوز: 0x0، المعرف: SHA512 آخر تحويل: 0x3، محجوز: 0x0: الطول: 8 النوع: 3، محجوز: 0x0، المعرف: SHA384 آخر تحويل: 0x3، محجوز: 0x0: الطول: 8 النوع: 3، محجوز: 0x0، المعرف: SHA256 آخر تحويل: 0x3، محجوز: 0x0: الطول: 8 النوع: 3، محجوز: 0x0، المعرف: SHA96 آخر تحويل: 0x3، محجوز: 0x0: الطول: 8 النوع: 3، محجوز: 0x0، المعرف: MD596 آخر تحويل: 0x3، محجوز: 0x0: الطول: 8 النوع: 4، محجوز: 0x0، المعرف: DH_GROUP_1536_MODP/Group 5 آخر تحويل: 0x0، محجوز: 0x0: الطول: 8 النوع: 4، محجوز: 0x0، المعرف: DH_GROUP_1024_MODP/Group 2 N الحمولة التالية: KE، محجوزة: 0x0، الطول: 24 حمولة KE التالية: الإعلام، محجوز: 0x0، الطول: 136 مجموعة DH: 2، محجوز: 0x0 *نوفمبر 11 19:31:35.874: IKEv2:Parse Notify Payload: SET_WINDOW_SIZE	

ةلومحم ددحت نأ بجيف N الرائدة نم النوع REKEY_SA التي متي إعادة تكوينها. إذا مل يقم لدابت CREATE_CHILD_SA اذه ةداعإب نيوكت SA موجود، فيجب فذح ةلومحم N.	NOTIFY(SET_WINDOW_SIZE) الحمولة التالية: ال شيء، مجحز: 0x0، الطول: 12 معرف بروتوكول الأمان: IKE، مجح spi: 0، النوع: SET_WINDOW_SIZE *في 11 نوفمبر 19:31:35.874: IKEv2:(معرف SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MSGid = 000003 CurState: Ready Event:_RECV_CREATE_CHILD *نوفمبر 11:31:35.874: IKEv2:(معرف SA = 2):الإجراء: Action_NULL *نوفمبر 11 19:31:35.874: (معرف IKEv2: (معرف SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MSGid = 000003 CurState: حدث CHILD_R_INIT:_RECV_CREATE_CHILD *نوفمبر 11:31:35.874: IKEv2:(معرف SA = 2):الإجراء: Action_NULL *نوفمبر 11 19:31:35.874: (معرف IKEv2: (معرف SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MSGid = 000003 CurState: حدث CHILD_R_INIT:_verify_msg *نوفمبر 11 19:31:35.874: (معرف IKEv2: (معرف SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MSGid = 000003 CurState: حدث CHILD_R_INIT:_chk_cc_type *نوفمبر 11 19:31:35.874: (معرف IKEv2: (معرف SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MSGid = 000003 CurState: CHILD_R_IKE حدث: EV_Rekey_IKESA *نوفمبر 11 19:31:35.874: (معرف IKEv2: (معرف SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MSGid = 000003 CurState: حدث CHILD_R_IKE:_GET_IKE_POLICY *11 نوفمبر 19:31:35.874: IKEv2:٪ الحصول على	

