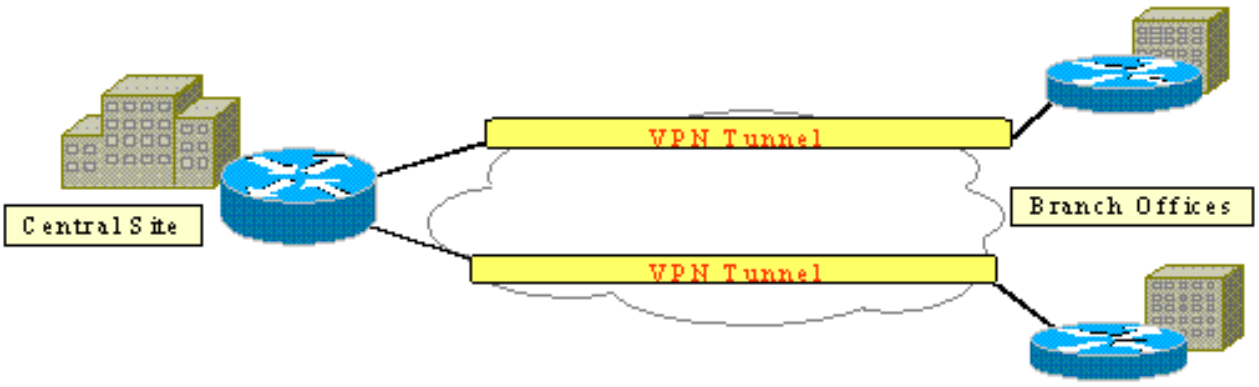
تكوين IPSec عبر ADSL على Cisco 2600/3600 باستخدام وحدات تشفير الأجهزة ADSL-WIC

المحتويات

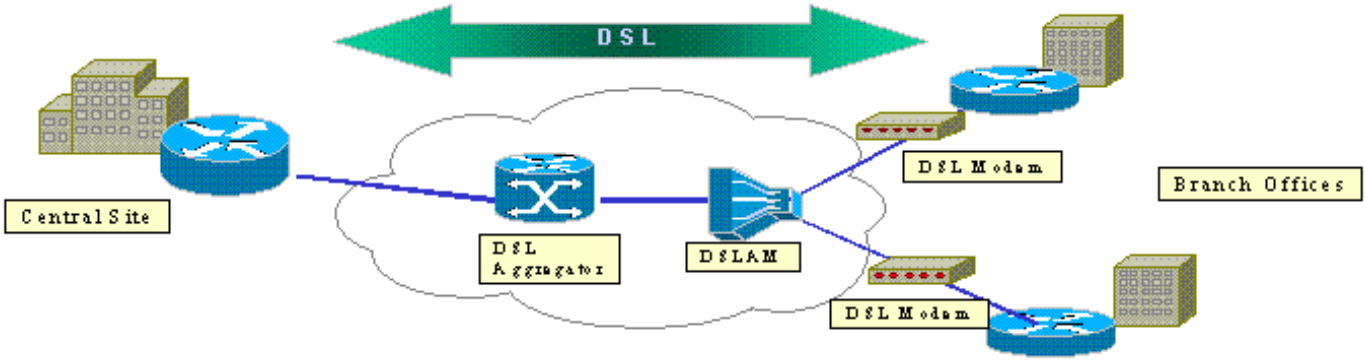
المقدمة

مع توسع الإنترنت، تطلب المكاتب الفرعية ان تكون صلاتها بالمواقع المركزية موثوق بها وآمنة على السواء. تقوم الشبكات الخاصة الظاهرية (VPN) بحماية المعلومات بين المكاتب البعيدة والمواقع المركزية أثناء تنقلها عبر الإنترنت. يمكن إستخدام أمان IP (IPSec) لضمان تشفير البيانات التي تمر عبر شبكات VPN هذه. يوفر التشفير طبقة أخرى من أمان الشبكة.



يوضح هذا الشكل شبكة VPN نموذجية ل IPSec. هناك عدد من الاتصالات من موقع إلى موقع للوصول عن بعد بين المكاتب الفرعية والمواقع المركزية. عادة، يتم توفير روابط شبكة WAN التقليدية مثل ترحيل الإطارات و ISDN وطلب المودم بين المواقع. ويمكن أن تتضمن هذه الاتصالات رسوما باهظة التكلفة للتوريد لمرة واحدة ورسوما شهرية باهظة الثمن. بالنسبة لمستخدمي ISDN والمودم، يمكن أن تكون هناك أوقات اتصال طويلة.

