تكوين عميل أجهزة Cisco VPN 3002 إلى موجه Cisco IOS باستخدام EzVPN في وضع امتداد الشبكة

المحتويات

المقدمة

يصف هذا المستند تكوين عميل جهاز Cisco VPN 3002 الذي يتصل بموجه Cisco IOS®في وضع امتداد الشبكة باستخدام برنامج Cisco IOS الإصدار 12.2(8)T ووظائف خادم EzVPN) Easy VPN). وهذا يسمح ل Cisco IOS بإنهاء أنفاق VPN التي تأتي من عملاء EzVPN، مثل عملاء PIX، VPN، و Cisco IOS EzVPN. هناك جزء صغير من خمسة اقترانات أمان (SAs) (واحد تبادل مفتاح الإنترنت [IKE] بالإضافة إلى أربعة IPSec) عند اتصال عميل VPN بجهاز وحدة الاستقبال والبث. وهذا يرجع إلى حقيقة أنه عندما يتصل عميل الشبكة الخاصة الظاهرية (VPN) بنقطة الاستقبال والبث، فإنه يتفاوض دائما بين وحدتي خدمة IPSec باستخدام عنوان IP الخاص بواجهة التركيز العامة لعنوان IP الخاص بنقطة الاستقبال والبث. يتم إستخدام هذا النفق لأغراض الإدارة للاتصال بعميل VPN من وحدة الاستقبال والبث إما من خلال واجهة المستخدم الرسومية (GUI) أو واجهة سطر الأوامر (CLI). ويتم ذلك تلقائيا. الآخر ل المعطيات حركة مرور بين الشبكة خلف ال VPN زبون وال cisco ios مسحاج تخديد.

ارجع إلى تكوين عميل أجهزة VPN 3002 إلى PIX 6.x لمعرفة المزيد حول نفس السيناريو حيث يكون خادم VPN هو PIX 6.x.

ارجع إلى تكوين اتصال بين عميل أجهزة VPN 3002 ومجمع VPN 3000 في وضع امتداد الشبكة لمعرفة المزيد حول السيناريو نفسه حيث يكون خادم VPN هو مركز Cisco VPN 3000 Series.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- عميل أجهزة Cisco VPN 3002
- برنامج IOS الإصدار T(8)12.2 من Cisco والإصدارات الأحدث

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

الاصطلاحات

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

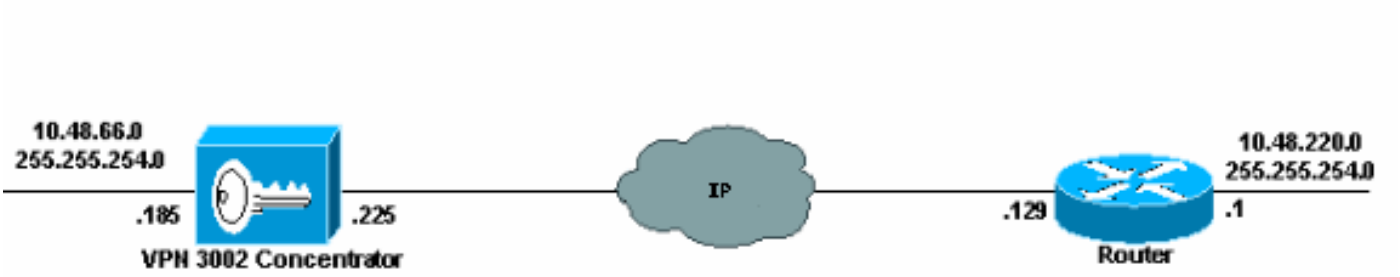
التكوينات

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للعثور على مزيد من المعلومات حول الأوامر المستخدمة في هذا المستند.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



يستخدم هذا المستند هذه التكوينات.

- موجه IOS من Cisco
- عميل أجهزة Cisco VPN 3002

موجه IOS من Cisco

```
akim#show running
Current configuration : 1449 bytes
!
version 12.2
```

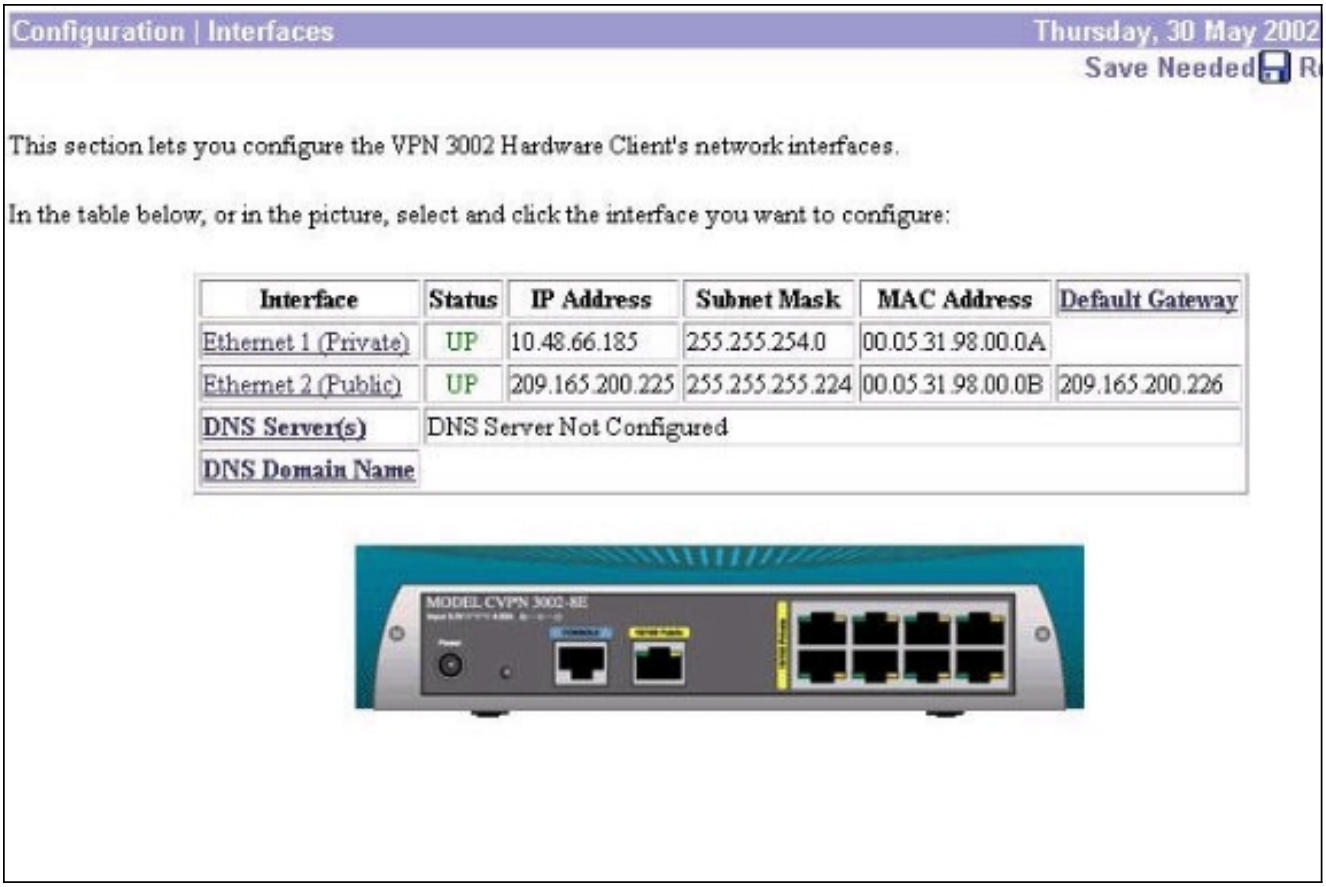
```
service config
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname akim
!
Enable Authentication, Authorizing and Accounting ---!
(AAA) !--- for user authentication and group
authorization. aaa new-model
To enable X-Auth for user authentication, !--- ---!
enable the AAA commands. aaa authentication login
userauthen local
To enable group authorization, !--- enable the AAA ---!
commands. aaa authorization network groupauthor local
aaa session-id common
!
Define the username and password to be used for X- ---!
Auth. username fadi password 0 cisco memory-size iomem
10 ip subnet-zero ! ! ! !--- Create an Internet Security
Association and !--- Key Management Protocol (ISAKMP)
policy for Phase 1 negotiations. crypto isakmp policy 3
encr 3des
authentication pre-share
group 2
!
Create a group with the pre-shared key for IKE ---!
authentication. crypto isakmp client configuration group
fadigroup
key cisco123
!
!
Create the Phase 2 policy for actual data ---!
encryption. crypto ipsec transform-set myset esp-3des
esp-sha-hmac
!
Create a dynamic map and !--- apply the transform ---!
set that was created earlier. crypto dynamic-map dynmap
10
set transform-set myset
!
Create the actual crypto map, !--- and apply the ---!
AAA lists that were created earlier. !--- These commands
associate the AAA commands to the crypto map. crypto map
clientmap client authentication list userauthen
crypto map clientmap isakmp authorization list
groupauthor
crypto map clientmap 10 ipsec-isakmp dynamic dynmap
!
!
!
!
!
!
!
!
fax interface-type fax-mail
mta receive maximum-recipients 0
!
!
!
!
Apply the crypto map on the interface where !--- ---!
traffic leaves the router. interface FastEthernet0/0
```

```
 ip address 209.165.202.129 255.255.255.224
                                 duplex auto
                                 speed auto
                           crypto map clientmap
                                          !
                              interface Serial0/0
                                   no ip address
                                        shutdown
                                   no fair-queue
                                  clockrate 2000000
                                          !
                              interface FastEthernet0/1
                            ip address 10.48.220.1 255.255.254.0
                                 duplex auto
                                 speed auto
                                          !
                              interface Serial0/1
                                   no ip address
                                        shutdown
                                  clockrate 2000000
                                          !
                                    ip classless
                  ip route 0.0.0.0 0.0.0.0 209.165.202.130
                                 ip http server
                               ip pim bidir-enable
                                          !
                                          !
                                          !
                                          !
                                call rsvp-sync
                                          !
                                          !
                              mgcp profile default
                                          !
                              dial-peer cor custom
                                          !
                                          !
                                          !
                                          !
                                          !
                                  line con 0
                                exec-timeout 0 0
                                  line aux 0
                                line vty 0 4
                                          !
                                          !
                                        end
```