	مفتاح مت الضغط عليه بالعنوان 10.0.0.2 *11 نوفمبر 19:31:35.874: IKEv2: الحصول على العنوان 10.0.0.2 المفتاح المضغوط من خلال *نوفمبر 11:31:35.874: IKEv2:إضافة مرحلة اقتراح 1-دعم إلى مجموعة سياسة الأدوات *11 نوفمبر 19:31:35.874: IKEv2:(معرف SA = 2):استخدام ملف تعريف IKEv2 "إعداد IKEv2 *نوفمبر 11 19:31:35.874: (معرف IKEv2: (معرف SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MSGid = 000003 CurState: حدث CHILD_R_IKE:_proc_msg *نوفمبر 11 19:31:35.874: (معرف IKEv2: (معرف SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MSGid = 000003 CurState: حدث CHILD_R_IKE:_set_policy *11 نوفمبر 19:31:35.874: IKEv2:(معرف SA = 2):إعداد السياسات التي تم تكوينها *نوفمبر 11 19:31:35.874: (معرف IKEv2: (معرف SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MSGid = 000003 CurState: CHILD_R_BLD_MSG الحدث: EV_GEN_DH_KEY *نوفمبر 11 19:31:35.874: (معرف IKEv2: (معرف SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MSGid = 000003 CurState: CHILD_R_BLD_MSG الحدث: EV_NO_EVENT *نوفمبر 11 19:31:35.874: (معرف IKEv2: (معرف SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MSGid = 000003 CurState: CHILD_R_BLD_MSG الحدث: EV_OK_RECD_DH_PUBKEY_RESP *نوفمبر 11:31:35.874: IKEv2:(معرف SA = 2):الإجراء: Action_NULL *نوفمبر 11 19:31:35.874: (معرف IKEv2: (معرف SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MSGid = 000003 CurState: CHILD_R_BLD_MSSSSB g event:EV_GEN_DH_Secret	

	*نوفمبر 11 19:31:35.881: (معرف IKEv2: (معرف SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MSGid = 000003 CurState: CHILD_R_BLD_MSG الحدث: EV_NO_EVENT *نوفمبر 11 19:31:35.882: (معرف IKEv2: (معرف SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MSGid = 000003 CurState: CHILD_R_BLD_MSG الحدث: EV_OK_RECD_DH_SECRET_RESP *نوفمبر 11 11:31:35.882: IKEv2:(معرف SA = 2):الإجراء: Action_NULL *نوفمبر 11 19:31:35.882: (معرف IKEv2: (معرف SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MSGid = 000003 CurState: CHILD_R_BLD_MSG الحدث: EV_BLD_MSG *نوفمبر 11 19:31:35.882: IKEv2:ConstructNotify Payload: SET_WINDOW_SIZE محتويات الحمولة: حمولة SA التالية: N، مجموعة: 0x0، الطول: 56 المقترح الأخير: 0x0، مجموع: 0x0، الطول: 52 المقترح: 1، معرف البروتوكول: IKE، مجم SPI: 0x0: مجموع: 0x3، الأخير للتحويل: 4 #trans: 8، الطول: 12 النوع: 1، مجموع: 0x0، المعرف: AES-CBC آخر تحويل: 0x3، مجموع: 0x0: الطول: 8 النوع: 2، مجموع: 0x0، المعرف: SHA1 آخر تحويل: 0x3، مجموع: 0x0: الطول: 8 النوع: 3، مجموع: 0x0، المعرف: SHA96 آخر تحويل: 0x0، مجموع: 0x0: الطول: 8 النوع: 4، مجموع: 0x0، المعرف: DH_GROUP_1024_MODP/Group 2 N الحمولة التالية: KE، مجموعة: 0x0، الطول: 24 حمولة KE التالية: الإعلام، مجموع: 0x0، الطول: 136 مجموعة DH: 2، مجموع: 0x0 Notify(set_window_size) الحمولة التالية: ال: 12 الطول، 0x0: مجموع، عيش معرف بروتوكول الأمان: IKE، مجم spi: 0، النوع: SET_WINDOW_SIZE	