يقدم خط المشترك الرقمي غير المتماثل (ADSL) بديلا متصلا دائما ومنخفض التكلفة لهذه روابط شبكة WAN التقليدية. توفر بيانات IPSec المشفرة عبر إرتباط ADSL اتصالا آمنا وموثوقا، كما توفر المال للعملاء. تتطلب المعدات التقليدية لأماكن عمل عملاء (CPE) ADSL التي تم إعدادها في مكتب فرعي مودم ADSL يتصل بجهاز يعمل على إنشاء حركة مرور بيانات IPSec وإنهائها. يوضح هذا الشكل شبكة ADSL نموذجية.



تدعم موجهات Cisco 2600 و 3600 بطاقة الواجهة WIC-1ADSL) ADSL WAN). هذا WIC-1ADSL هو حل وصول عن بعد متعدد الخدمات مصمم لتلبية إحتياجات المكاتب الفرعية. يؤدي إدخال وحدات WIC-1ADSL وتشفير الأجهزة إلى تحقيق الطلب على بروتوكولات IPSec و DSL في مكتب فرعي في حل موجه واحد. ويعمل WIC-1ADSL على التخلص من الحاجة إلى مودم DSL منفصل. توفر وحدة تشفير الأجهزة ما يصل إلى عشرة أضعاف الأداء مقارنة بتشفير البرامج فقط لأنها تقوم بإلغاء تحميل التشفير الذي يعالج من الموجه.

للحصول على مزيد من المعلومات حول هذين النوعين، ارجع إلى بطاقات واجهة ADSL WAN لسلسلة موجهات الوصول النمطية 1700 و 2600 و 3700 ووحدات الشبكة الخاصة الظاهرية لسلسلة Cisco 1700 و 2600 و 3600 و 3700.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

الموجهات من السلسلة 3600/2600 من Cisco:

- برنامج IOS® الإصدار 12.1(5)YB Enterprise Plus 3DES مجموعة ميزات
- DRAM 64 ميجابايت لسلسلة Cisco 2600 و DRAM 96 ميجابايت لسلسلة Cisco 3600
- Flash 16 ميجابايت ل the Cisco 2600 Series، Flash 32 ميجابايت ل the Cisco 3600 Series
- WIC-1 ADSL
- وحدات تشفير الأجهزةAIM-VPN/BP و AIM-VPN/EP لسلسلة Cisco 2600NM-VPN/MP ل the Cisco 3620/3640AIM-VPN/HP ل the Cisco 3660

السلسلة Cisco 6400 Series:

- برنامج IOS الإصدار 12.1(5)DC1 من Cisco
- ذاكرة DRAM سعة 64 ميجابايت

- Flash سعة 8 ميجابايت

السلسلة 6160 من Cisco:

- برنامج IOS الإصدار DA2(7)12.1 من Cisco
- ذاكرة DRAM سعة 64 ميجابايت
- Flash سعة 16 ميجابايت

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

الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى اصطلاحات تلميحات Cisco التقنية.

التكوين

في هذا القسم، تقدم لك المعلومات التي يمكنك إستخدامها لتكوين الميزات الموضحة في هذا المستند.