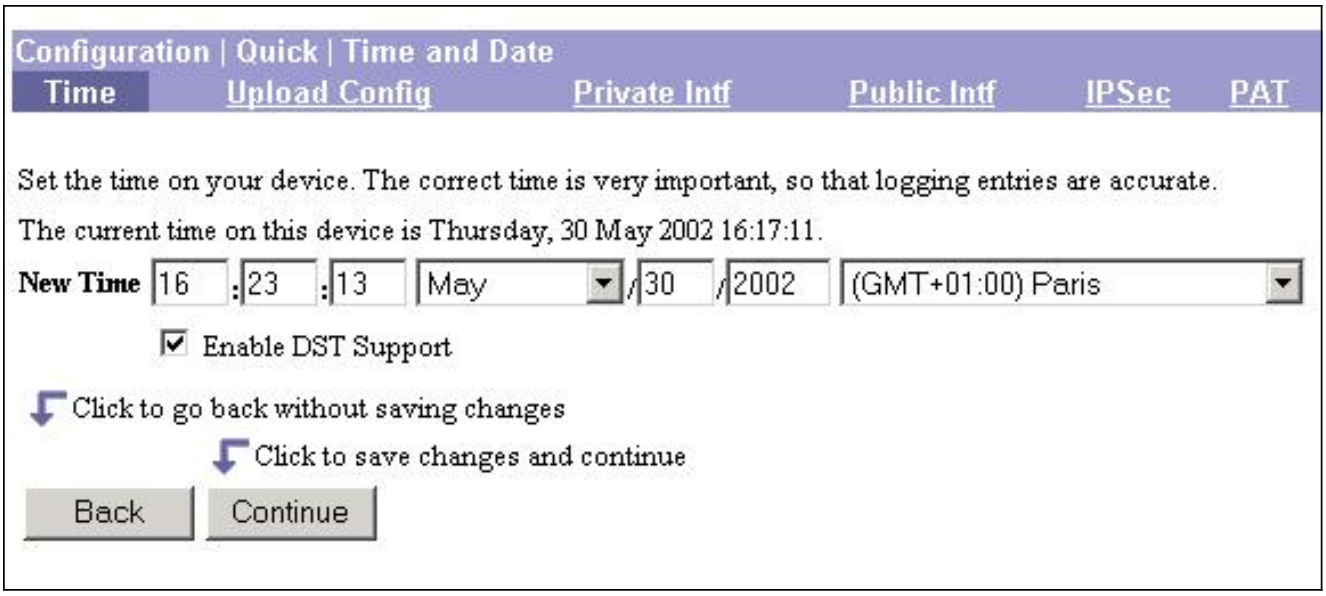
تكوين عميل أجهزة Cisco VPN 3002

أتمت هذا steps in order to شكلت ال VPN زبون:

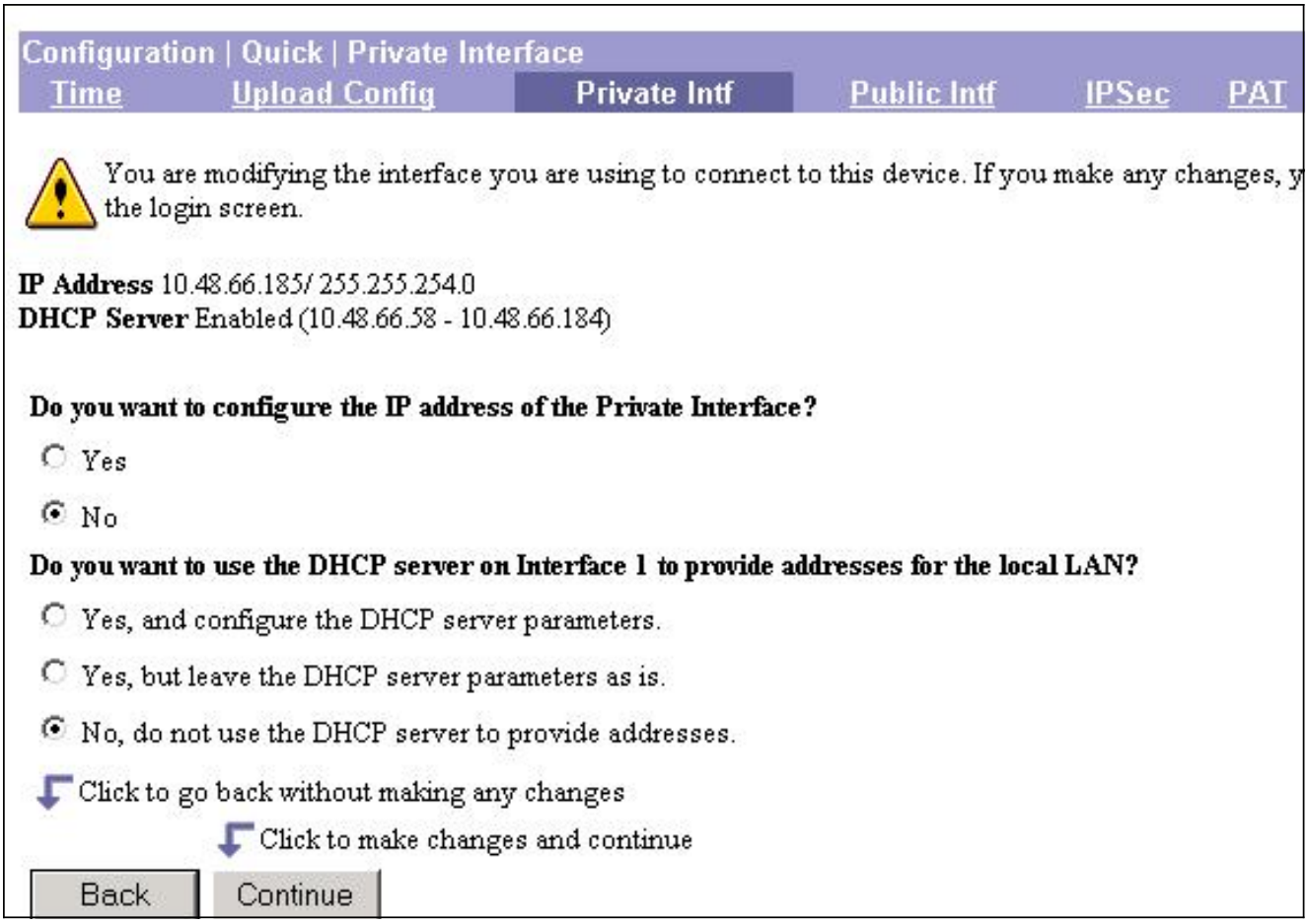
1. أخترت **تشكيل>قارن** وفحصت العنوان.



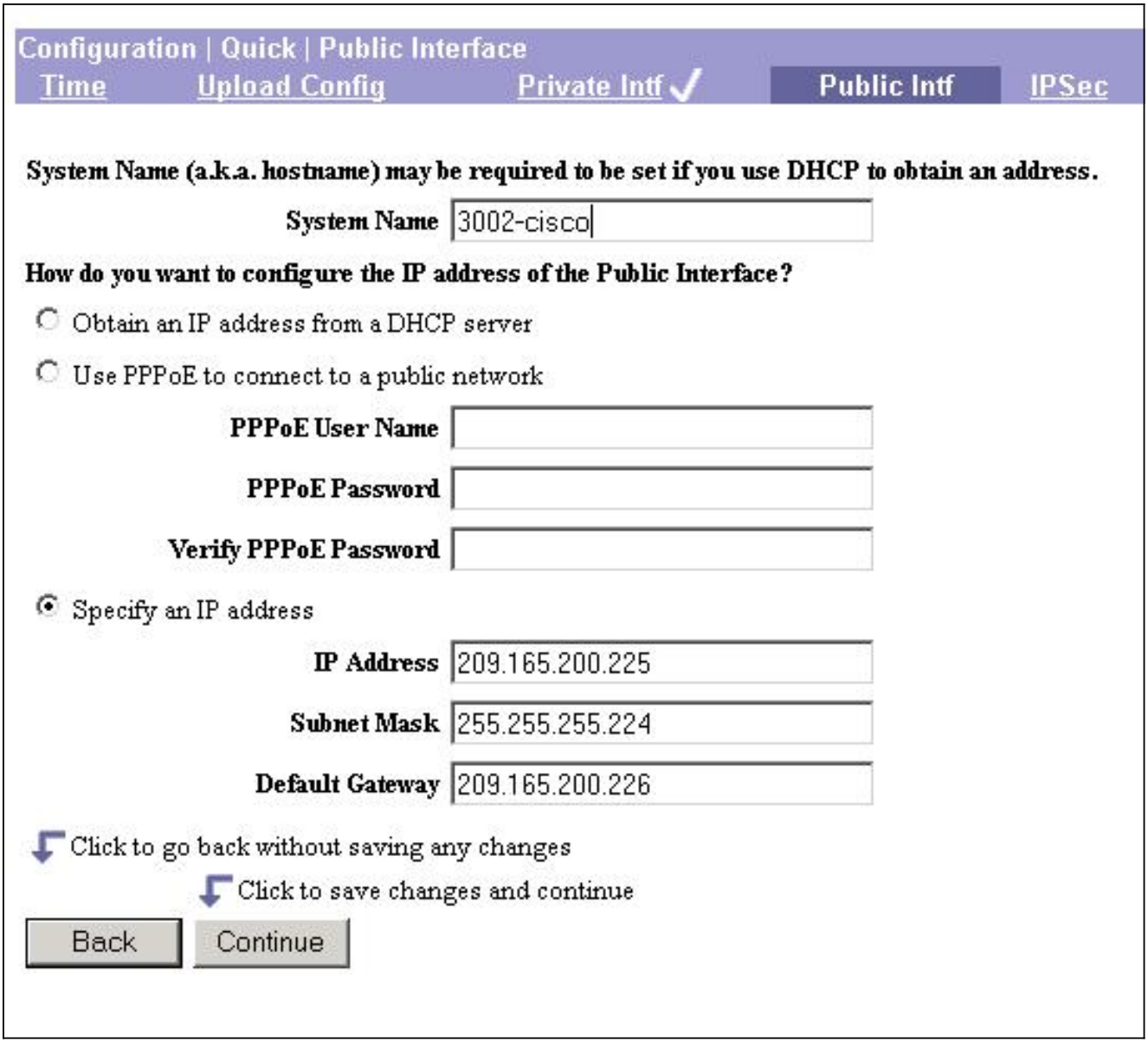
2. حدد **تكوين>سريع>الوقت والتاريخ>الوقت** لتعيين الوقت والتحقق من صحته.