	*نوفمبر 11 19:31:35.869: IKEv2:(معرف SA = 2):الحمولة التالية: ENCR، الإصدار: 2.0 نوع Exchange: CREATE_CHILD_SA، العلامات:معرف رسالة البادئ: 2، الطول: 460 محتويات الحمولة: الحمولة التالية ل ENCR: SA، محجوزة: 0x0، الطول: 432 *نوفمبر 11:31:35.873: IKEv2:Build Notify Payload: SET_WINDOW_SIZE محتويات الحمولة: حمولة SA التالية: N، محجوزة: 0x0، الطول: 152 المقترح الأخير: 0x0، محجوز: 0x0، الطول: 148 المقترح: 1، معرف البروتوكول: IKE، حجم SPI: 8، #trans: 15 تحويل أخير: 0x3، محجوز: 0x0: الطول: 12 النوع: 1، محجوز: 0x0، المعرف: AES-CBC آخر تحويل: 0x3، محجوز: 0x0: الطول: 12 النوع: 1، محجوز: 0x0، المعرف: AES-CBC آخر تحويل: 0x3، محجوز: 0x0: الطول: 12 النوع: 1، محجوز: 0x0، المعرف: AES-CBC آخر تحويل: 0x3، محجوز: 0x0: الطول: 8 النوع: 2، محجوز: 0x0، المعرف: SHA512 آخر تحويل: 0x3، محجوز: 0x0: الطول: 8 النوع: 2، محجوز: 0x0، المعرف: SHA384 آخر تحويل: 0x3، محجوز: 0x0: الطول: 8 النوع: 2، محجوز: 0x0، المعرف: SHA256 آخر تحويل: 0x3، محجوز: 0x0: الطول: 8 النوع: 2، محجوز: 0x0، المعرف: SHA1 آخر تحويل: 0x3، محجوز: 0x0: الطول: 8 النوع: 2، محجوز: 0x0، المعرف: MD5 آخر تحويل: 0x3، محجوز: 0x0: الطول: 8 النوع: 3، محجوز: 0x0، المعرف: SHA512 آخر تحويل: 0x3، محجوز: 0x0: الطول: 8 النوع: 3، محجوز: 0x0، المعرف: SHA384 آخر تحويل: 0x3، محجوز: 0x0: الطول: 8 النوع: 3، محجوز: 0x0، المعرف: SHA256 آخر تحويل: 0x3، محجوز: 0x0: الطول: 8 النوع: 3، محجوز: 0x0، المعرف: SHA96 آخر تحويل: 0x3، محجوز: 0x0: الطول: 8 النوع: 3، محجوز: 0x0، المعرف: MD596 آخر تحويل: 0x3، محجوز: 0x0: الطول: 8 النوع: 4، محجوز: 0x0، المعرف: DH_GROUP_1536_MODP/Group 5 آخر تحويل: 0x0، محجوز: 0x0: الطول: 8 النوع: 4، محجوز: 0x0، المعرف:	يتم تلقي هذه الحزمة بواسطة الموجه 2.