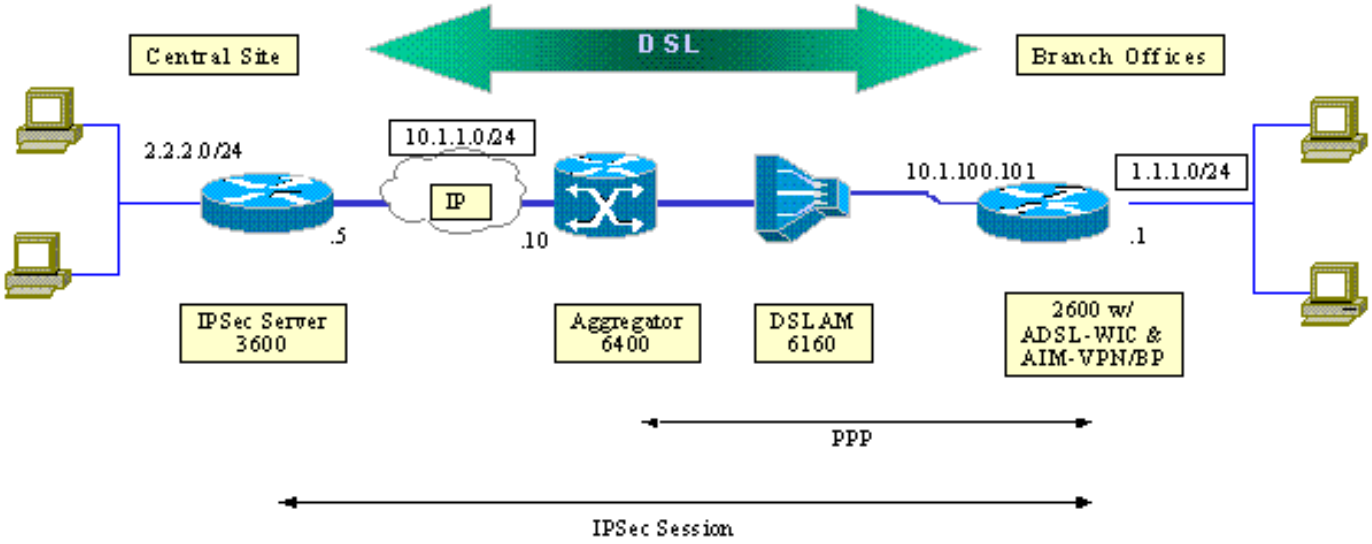
ملاحظة: للعثور على معلومات إضافية حول الأوامر المستخدمة في هذا المستند، أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط).

الرسم التخطيطي للشبكة

يستعمل هذا وثيقة الشبكة setup يبدي هذا رسم بياني.

يحاكي هذا الاختبار اتصال IPSec VPN يستخدم ADSL في بيئة نموذجية للمكاتب الفرعية.

يدرب Cisco 2600/3600 مع ADSL-WIC ووحدة تشفير الأجهزة حتى Cisco 6160 Digital Subscriber Line Access Multiplexer (DSLAM). يتم إستخدام Cisco 6400 كجهاز تجميع ينهي جلسة PPP التي تبدأ من موجه Cisco 2600. ينشأ نفق IPSec في CPE 2600 وينتهي في Cisco 3600 في المكتب المركزي، جهاز وحدة الاستقبال والبث ل IPSec في هذا السيناريو. تم تكوين جهاز وحدة الاستقبال والبث لقبول الاتصالات من أي عميل بدلا من التجزيء الفردي. كما يتم إختبار جهاز وحدة الاستقبال والبث باستخدام مفاتيح مشتركة مسبقا فقط وخوارزمية التجزئة (SHA) الآمنة لمعالج الخدمة الطرفية 3DES و ESP) Edge Service Processor)-رمز مصادقة الرسائل المستند إلى التجزئة (HMAC).



التكوينات

يستخدم هذا المستند التكوينات التالية:

- موجّه Cisco 2600
- جهاز وحدة الاستقبال والبث IPSec - الموجه Cisco 3600
- Cisco 6160 DSLAM
- معالج المسار عقدة (NRP) (Cisco 6400 Node Route Processor

لاحظ هذه النقاط حول التكوينات:

- يتم إستخدام مفتاح مشترك مسبقا. من أجل إعداد جلسات عمل IPSec إلى أقران متعددين، يجب عليك تحديد عبارات تعريف مفتاح متعددة أو تحتاج إلى تكوين خريطة تشفير ديناميكية. إذا كانت جميع جلسات العمل تشترك في مفتاح واحد، فيجب عليك إستخدام عنوان نظير 0.0.0.0.
- يمكن تعريف مجموعة التحويل ل ESP أو رأس المصادقة (AH) أو كليهما للمصادقة المزدوجة.
- يجب تعريف تعريف نهج تشفير واحد على الأقل لكل نظير. تحدد خرائط التشفير النظير الذي سيتم إستخدامه لإنشاء جلسة عمل IPSec. يستند القرار إلى تطابق العنوان المحدد في قائمة الوصول. في هذه الحالة، ستكون قائمة الوصول 101.
- يجب تعريف خرائط التشفير لكل من الواجهات المادية (الواجهة ATM 0/0 في هذه الحالة) والقالب الظاهري.
- يناقش التكوين المقدم في هذا المستند نفق IPSec فقط عبر اتصال DSL. قد تكون هناك حاجة إلى ميزات أمان إضافية لضمان عدم تعرض شبكتك للخطر. يمكن أن تتضمن ميزات الأمان هذه قوائم تحكم في الوصول (ACL) إضافية وترجمة عنوان الشبكة (NAT) واستخدام جدار حماية مع وحدة خارجية أو مجموعة ميزات جدار حماية IOS. يمكن إستخدام كل من هذه الميزات لتقييد حركة المرور غير IPSec إلى الموجه ومنه.