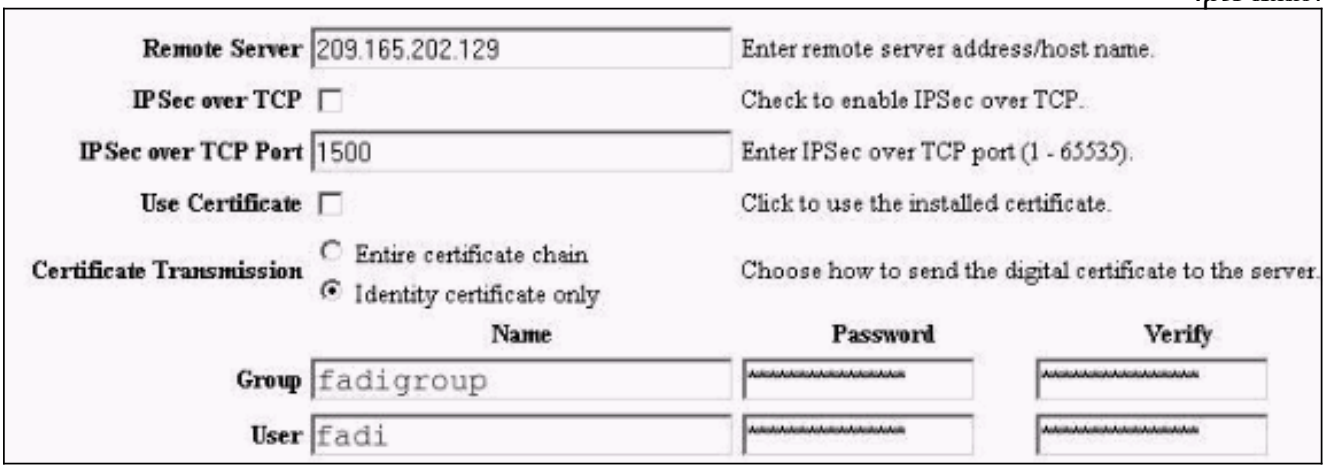
3. أخترت **تشكيل>سريع>قارن خاص>قارن خاص>قارن خاص** أن يشكل العنوان ساكن إستاتيكي على المضيف داخلي (ما من DHCP).
4. حدد **لا** ل "هل تريد تكوين عنوان IP الخاص للواجهة الخاصة؟ ".
5. حدد **لا، ألا تستخدم خادم DHCP لتقديم عناوين** ل "هل تريد إستخدام خادم DHCP على الواجهة 1 لتقديم عناوين للشبكة المحلية؟
".



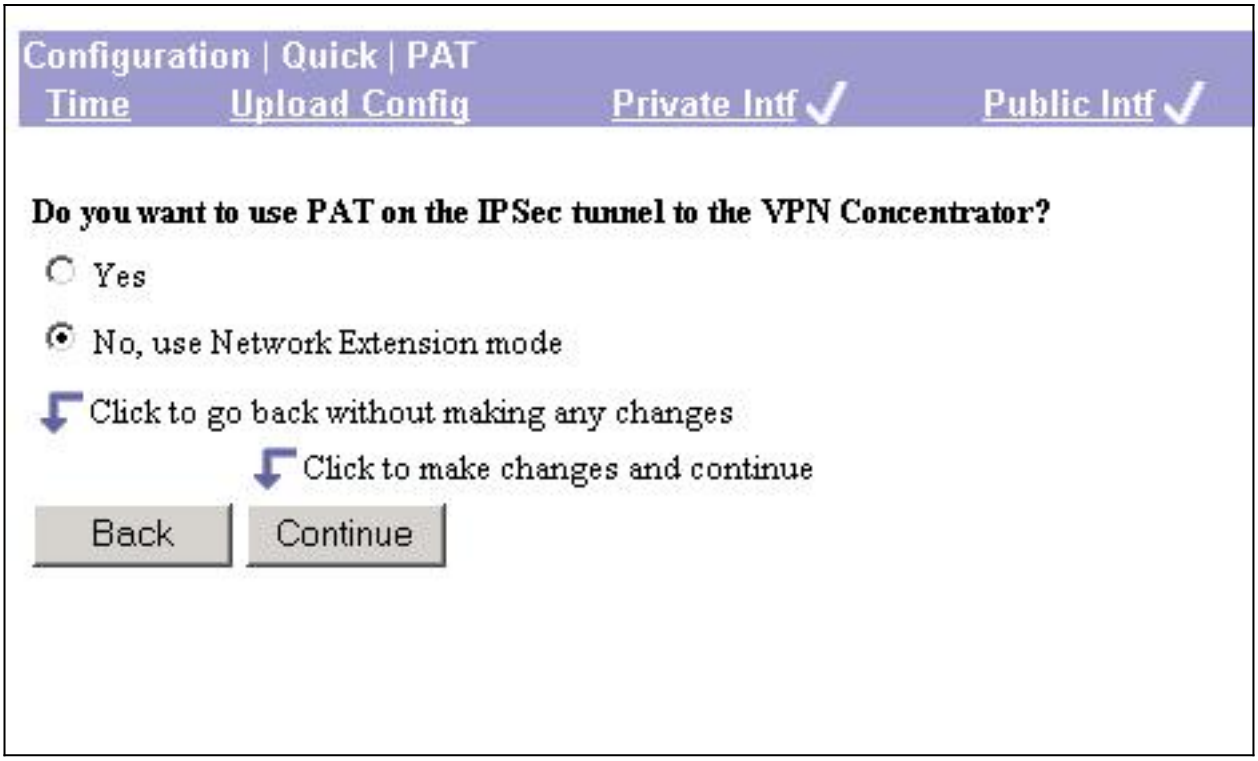
6. عينت عنوان إن يتلقى أنت ساكن إستاتيكي بتحديد **تشكيل>سريع>قارن عام>عام**.
7. من نافذة الواجهة العامة، حدد **تحديد عنوان IP** وأدخل عنوان IP المناسب وقناع الشبكة الفرعية والمدخل الافتراضي.



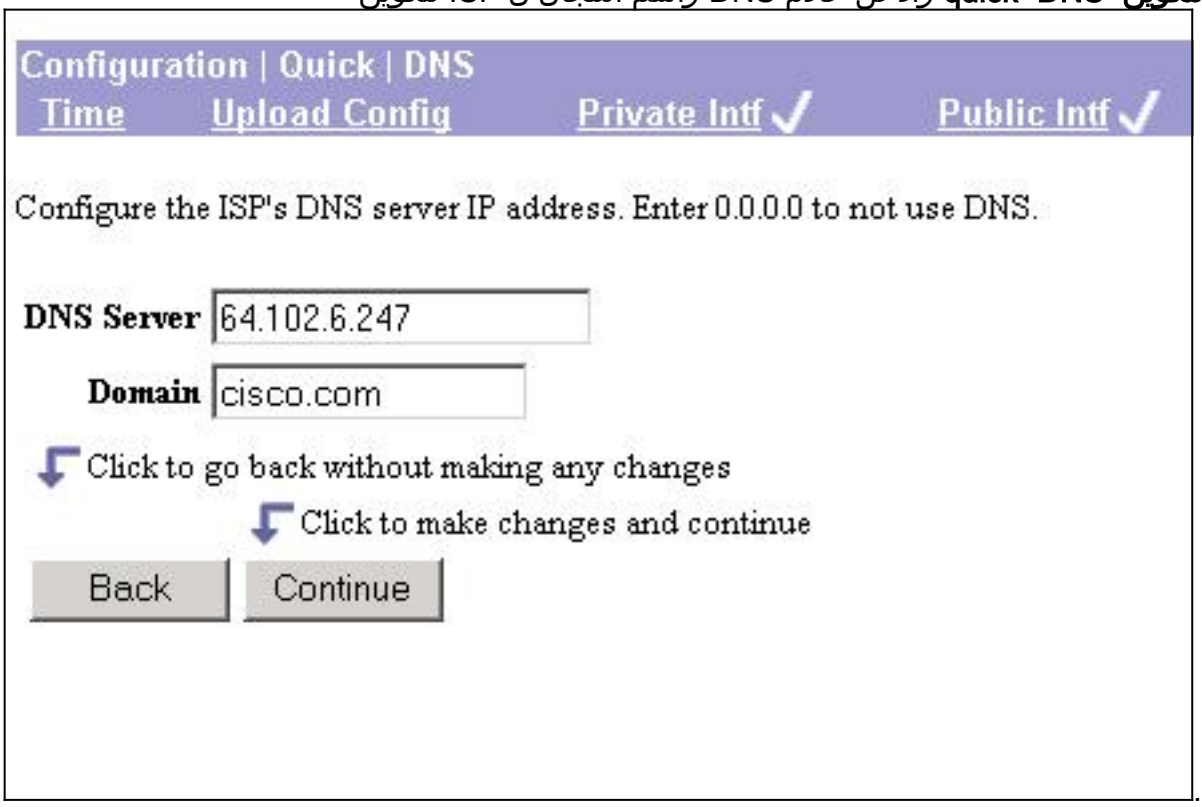
8. قم بتكوين نظير VPN البعيد (عنوان IP العام للموجه). للقيام بذلك، حدد تكوين > سريع > IPSec وأدخل مجموعة الملفات التالية لاسم المجموعة، و Cisco123 لكلمة مرور المجموعة، وfadi لاسم المستخدم، وCisco لكلمة مرور
المستخدم.