	DH_GROUP_1024_MODP/Group 2 N الحمولة التالية: KE، مججوزة: 0x0، الطول: 24 الحمولة التالية ل KE: الإعلام، مججوز: 0x0، الطول: 136 مجموعة DH: 2، مججوز: 0x0 Notify(set_window_size) الحمولة التالية: ال شيء، مججوز: 0x0، الطول: 12 معرف بروتوكول الأمان: IKE، حجم spi: 0، النوع: SET_WINDOW_SIZE	
	*نوفمبر 11 19:31:35.882: IKEv2:(معرف SA = 2):الحمولة التالية: ENCR، الإصدار: 2.0 نوع Exchange: CREATE_CHILD_SA، العلامات: معرف الرسالة MSG-RESPONSE الخاصبالمستجيب: 3، الطول: 300 محتويات الحمولة: حمولة SA التالية: N، مججوزة: 0x0، الطول: 56 المقترح الأخير: 0x0، مججوز: 0x0، الطول: 52 المقترح: 1، معرف البروتوكول: IKE، حجم SPI: 8، #trans: 4 التحويل الأخير: 0x3، مججوز: 0x0: الطول: 12 النوع: 1، مججوز: 0x0، المعرف: AES-CBC آخر تحويل: 0x3، مججوز: 0x0: الطول: 8 النوع: 2، مججوز: 0x0، المعرف: SHA1 آخر تحويل: 0x3، مججوز: 0x0: الطول: 8 النوع: 3، مججوز: 0x0، المعرف: SHA96 آخر تحويل: 0x0، مججوز: 0x0: الطول: 8 النوع: 4، مججوز: 0x0، المعرف: DH_GROUP_1024_MODP/Group 2 N الحمولة التالية: KE، مججوزة: 0x0، الطول: 24 الحمولة التالية ل KE: الإعلام، مججوز: 0x0، الطول: 136 مجموعة DH: 2، مججوز: 0x0 *نوفمبر 11 19:31:35.882: IKEv2:Parse Notify Payload: SET_WINDOW_SIZE NOTIFY(SET_WINDOW_SIZE) الحمولة التالية: ال شيء، مججوز: 0x0، الطول: 12 معرف بروتوكول الأمان: IKE، حجم spi: 0، النوع: SET_WINDOW_SIZE *نوفمبر 11 19:31:35.882: (معرف IKEv2: (معرف SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3 (I) MSGid = 000003	يبني الموجه 2 الآن ا على تبادل CHILD_SA هي إستجابة CREATE_CHILD_SA. تحتوي حزمة CHILD_S على: • SA HDR (نوع version.flags/exch • nonce NI(إختيار تم إنشاء CHILD كجزء من التبادل الأولي، فيجب ع إرسال حمولة KE ثانية ومرة واحدة • حمولة SA • KEi (مفتاح إختي يمكن أن يحتوي CREATE_CHILD إختياريا على حم DH لتبادل KE إضافي لتمكين إ ضمانات أقوى ل توجيه سرية CHILD_SA. إذا ك عرض SA يتضم مجموعات DH مخت فيجب أن يكون عنصرا من المجم التي يتوقع ال أن يقبلها المستجيب. إذا تخمين خطأ، فسيفشل تب CREATE_CHILD ويجب إعادة المحاو

	CurState: CHILD_I_Wait الحدث: EV_RECV_CREATE_CHILD *نوفمبر 11:31:35.882: IKEv2:(معرف SA = 2):الإجراء: Action_NULL *في 11 نوفمبر 19:31:35.882: (معرف IKEv2: (معرف SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MSGid = 000003 CurState: CHILD_I_PROC الحدث: EV_CHK4_NOTIFY *في 11 نوفمبر 19:31:35.882: (معرف IKEv2: (معرف SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MSGid = 000003 CurState: CHILD_I_PROC: EV_VERIFY_MSG *نوفمبر 11 19:31:35.882: (معرف IKEv2: (معرف SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MSGid = 000003 CurState: حدث CHILD_I_PROC:_proc_msg *نوفمبر 11 19:31:35.882: (معرف IKEv2: (معرف SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MSGid = 000003 CurState: حدث CHILD_I_PROC:_chk4_pfs *نوفمبر 11 19:31:35.882: (معرف IKEv2: (معرف SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MSGid = 000003 CurState: حدث CHILD_I_PROC:_gen_dh_secret *نوفمبر 11 19:31:35.890: (معرف IKEv2: (معرف SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MSGid = 000003 CurState: حدث CHILD_I_PROC:_NO_EVENT *نوفمبر 11 19:31:35.890: (معرف IKEv2: (معرف SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MSGid = 000003 CurState: حدث CHILD_I_PROC:_OK_RECD_DH_SECRET_RESP *نوفمبر 11:31:35.890: IKEv2:(معرف SA = 2):الإجراء: Action_NULL *نوفمبر 11 19:31:35.890: (معرف IKEv2: (معرف SA = 2):SM Trace-> SA:	KEi مختلف. • n (Notify payload optional): يتم استخدام حمولة الإعلام لإرسال البيانات المعلوماتية، م الحالات والأخطا الحالة، إلى نظي يمكن أن تظهر ح الإعلام في رسا إستجابة (عادة م بسبب رفض الطل أو في تبادل مع (للإبلاغ عن أخط IKE)، أو في طلب أي رسالة أخرى للإشارة إلى إمك المرسل أو لتعد الطلب. إذا معنى تبادل CREATE_CHILD هذا يعمل على إع SA موجو تكوين IKE_SA، بخلاف أن تحدد الحمولة البادئة من نوع REKEY_SA SA ال يتم إعادة تكوي لم يقم تبادل CREATE_CHILD هذا بإعادة تكوي موجود، فيجب حذ حمولة N. الرسالة 2 الموجه لسري ويكمل تنشيط CHIL الجديد.