موجّه Cisco 2600

```
crypto isakmp policy 10
 Defines the ISAKMP parameters to be negotiated. ---!
authentication pre-share !--- Defines the pre-shared key
 to be exchanged with the peer. crypto isakmp key pre-
 shared address 10.1.1.5 ! crypto ipsec transform-set
 strong esp-des esp-sha-hmac !--- Defines the transform
 set for ESP and/or AH. ! crypto map vpn 10 ipsec-isakmp
set peer 10.1.1.5 set transform-set strong match address
 102 !--- Defines the crypto policy that includes the
```

```
peer IP address, !--- transform set that is used, as well as the access list !--- that defines the packets that are encrypted. ! interface ATM0/0 no ip address atm vc-per-vp 256 no atm ilmi-keepalive dsl operating-mode auto no fair-queue ! interface ATM0/0.1 point-to-point pvc 0/35 encapsulation aal5mux ppp dialer dialer pool-member 1 ! crypto map vpn !--- Applies the crypto map to the ATM sub-interface. ! interface FastEthernet0/1 ip address 1.1.1.1 255.255.255.0 duplex 100 speed full ! interface Dialer1 ip address 10.1.100.101 255.255.255.0 dialer pool 1 encapsulation ppp ppp pap sent-username 2621a password 7 045802150C2E crypto map vpn !--- Applies the crypto map to the Dialer interface. ! ip classless ! ip route 2.2.2.0 255.255.255.0 10.1.1.5 ip route 10.1.1.0 255.255.255.0 10.1.100.1 !--- Static routes between 2600 CPE and IPSec server. ip route 0.0.0.0 0.0.0.0 Dialer1 ! access-list 102 permit ip 1.1.1.0 0.0.0.255 2.2.2.0 0.0.0.255 !--- Access list that defines the addresses that are encrypted. ! end
```

جهاز وحدة الاستقبال والبث IPSec - الموجه Cisco 3600

```
crypto isakmp policy 10
Defines the ISAKMP parameters to be negotiated. ---!
authentication pre-share !--- Defines the pre-shared key to be exchanged with the peer. crypto isakmp key pre-shared address 10.1.100.101 ! crypto ipsec transform-set strong esp-des esp-sha-hmac !--- Defines the transform set for ESP and/or AH. ! crypto map vpn 10 ipsec-isakmp set peer 10.1.100.101 set transform-set strong match address 102 !--- Defines the crypto policy that includes the peer IP address, !--- transform set that are used, and the access list !--- that defines the packets to be encrypted. ! interface FastEthernet0/0 ip address 10.1.1.5 255.255.255.0 duplex 100 speed full crypto map vpn !--- Applies the crypto map to the Fast Ethernet interface. ! interface FastEthernet0/1 ip address 2.2.2.1 255.255.255.0 speed full full-duplex ! ip route 1.1.1.0 255.255.255.0 10.1.1.10 ip route 10.1.100.0 255.255.255.0 10.1.1.10 ! access-list 102 permit ip 2.2.2.0 0.0.0.255 1.1.1.0 0.0.0.255 !--- Access list that defines the addresses to be encrypted. ! end
```

Cisco 6160 DSLAM

```
dsl-profile full
dmt bitrate maximum fast downstream 10240 upstream 1024
dmt bitrate maximum interleaved downstream 0 upstream 0
!
atm address
47.0091.8100.0000.0004.6dd6.7c01.0004.6dd6.7c01.00
atm router pnni
no aesa embedded-number left-justified
none 1 level 56 lowest
redistribute atm-static
!
interface atm0/0
no ip address
atm maxvp-number 0
atm maxvc-number 4096
atm maxvci-bits 12
!
interface atm 1/2
```

```
                                                    no ip address
                                                dsl profile full
                                            no atm ilmi-keepalive
                                    atm soft-vc 0 35 dest-address
c12b.cd81.4000.0c80.8000.00 0 36.47.0091.8100.0000.0004
                                            rx-cttr 1 tx-cttr 1
The previous two lines need to be on one line. !--- ---!
    The network service access point (NSAP) !--- address
 comes from the NSP on the Cisco 6400. Issue !--- a show
                                        .atm address command


                                                            !
```