9. أخترت **تشكيل>سريع>ضرب** واخترت **لا، إستعمال شبكة ملحق أسلوب** من ال ضرب نافذة أن يشكل شبكة إمتداد
أسلوب.

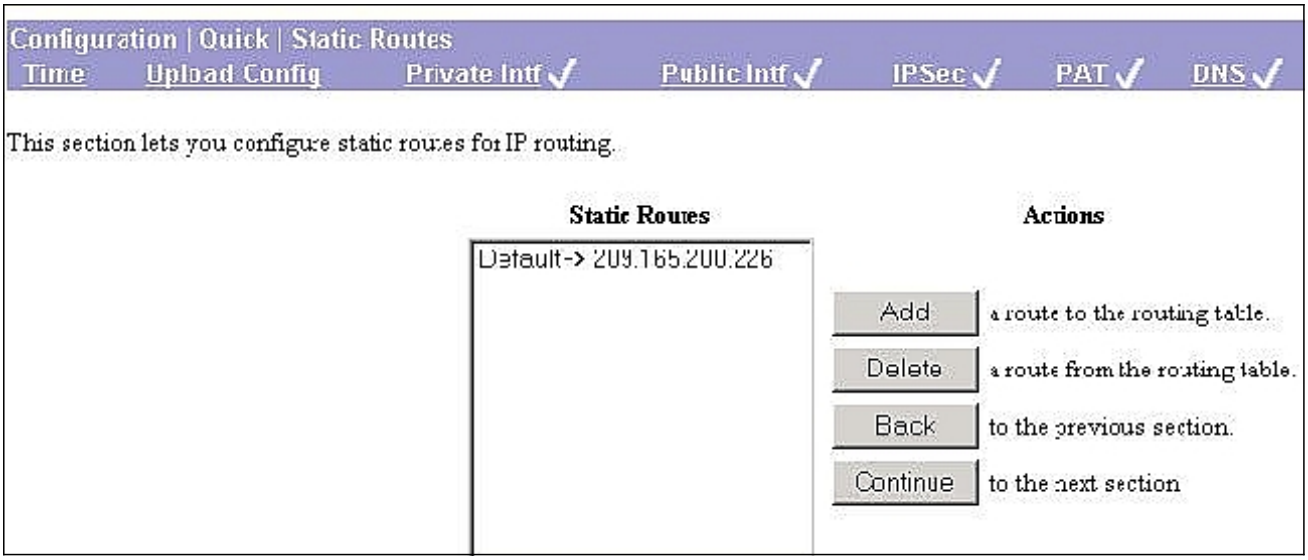


10. حدد **التكوين>DNS>quick** وأدخل خادم DNS واسم المجال ل ISP لتكوين



.DNS

11. حدد **تكوين>سريع>المسارات الثابتة** وانقر فوق **إضافة** لإضافة مسار ثابت إلى جدول التوجيه لتكوين البوابة الافتراضية لعميل
.VPN



التحقق من الصحة

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

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

ارجع إلى أستكشاف أخطاء أمان IP وإصلاحها - فهم أوامر **debug** واستخدامها لأوامر **show** ذات الصلة.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

ملاحظة: إن ضرب يمكن استعملت في cisco VPN 3002 زبون، ال reload يزيل ال username وكلمة أن يتواجد. يجب تكوين اسم المستخدم وكلمة المرور الجديدين للعميل.

ملاحظة: إن ضرب يعجز (NEM) يكون استعملت، ال reload يحتفظ ال username وكلمة provided that الرأس نهاية يكون شكلت أن ينقذ ال username وكلمة.

إجراء استكشاف الأخطاء وإصلاحها

هذه معلومات أستكشاف الأخطاء وإصلاحها المتعلقة بهذا التكوين. للحصول على معلومات إضافية حول أستكشاف الأخطاء وإصلاحها، ارجع إلى أستكشاف أخطاء أمان IP وإصلاحها - فهم أوامر **debug** واستخدامها. أكمل الخطوات التالية لاستكشاف أخطاء التكوين وإصلاحها:

1. تأكد من الاطلاع على المرحلة الأولى وإنشاء المرحلة الثانية. أستخدم الخط الأساسي **تصحيح الأخطاء** في قسم أوامر أستكشاف الأخطاء وإصلاحها.
2. ما إن يرى أنت ال SAs، أرسلت حركة مرور بين الشبكة محمي أن يختبر الموصولية.