	I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MSGid = 000003 CurState: حدث CHILD_I_PROC:_chk_ike_rekey *نوفمبر 11 19:31:35.890: (معرف IKEv2: (معرف SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MSGid = 000003 CurState: حدث CHILD_I_PROC:_gen_skeyid *نوفمبر 11 19:31:35.890: IKEv2:(معرف SA = 2):إنشاء skeyid *نوفمبر 11 19:31:35.890: (معرف IKEv2: (معرف SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MSGid = 000003 CurState: CHILD_I_DONE الحدث: EV_ACTIVATION_SA *نوفمبر 11 19:31:35.890: (معرف IKEv2: (معرف SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MSGid = 000003 CurState: حدث CHILD_I_DID:_UPDATE_CAC_STATS *11 نوفمبر 19:31:35.890: تم تنشيط طلب IKEv2:New IKEV2 *نوفمبر 11:31:35.890: IKEv2:فشل في تقليل عدد مرات التفاوض الصادرة *نوفمبر 11 19:31:35.890: (معرف IKEv2: (معرف SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MSGid = 000003 CurState: حدث CHILD_I_DID:_CHECK_DUPE *نوفمبر 11 19:31:35.890: (معرف IKEv2: (معرف SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MSGid = 000003 CurState: حدث CHILD_I_DID:_قفاوم *نوفمبر 11 19:31:35.890: (معرف IKEv2: (معرف SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MSGid = 000003 CurState: حدث Exit: EV_CHK قلعم *نوفمبر 11 19:31:35.890: IKEv2:(معرف SA = 2):إستجابة تمت معالجتها باستخدام معرف الرسالة 3، يمكن إرسال الطلبات من النطاق 4 إلى 8	

	*في 11 نوفمبر 19:31:35.890: (معرف IKEv2: (معرف SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (I) MSGid = 0000003 CurState: Exit Event: MEV: no_event	
يستلم الموجه 1 حزمة الاستجابة من الموجه 2 ويكمل تنشيط CHILD_SA.	*نوفمبر 11 19:31:35.882: IKEv2:(معرف الدخلة (SA) = 2):الحمولة التالية: ENCR، الإصدار: 2.0 نوع Exchange: CREATE_CHILD_SA، العلامات: معرف الرسالة MSG-RESPONSE الخاص بالمستجيب: 3، الطول: 300 محتويات الحمولة: الحمولة التالية ل ENCR: SA، محجوزة: 0x0، الطول: 272 *نوفمبر 11 19:31:35.882: (معرف IKEv2: (معرف SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MSGid = 000003 CurState: CHILD_R_BLD_MSSSSSD g event:EV_CHK_IKE_REKEY *نوفمبر 11 19:31:35.882: (معرف IKEv2: (معرف SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MSGid = 000003 CurState: CHILD_R_BLD_MSG الحدث: EV_GEN_SKEYID *11 نوفمبر 19:31:35.882: IKEv2:(معرف SA = 2):إنشاء معرف Skeyid *نوفمبر 11 19:31:35.882: (معرف IKEv2: (معرف SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MSGid = 000003 CurState: CHILD_R_DONE:Event EV_ACTIVATION_SA *نوفمبر 11 19:31:35.882: IKEv2:Store MIB index ikev2 3، النظام الأساسي 62 *نوفمبر 11 19:31:35.882: (معرف IKEv2: (معرف SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MSGid = 000003 CurState: حدث CHILD_R_DONE:_UPDATE_CAC_STATS *11 نوفمبر 19:31:35.882: تم تنشيط طلب IKEv2:New IKEV2	