بروتوكول وقت الشبكة (NRP) طراز 6400 من Cisco

```
                                                            !
                                    username cisco password cisco
                                                            !
                                            vc-class atm pppoa
                            encapsulation aal5mux ppp Virtual-template1
                                                            !
                                        interface loopback 0
                                ip address 10.1.100.1 255.255.255.0
                                                            !
                                        interface atm 0/0/0
                                              no ip address
                                        no ip route-cache
                                       no ip mroute-cache
                                no atm auto-configuration
                                    atm ilmi-keepalive 10
                                             pvc 0/16 ilmi
                                                            !
                                      hold-queue 1000 in
                                                            !
                            interface atm 0/0/0.1 multipoint
                                        no ip route-cache
                                        no ip mroute-cach
                                          class-int pppoa
                                                 pvc 0/36
                                                            !
                                    interface fast 0/0/0
                                ip address 10.1.1.10 255.255.255.0
                                        no ip route-cache
                                      no ip mroute-cache
                                             half-duplex
                                                            !
                                interface Virtual-Template1
                                    ip unnumbered Loopback0
                                           no ip route-cache
                                peer default ip address pool pppoa
                                   ppp authentication pap chap
                                    ppp ipcp accept-address
                                                ppp multilink
                                no ppp multilink fragmentation
                                                            !
                            ip local pool pppoa 10.1.100.2 10.1.100.100
                                                            !
```

كافيتس

يمكن تكوين إتصالات ADSL باستخدام قالب ظاهري أو واجهة المتصل.

يتم إستخدام واجهة المتصل لتكوين DSL CPE لتلقي عنوان من موفر الخدمة (يتم التفاوض على عنوان IP). تعد واجهة القالب الظاهري واجهة منسدلة ولا تدعم خيار العنوان الذي تم التفاوض عليه، وهو أمر ضروري في بيئة DSL. تم تنفيذ واجهات القالب الظاهري في البداية لبيئات DSL. تعد واجهة المتصل حاليا هي التكوين الموصى به على جانب DSL CPE.

تم العثور على مشكلتين في وقت تكوين واجهات المتصل باستخدام IPSec:

- معرف تصحيح الأخطاء من Cisco CSCdu30070 (العملاء المسجلون فقط) — IPSec عبر DSL:مدخل قائمة انتظار على واجهة متصل DSL.
- معرف تصحيح الأخطاء من Cisco CSCdu30335 (العملاء المسجلون فقط) —IPSec المستند إلى الأجهزة عبر DSL: مدخل قائمة انتظار على واجهة المتصل.

ال workaround حالي ل كلا من هذا إصدار أن يشكل ال DSL CPE مع الإستعمالمن ال virtual-template قارن كما هو موضح في التشكيل.

تم تخطيط الإصلاحات لكل من هذه المشاكل لبرنامج Cisco IOS Software، الإصدار 12.2(4)T. بعد هذا الإصدار، يتم نشر إصدار محدث من هذا المستند لعرض تكوين واجهة المتصل كخيار آخر.

التحقق من الصحة

يوفر هذا القسم المعلومات التي يمكنك إستخدامها للتأكد من أن التكوين يعمل بشكل صحيح.

يمكن إستخدام العديد من أوامر **العرض** للتحقق من إنشاء جلسة عمل IPSec بين الأقران. تكون الأوامر ضرورية فقط على نظائر IPSec، في هذه الحالة السلسلة 2600 و 3600 من Cisco.

يتم دعم بعض أوامر **العرض بواسطة** أداة مترجم الإخراج (العملاء المسجلون فقط)، والتي تتيح لك عرض تحليل إخراج أمر **العرض**.

- **show crypto engine connections active**—يعرض كل مرحلة SA 2 بنيت ومقدار حركة المرور المرسلة.
- **show crypto ipSec sa** — يعرض IPSec sa الذي تم إنشاؤه بين الأقران.