أوامر استكشاف الأخطاء وإصلاحها

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

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

- **debug crypto ipSec**—يعرض أحداث IPSec.
- **debug crypto isakmp**—يعرض الرسائل المتعلقة بأحداث IKE.
- **debug crypto engine**—يعرض رسائل تصحيح الأخطاء حول محركات التشفير، التي تقوم بالتشفير وفك التشفير.

```
*Cisco IOS has received a request for new SA from the VPN Client.* 03:36:19: ISAKMP (0:0): *---!*
received packet from 209.165.200.225 (N) NEW SA 03:36:19: ISAKMP: local port 500, remote port
500 03:36:19: ISAKMP (0:1): (Re)Setting client xauth list userauthen and state 03:36:19: ISAKMP:
Locking CONFIG struct 0x631B752C from crypto_ikmp_config_initialize_sa, count 1 03:36:19: ISAKMP
(0:1): processing SA payload. message ID = 0 03:36:19: ISAKMP (0:1): processing ID payload.
message ID = 0 03:36:19: ISAKMP (0:1): processing vendor id payload 03:36:19: ISAKMP (0:1):
vendor ID seems Unity/DPD but bad major 03:36:19: ISAKMP (0:1): vendor ID is XAUTH 03:36:19:
ISAKMP (0:1): processing vendor id payload 03:36:19: ISAKMP (0:1): vendor ID is Unity *!--- Cisco
IOS checks the incoming ISAKMP proposal with the policy !--- defined in Cisco IOS.* 03:36:19:
ISAKMP (0:1): Checking ISAKMP transform 1 against priority 3 policy 03:36:19: ISAKMP: default
group 2 03:36:19: ISAKMP: encryption 3DES-CBC 03:36:19: ISAKMP: hash SHA 03:36:19: ISAKMP: auth
XAUTHInitPreShared 03:36:19: ISAKMP: life type in seconds 03:36:19: ISAKMP: life duration (VPI)
of 0x7F 0xFF 0xFF 0xFF 03:36:19: ISAKMP (0:1): atts are acceptable. Next payload is 3 03:36:19:
CryptoEngine0: generate alg parameter 03:36:19: CRYPTO_ENGINE: Dh phase 1 status: 0 03:36:19:
CRYPTO_ENGINE: Dh phase 1 status: 0 03:36:19: ISAKMP (0:1): processing KE payload. message ID =
0 03:36:19: CryptoEngine0: generate alg parameter 03:36:19: ISAKMP (0:1): processing NONCE
payload. message ID = 0 03:36:19: ISAKMP (0:1): processing vendor id payload 03:36:19: ISAKMP
(0:1): vendor ID seems Unity/DPD but bad major 03:36:19: ISAKMP (0:1): vendor ID is XAUTH
03:36:19: ISAKMP (0:1): processing vendor id payload 03:36:19: ISAKMP (0:1): vendor ID is Unity
03:36:19: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH Old State = IKE_READY New State
= IKE_R_AM_AAA_AWAIT 03:36:19: ISAKMP: got callback 1 03:36:19: CryptoEngine0: create ISAKMP
SKEYID for conn id 1 03:36:19: ISAKMP (0:1): SKEYID state generated 03:36:19: ISAKMP (0:1): SA
is doing pre-shared key authentication plux XAUTH using id type ID_IPV4_ADDR 03:36:19: ISAKMP
(1): ID payload next-payload : 10 type : 1 protocol : 17 port : 500 length : 8 03:36:19: ISAKMP
(1): Total payload length: 12 03:36:19: CryptoEngine0: generate hmac context for conn id 1
03:36:19: ISAKMP (0:1): sending packet to 209.165.200.225 (R) AG_INIT_EXCH 03:36:19: ISAKMP
(0:1): Input = IKE_MESG_FROM_AAA, PRESHARED_KEY_REPLY Old State = IKE_R_AM_AAA_AWAIT New State =
IKE_R_AM2 03:36:27: ISAKMP (0:1): received packet from 209.165.200.225 (R) AG_INIT_EXCH
03:36:28: ISAKMP (0:1): sending packet to 209.165.200.225 (R) AG_INIT_EXCH 03:36:28: ISAKMP
(0:1): received packet from 209.165.200.225 (R) AG_INIT_EXCH 03:36:28: ISAKMP (0:1): processing
HASH payload. message ID = 0 03:36:28: CryptoEngine0: generate hmac context for conn id 1
03:36:28: ISAKMP (0:1): processing NOTIFY INITIAL_CONTACT protocol 1 spi 0, message ID = 0, sa =
63393F7C 03:36:28: ISAKMP (0:1): Process initial contact, bring down existing phase 1 and 2 SA's
03:36:28: ISAKMP (0:1): returning IP addr to the address pool 03:36:28: ISAKMP (0:1): peer does
not do paranoid keepalives. 03:36:28: ISAKMP (0:1): processing vendor id payload 03:36:28:
ISAKMP (0:1): vendor ID is DPD *!--- Phase 1 is now complete and ISAKMP SA is negoitated.*
03:36:28: ISAKMP (0:1): SA has been authenticated with 209.165.200.225 03:36:28: CryptoEngine0:
clear dh number for conn id 1 03:36:28: CryptoEngine0: generate hmac context for conn id 1
03:36:28: ISAKMP (0:1): sending packet to 209.165.200.225 (R) QM_IDLE 03:36:28: ISAKMP (0:1):
purging node -2033367886 03:36:28: ISAKMP: Sending phase 1 responder lifetime 86400 03:36:28:
ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH Old State = IKE_R_AM2 New State =
IKE_P1_COMPLETE 03:36:28: IPSEC(key_engine): got a queue event... 03:36:28:
IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP 03:36:28:
IPSEC(key_engine_delete_sas): delete all SAs shared with 209.165.200.225 *!--- Proceed to the
Extended Authentication. !--- Remember that XAUTH is done before Phase 2 and after Phase 1.*
03:36:28: ISAKMP (0:1): Need XAUTH 03:36:28: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
IKE_PHASE1_COMPLETE Old State = IKE_P1_COMPLETE New State = IKE_XAUTH_AAA_START_LOGIN_AWAIT
03:36:28: ISAKMP: got callback 1 03:36:28: ISAKMP/xauth: request attribute XAUTH_TYPE_V2
03:36:28: ISAKMP/xauth: request attribute XAUTH_MESSAGE_V2 03:36:28: ISAKMP/xauth: request
attribute XAUTH_USER_NAME_V2 03:36:28: ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD_V2
03:36:28: CryptoEngine0: generate hmac context for conn id 1 03:36:28: ISAKMP (0:1): initiating
peer config to 209.165.200.225. ID = 1189186805 03:36:28: ISAKMP (0:1): sending packet to
209.165.200.225 (R) CONF_XAUTH 03:36:28: ISAKMP (0:1): Input = IKE_MESG_FROM_AAA,
```