	*ربمفون 11 19:31:35.882: لشف IKEv2:يف مداقلا ضوافتلا تارم ددع ليلقت *ربمفون 11 19:31:35.882: (فرعم IKEv2: (فرعم SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MSGid = 000003 CurState: CHILD_R_DONE ثدحلا: EV_CHECK_DUPE *ربمفون 11 19:31:35.882: (فرعم IKEv2: (فرعم SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MSGid = 000003 CurState: ثدح CHILD_R_DONE:_قفاوم *ربمفون 11 19:31:35.882: (فرعم IKEv2: (فرعم SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MSGid = 000003 CurState: ثدح CHILD_R_DONE:_start_del_neg_tmr *ربمفون 11:31:35.882: IKEv2:(فرعم SA = 2):ءارجإلا: Action_NULL *ربمفون 11 19:31:35.882: (فرعم IKEv2: (فرعم SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MSGid = 000003 CurState: ثدح Exit: EV_CHK قلعم *ربمفون 11 19:31:35.882: IKEv2:(فرعم SA = 2):ةباجتسإ ةلسرم عم فرعم ةلاسرلا 3، نكمي 8 ىلإ 4 قاطنلا نم تابلطلا لوبق *ربمفون 11 19:31:35.882: (فرعم IKEv2: (فرعم SA = 2):SM Trace-> SA: I_SPI=0C33DB40DBAAADE6 R_SPI=F14E2BBA78024DE3 (R) MSGid = 0000003 CurState: Exit Event: MEV: no_event	

التحقق من النفق

ISAKMP

<#root>

```
show crypto ikev2 sa detailed
```

إخراج الموجه 1

<#root>

Router1#

show crypto ikev2 sa detailed

```
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote             fvrf/ivrf         Status
1         10.0.0.1/500          10.0.0.2/500       none/none         READY
      Encr: AES-CBC, keysize: 128,
         Hash: SHA96, DH Grp:2,
         Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 120/10 sec
      CE id: 1006, Session-id: 4
      Status Description: Negotiation done
      Local spi: E58F925107F8B73F     Remote spi: AFD098F4147869DA
      Local id: 10.0.0.1
      Remote id: 10.0.0.2
      Local req msg id:  2       Remote req msg id:  0
      Local next msg id: 2       Remote next msg id: 0
      Local req queued:  2       Remote req queued:  0
      Local window:      5       Remote window:      5
      DPD configured for 0 seconds, retry 0
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Initiator of SA : Yes
```

إخراج الموجه 2

<#root>

Router2#

show crypto ikev2 sa detailed

```
 IPv4 Crypto IKEv2  SA

Tunnel-id Local           Remote              fvrf/ivrf          Status
2         10.0.0.2/500    10.0.0.1/500        none/none          READY
      Encr: AES-CBC, keysize: 128, Hash: SHA96,
         DH Grp:2, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 120/37 sec
      CE id: 1006, Session-id: 4
      Status Description: Negotiation done
      Local spi: AFD098F4147869DA       Remote spi: E58F925107F8B73F
      Local id: 10.0.0.2
      Remote id: 10.0.0.1
      Local req msg id:  0              Remote req msg id:  2
      Local next msg id: 0              Remote next msg id: 2
      Local req queued:  0              Remote req queued:  2
      Local window:      5              Remote window:      5
      DPD configured for 0 seconds, retry 0
```

```
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Initiator of SA : No
```