هذا نموذج لمخرجات الأمر **show crypto engine connections active**.

```
show crypto engine connections active

ID   Interface        IP-Address   State Algorithm           Encrypt Decrypt
      none>           <none>       set   HMAC_SHA+DES_56_CB  0       0>    1
      Virtual-Template1 10.1.100.101 set   HMAC_SHA            0       4 200
      Virtual-Template1 10.1.100.101 set   HMAC_SHA            4       0 201
```

هذا نموذج لمخرجات الأمر لأمر **show crypto ipSec**.

```
show crypto ipsec sa

                                Interface:  Virtual-Template1
                        Crypto map tag: vpn, local addr. 10.1.100.101

                       (Local ident (addr/mask/prot/port):  (1.1.1.0/255.255.255.0/0/0
                       (Remote ident (addr/mask/prot/port): (2.2.2.0/255.255.255.0/0/0
                                                    Current_peer:  10.1.1.5
                                                 {,PERMIT, flags= {origin_is_acl
                     pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4#
```

```
                                    pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4#
                                          pkts compressed: 0, #pkts decompressed: 0#
                  pkts not compressed: 0, #pkts compr failed: 0, # pkts decompress failed: 0#
                                                send errors 11, #recv errors 0#

                  local crypto endpt:  10.1.100.101, remote crypto endpt.: 10.1.1.5
                                                  path mtu 1500, media mtu 1500
                                                current outbound spi:  BB3629FB

                                                                 :inbound esp sas
                                                      (spi:  0x70C3B00B(1891872779
                                                transform: esp-des, esp-md5-hmac
                                                     {,in use settings ={Tunnel
                                          slot: 0, conn id: 2000, flow_id: 1, crypto map: vpn
                                    (sa timing: remaining key lifetime (k/sec): (4607999/3446
                                                                   IV size: 8 bytes
                                                  Replay detection support: Y

                                                                  :Inbound ah sas

                                                                 :Inbound pcp sas

                                                                 :Outbound esp sas
                                                      (Spi: 0xBB3629FB(3140889083
                                                Transform: esp-des, esp-md5-hmac
                                                     {,In use settings ={Tunnel
                                          Slot:0, conn id: 2001, flow_id: 2, crypto map: vpn
                                    (Sa timing: remaining key lifetime (k/sec): (4607999/3446
                                                                   IV size: 8bytes
                                                  Replay detection support: Y

                                                                 :Outbound ah sas

                                                                :Outbound pcp sas
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم المعلومات التي يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

تعني الرسالة " = "0x8 التي يتم الإبلاغ عنها بواسطة الأمر **debug atm events** عادة أن WIC1-ADSL غير قادر على تلقي "اكتشاف الناقل" من DSLAM المتصل. وفي هذه الحالة، يحتاج العميل إلى التأكد من أن إشارة DSL مزودة على السلكين المتوسطين المتعلقين بموصل RJ11. توفر بعض Telco إشارة DSL على الدباسين الخارجيين بدلا من ذلك.

أوامر استكشاف الأخطاء وإصلاحها

يتم دعم بعض أوامر **العرض بواسطة** أداة مترجم الإخراج (العملاء المسجلون فقط)، والتي تتيح لك عرض تحليل إخراج أمر **العرض**.

ملاحظة: قبل إصدار أوامر **debug**، راجع المعلومات المهمة في أوامر تصحيح الأخطاء.

تحذير: لا تقوم بتشغيل تصحيح الأخطاء على شبكة مباشرة. يمكن أن يؤدي حجم المعلومات التي يتم عرضها إلى تحميل الموجه بشكل زائد إلى النقطة التي لا يتم فيها إصدار رسائل CPUHOG أو تدفق البيانات.

- **debug crypto IPSec**—يعرض أحداث IPSec.
- **debug crypto ISAKMP**—يعرض الرسائل المتعلقة بأحداث IKE.

ملخص

يوفر تنفيذ بروتوكول IPSec عبر اتصال ADSL اتصال شبكة آمن وموثوق به بين المكاتب الفرعية والمواقع المركزية. يوفر إستخدام السلسلة Cisco 2600/3600 مع ADSL-WIC ووحدات تشفير الأجهزة تكلفة ملكية أقل للعميل حيث يمكن الآن تحقيق ADSL و IPSec في حل موجه واحد. يجب أن يكون التكوين والتحذيرات المدرجة في هذه الورقة بمثابة دليل إرشادي أساسي لإعداد هذا النوع من الاتصال.

معلومات ذات صلة

- مقدمة عن تشفير أمان IPSec) IP)
- الموجّهات من السلسلة 2600 من Cisco
- الشبكات الخاصة الظاهرية
- الدعم الفني ل DSL و LRE
- دعم منتجات البوابات العالمية
- دعم تقنية الطلب والوصول
- الدعم الفني - 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).