IPsec

<#root>

show crypto ipsec sa

ملاحظة: في هذا الإخراج، على عكس ما هو الحال في IKEv1، تظهر قيمة مجموعة PFS DH على هيئة "PFS (Y/N): N، مجموعة DH: none" أثناء تفاوض النفق الأول، لكن بعد حدوث مفتاح مفتاح آخر، تظهر القيم الصحيحة. هذا ليس خطأ، حتى وإن كان السلوك موصوف في cisco بق id CSCug67056. (يمكن لمستخدمي Cisco المسجلين الوصول إلى أدوات Cisco الداخلية أو المعلومات.)
الفرق بين IKEv1 و IKEv2 هو أنه في الحالة الأخيرة، يتم إنشاء SAs الخاصة بالأطفال كجزء من تبادل المصادقة نفسه. سيتم إستخدام مجموعة DH التي تم تكوينها ضمن خريطة التشفير فقط أثناء المفاتيح. بالتالي، سترى PFS (Y/N): N، مجموعة DH: none حتى المفاتيح الأول.
مع IKEv1، سترى سلوك مختلف، لأن إنشاء Child SA يحدث أثناء "الوضع السريع"، وللرسالة CREATE_CHILD_SA توفير لحمل حمولة Key Exchange التي تحدد معلمات DH الاستخراج سر مشترك جديد.

إخراج الموجه 1

<#root>

```
Router1#
```

show crypto ipsec sa

```
interface: Tunnel0
    Crypto map tag: Tunnel0-head-0,
         local addr 10.0.0.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port):
         (0.0.0.0/0.0.0.0/256/0)
   remote ident (addr/mask/prot/port):
         (0.0.0.0/0.0.0.0/256/0)
   current_peer 10.0.0.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 10, #pkts encrypt:
         10, #pkts digest: 10
    #pkts decaps: 10, #pkts decrypt:
         10, #pkts verify: 10
    #pkts compressed: 0, #pkts decompressed: 0
```

```
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.0.0.1,
         remote crypto endpt.: 10.0.0.2
     path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
     current outbound spi: 0xF6083ADD(4127734493)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x6B74CB79(1802816377)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 18, flow_id: SW:18,
         sibling_flags 80000040,
         crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec):
         (4276853/3592)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xF6083ADD(4127734493)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 17, flow_id: SW:17,
         sibling_flags 80000040,
         crypto map: Tunnel0-head-0
        sa timing: remaining key
         lifetime (k/sec): (4276853/3592)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```

إخراج الموجه 2

<#root>

```
Router2#
```

show crypto ipsec sa

```
interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 10.0.0.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/256/0)
```

```
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/256/0)
   current_peer 10.0.0.1 port 500
     PERMIT, flags={origin_is_acl,}
    #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: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.0.0.2,
         remote crypto endpt.: 10.0.0.1
     path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
     current outbound spi: 0x6B74CB79(1802816377)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xF6083ADD(4127734493)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 17, flow_id: SW:17,
         sibling_flags 80000040,
         crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime
         (k/sec): (4347479/3584)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x6B74CB79(1802816377)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 18, flow_id: SW:18,
         sibling_flags 80000040,
         crypto map: Tunnel0-head-0
        sa timing: remaining key
         lifetime (k/sec): (4347479/3584)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```

يمكنك أيضا التحقق من إخراج الأمر show crypto session على كل الموجهين؛ يعرض هذا الإخراج حالة جلسة عمل النفق up-active.

<#root>

Router1#

show crypto session

```
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.0.0.2 port 500
  IKEv2 SA: local 10.0.0.1/500 remote 10.0.0.2/500 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map

Router2#
```

show cry session

```
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.0.0.1 port 500
  IKEv2 SA: local 10.0.0.2/500 remote 10.0.0.1/500 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
```

معلومات ذات صلة

- تصحيح أخطاء مستوى البروتوكول وتبادل حزم IKEv2
- الدعم الفني والتنزيلات من Cisco

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).