IKE_AAA_START_LOGIN Old State = IKE_XAUTH_AAA_START_LOGIN_AWAIT New State = IKE_XAUTH_REQ_SENT 03:36:28: ISAKMP (0:1): received packet from 209.165.200.225 (R) CONF_XAUTH 03:36:28: ISAKMP (0:1): processing transaction payload from 209.165.200.225. message ID = 1189186805 03:36:28: CryptoEngine0: generate hmac context for conn id 1 03:36:28: ISAKMP: Config payload REPLY 03:36:28: ISAKMP/xauth: reply attribute XAUTH_USER_NAME_V2 03:36:28: ISAKMP/xauth: reply attribute XAUTH_USER_PASSWORD_V2 03:36:28: ISAKMP (0:1): deleting node 1189186805 error FALSE reason "done with xauth request/reply exchange" 03:36:28: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_CFG_REPLY Old State = IKE_XAUTH_REQ_SENT New State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT 03:36:28: ISAKMP: got callback 1 03:36:28: CryptoEngine0: generate hmac context for conn id 1 03:36:28: ISAKMP (0:1): initiating peer config to 209.165.200.225. ID = 1490194005 03:36:28: ISAKMP (0:1): sending packet to 209.165.200.225 (R) CONF_XAUTH 03:36:28: ISAKMP (0:1): Input = IKE_MESG_FROM_AAA, IKE_AAA_CONT_LOGIN Old State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT New State = IKE_XAUTH_SET_SENT 03:36:28: ISAKMP (0:1): received packet from 209.165.200.225 (R) CONF_XAUTH 03:36:28: ISAKMP (0:1): processing transaction payload from 209.165.200.225. message ID = 1490194005 03:36:28: CryptoEngine0: generate hmac context for conn id 1 03:36:28: ISAKMP: Config payload ACK 03:36:28: ISAKMP (0:1): XAUTH ACK Processed 03:36:28: ISAKMP (0:1): deleting node 1490194005 error FALSE reason "done with transaction" 03:36:28: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_CFG_ACK Old State = IKE_XAUTH_SET_SENT New State = IKE_P1_COMPLETE 03:36:28: ISAKMP (0:1): received packet from 209.165.200.225 (R) QM_IDLE 03:36:28: ISAKMP (0:1): processing transaction payload from 209.165.200.225. message ID = 113305927 03:36:28: CryptoEngine0: generate hmac context for conn id 1 03:36:28: ISAKMP: Config payload REQUEST 03:36:28: ISAKMP (0:1): checking request: 03:36:28: ISAKMP: IP4_DNS 03:36:28: ISAKMP: IP4_DNS 03:36:28: ISAKMP: IP4_NBNS 03:36:28: ISAKMP: IP4_NBNS 03:36:28: ISAKMP: SPLIT_INCLUDE 03:36:28: ISAKMP: DEFAULT_DOMAIN 03:36:28: ISAKMP: UNKNOWN Unknown Attr: 0x7005 03:36:28: ISAKMP: UNKNOWN Unknown Attr: 0x7007 03:36:28: ISAKMP: UNKNOWN Unknown Attr: 0x7800 03:36:28: ISAKMP: UNKNOWN Unknown Attr: 0x7801 03:36:28: ISAKMP: UNKNOWN Unknown Attr: 0x7802 03:36:28: ISAKMP: UNKNOWN Unknown Attr: 0x7803 03:36:28: ISAKMP: UNKNOWN Unknown Attr: 0x7804 03:36:28: ISAKMP: UNKNOWN Unknown Attr: 0x7805 03:36:28: ISAKMP: UNKNOWN Unknown Attr: 0x7806 03:36:28: ISAKMP: UNKNOWN Unknown Attr: 0x7009 03:36:28: ISAKMP: APPLICATION_VERSION 03:36:28: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_CFG_REQUEST Old State = IKE_P1_COMPLETE New State = IKE_CONFIG_AUTHOR_AAA_AWAIT 03:36:28: ISAKMP (0:1): Unknown Input: state = IKE_CONFIG_AUTHOR_AAA_AWAIT, major, minor = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE 03:36:28: ISAKMP: got callback 1 03:36:28: ISAKMP (0:1): Config attributes requested butconfig attributes not in crypto map. Sending empty reply. 03:36:28: ISAKMP (0:1): attributes sent in message: 03:36:28: ISAKMP: Unknown Attr: UNKNOWN (0x7005) 03:36:28: ISAKMP: Unknown Attr: UNKNOWN (0x7007) 03:36:28: ISAKMP: Unknown Attr: UNKNOWN (0x7800) 03:36:28: ISAKMP: Unknown Attr: UNKNOWN (0x7801) 03:36:28: ISAKMP: Unknown Attr: UNKNOWN (0x7802) 03:36:28: ISAKMP: Unknown Attr: UNKNOWN (0x7803) 03:36:28: ISAKMP: Unknown Attr: UNKNOWN (0x7804) 03:36:28: ISAKMP: Unknown Attr: UNKNOWN (0x7805) 03:36:28: ISAKMP: Unknown Attr: UNKNOWN (0x7806) 03:36:28: ISAKMP: Unknown Attr: UNKNOWN (0x7009) 03:36:28: ISAKMP: Sending APPLICATION_VERSION string: Cisco Internetwork Operating System Software IOS (tm) 3600 Software (C3640-JK9S-M), Version 12.2(8)T1, RELEASE SOFTWARE (fc2) TAC Support: http://www.cisco.com/tac Copyright (c) 1986-2002 by cisco Systems, Inc. Compiled Sun 31-Mar-02 03:30 by ccai 03:36:28: CryptoEngine0: generate hmac context for conn id 1 03:36:28: ISAKMP (0:1): responding to peer config from 209.165.200.225. ID = 113305927 03:36:28: ISAKMP (0:1): sending packet to 209.165.200.225 (R) CONF_ADDR 03:36:28: ISAKMP (0:1): deleting node 113305927 error FALSE reason "" 03:36:28: ISAKMP (0:1): Input = IKE_MESG_FROM_AAA, IKE_AAA_GROUP_ATTR Old State = IKE_CONFIG_AUTHOR_AAA_AWAIT New State = IKE_P1_COMPLETE 03:36:28: ISAKMP (0:1): received packet from 209.165.200.225 (R) QM_IDLE 03:36:28: CryptoEngine0: generate hmac context for conn id 1 03:36:28: ISAKMP (0:1): processing HASH payload. message ID = 1022849755 03:36:28: ISAKMP (0:1): processing SA payload. message ID = 1022849755 *!--- ISAKMP now verifies the IPSec proposal !--- to see if it is acceptable.* 03:36:28: ISAKMP (0:1): Checking IPSec proposal 1 03:36:28: ISAKMP: transform 1, ESP_3DES 03:36:28: ISAKMP: attributes in transform: 03:36:28: ISAKMP: SA life type in seconds 03:36:28: ISAKMP: SA life duration (VPI) of 0x7F 0xFF 0xFF 0xFF 03:36:28: ISAKMP: encaps is 1 03:36:28: ISAKMP: authenticator is HMAC-SHA 03:36:28: validate proposal 0 03:36:28: ISAKMP (0:1): atts are acceptable. *!--- As the attributes are acceptable, ISAKMP asks !--- IPSec to validate the proposal.* 03:36:28: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 209.165.202.129, remote= 209.165.200.225, local_proxy= 209.165.202.129/255.255.255.255/0/0 (type=1), remote_proxy= 209.165.200.225/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-3des esp-sha-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 03:36:28: validate proposal request 0 03:36:28: ISAKMP (0:1): processing NONCE payload. message ID = 1022849755 03:36:28: ISAKMP (0:1): processing ID payload. message ID = 1022849755 03:36:28: ISAKMP (0:1): processing ID payload. message ID = 1022849755 03:36:28: ISAKMP (0:1): asking for 1 spis from ipsec 03:36:28: ISAKMP (0:1): Node 1022849755,

Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE
03:36:28: IPSEC(key_engine): got a queue event... 03:36:28: IPSEC(spi_response): getting spi
1910172102 for SA from 209.165.202.129 to 209.165.200.225 for prot 3 03:36:28: ISAKMP: received
ke message (2/1) 03:36:28: CryptoEngine0: generate hmac context for conn id 1 03:36:28: ISAKMP
(0:1): sending packet to 209.165.200.225 (R) QM_IDLE 03:36:28: ISAKMP (0:1): Node 1022849755,
Input = IKE_MESG_FROM_IPSEC, IKE_SPI_REPLY Old State = IKE_QM_SPI_STARVE New State =
IKE_QM_R_QM2 03:36:28: ISAKMP (0:1): received packet from 209.165.200.225 (R) QM_IDLE 03:36:28:
CryptoEngine0: generate hmac context for conn id 1 03:36:28: ipsec allocate flow 0 03:36:28:
ipsec allocate flow 0 *!--- After IPSec validates the proposal, !--- IPSec proceeds to create the IPSec SAs.* 03:36:28: ISAKMP (0:1): Creating IPSec SAs 03:36:28: inbound SA from 209.165.200.225
to 209.165.202.129 (proxy 209.165.200.225 to 209.165.202.129) 03:36:28: has spi 0x71DAE9C6 and
conn_id 2000 and flags 4 03:36:28: lifetime of 2147483647 seconds 03:36:28: outbound SA from
209.165.202.129 to 209.165.200.225 (proxy 209.165.202.129 to 209.165.200.225) 03:36:28: has spi
101033821 and conn_id 2001 and flags C 03:36:28: lifetime of 2147483647 seconds 03:36:28: ISAKMP
(0:1): deleting node 1022849755 error FALSE reason "quick mode done (await()" 03:36:28: ISAKMP
(0:1): Node 1022849755, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH Old State = IKE_QM_R_QM2 New
State = IKE_QM_PHASE2_COMPLETE 03:36:28: IPSEC(key_engine): got a queue event... 03:36:28:
IPSEC(initialize_sas): , (key eng. msg.) INBOUND local= 209.165.202.129, remote=
209.165.200.225, *!--- This is the management tunnel.* **local_proxy= 209.165.202.129/0.0.0.0/0/0**
,((type=1
,(remote_proxy= 209.165.200.225/0.0.0.0/0/0 (type=1
, protocol= ESP, transform= esp-3des esp-sha-hmac
,lifedur= 2147483647s and 0kb
spi= 0x71DAE9C6(1910172102), conn_id= 2000, keysize= 0, flags= 0x4
, :(IPSEC(initialize_sas :03:36:28
,key eng. msg.) OUTBOUND local= 209.165.202.129, remote= 209.165.200.225)
,(local_proxy= 209.165.202.129/0.0.0.0/0/0 (type=1
,(remote_proxy= 209.165.200.225/0.0.0.0/0/0 (type=1
,protocol= ESP, transform= esp-3des esp-sha-hmac
,lifedur= 2147483647s and 0kb
spi= 0x605A75D(101033821), conn_id= 2001, keysize= 0, flags= 0xC
,IPSEC(create_sa): sa created :03:36:28
,sa) sa_dest= 209.165.202.129, sa_prot= 50)
,(sa_spi= 0x71DAE9C6(1910172102
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 2000
,IPSEC(create_sa): sa created :03:36:28
,sa) sa_dest= 209.165.200.225, sa_prot= 50)
,(sa_spi= 0x605A75D(101033821
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 2001
(ISAKMP: received ke message (4/1 :03:36:28
ISAKMP: Locking CONFIG struct 0x631B752C for :03:36:28
crypto_ikmp_config_handle_kei_mess, count 2
ISAKMP (0:1): received packet from 209.165.200.225 (R) QM_IDLE :03:36:32
CryptoEngine0: generate hmac context for conn id 1 :03:36:32
ISAKMP (0:1): processing HASH payload. message ID = 852253052 :03:36:32
ISAKMP (0:1): processing SA payload. message ID = 852253052 :03:36:32
ISAKMP (0:1): Checking IPSec proposal 1 :03:36:32
ISAKMP: transform 1, ESP_3DES :03:36:32
:ISAKMP: attributes in transform :03:36:32
ISAKMP: SA life type in seconds :03:36:32
ISAKMP: SA life duration (VPI) of 0x7F 0xFF 0xFF 0xFF :03:36:32
ISAKMP: encaps is 1 :03:36:32
ISAKMP: authenticator is HMAC-SHA :03:36:32
validate proposal 0 :03:36:32
.ISAKMP (0:1): atts are acceptable :03:36:32
,IPSEC(validate_proposal_request): proposal part #1 :03:36:32
,key eng. msg.) INBOUND local= 209.165.202.129, remote= 209.165.200.225)
,(local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4
,(remote_proxy= 10.48.66.0/255.255.254.0/0/0 (type=4
, protocol= ESP, transform= esp-3des esp-sha-hmac
,lifedur= 0s and 0kb
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
validate proposal request 0 :03:36:32
ISAKMP (0:1): processing NONCE payload. message ID = 852253052 :03:36:32

```
                    ISAKMP (0:1): processing ID payload. message ID = 852253052 :03:36:32
                    ISAKMP (0:1): processing ID payload. message ID = 852253052 :03:36:32
                                ISAKMP (0:1): asking for 1 spis from ipsec :03:36:32
          ISAKMP (0:1): Node 852253052, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH :03:36:32
                                Old State = IKE_QM_READY  New State = IKE_QM_SPI_STARVE
                                      ...IPSEC(key_engine): got a queue event :03:36:32
                                IPSEC(spi_response): getting spi 3997625134 for SA :03:36:32
                                  from 209.165.202.129 to 209.165.200.225 for prot 3
                                                (ISAKMP: received ke message (2/1 :03:36:32
                                CryptoEngine0: generate hmac context for conn id 1 :03:36:32
                    ISAKMP (0:1): sending packet to 209.165.200.225 (R) QM_IDLE :03:36:32
        ISAKMP (0:1): Node 852253052, Input = IKE_MESG_FROM_IPSEC, IKE_SPI_REPLY :03:36:32
                                Old State = IKE_QM_SPI_STARVE  New State = IKE_QM_R_QM2
                ISAKMP (0:1): received packet from 209.165.200.225 (R) QM_IDLE :03:36:32
                                CryptoEngine0: generate hmac context for conn id 1 :03:36:32
                                                    ipsec allocate flow 0 :03:36:32
                                                    ipsec allocate flow 0 :03:36:32
                                                ISAKMP (0:1): Creating IPSec SAs :03:36:32
                     inbound SA from 209.165.200.225 to 209.165.202.129         :03:36:32
                                                (proxy 10.48.66.0 to 0.0.0.0)
                        has spi 0xEE46EB2E and conn_id 2002 and flags 4         :03:36:32
                                            lifetime of 2147483647 seconds      :03:36:32
                    outbound SA from 209.165.202.129 to 209.165.200.225         :03:36:32
                                                    (proxy 0.0.0.0 to 10.48.66.0)
                         has spi 674305339 and conn_id 2003 and flags C         :03:36:32
                                            lifetime of 2147483647 seconds      :03:36:32
"()ISAKMP (0:1): deleting node 852253052 error FALSE reason "quick mode done (await :03:36:32
          ISAKMP (0:1): Node 852253052, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH :03:36:32
                                Old State = IKE_QM_R_QM2  New State = IKE_QM_PHASE2_COMPLETE
                                      ...IPSEC(key_engine): got a queue event :03:36:32
   IPSec now initializes the SAs as these are !--- stored in the SA Database. 03:36:32: ---!
             IPSEC(initialize_sas): , (key eng. msg.) INBOUND local= 209.165.202.129, remote=
209.165.200.225, !--- This SA is for the actual data traffic between the !--- networks behind
          ,(the VPN Client and the Cisco IOS router. local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4
                                    ,(remote_proxy= 10.48.66.0/255.255.254.0/0/0 (type=4
                                          , protocol= ESP, transform= esp-3des esp-sha-hmac
                                                    ,lifedur= 2147483647s and 0kb
                    spi= 0xEE46EB2E(3997625134), conn_id= 2002, keysize= 0, flags= 0x4
                                                    , :(IPSEC(initialize_sas :03:36:32
               ,key eng. msg.) OUTBOUND local= 209.165.202.129, remote= 209.165.200.225)
                                        ,(local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4
                                    ,(remote_proxy= 10.48.66.0/255.255.254.0/0/0 (type=4
                                       , protocol= ESP, transform= esp-3des esp-sha-hmac
                                                    ,lifedur= 2147483647s and 0kb
                     spi= 0x2831153B(674305339), conn_id= 2003, keysize= 0, flags= 0xC
                                                ,IPSEC(create_sa): sa created :03:36:32
                                          ,sa) sa_dest= 209.165.202.129, sa_prot= 50)
                                                ,(sa_spi= 0xEE46EB2E(3997625134
                                  sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 2002
                                                ,IPSEC(create_sa): sa created :03:36:32
                                          ,sa) sa_dest= 209.165.200.225, sa_prot= 50)
                                                ,(sa_spi= 0x2831153B(674305339
                                  sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 2003
                                                (ISAKMP: received ke message (4/1 :03:36:32
                                  ISAKMP: Locking CONFIG struct 0x631B752C for :03:36:32
                                           crypto_ikmp_config_handle_kei_mess, count 3
```

تصحيح أخطاء عميل الأجهزة VPN 3002

من واجهة المستخدم الرسومية (GUI) الخاصة بعميل شبكة VPN، حدد تكوين > نظام > أحداث > فئات وتمكين IKE، و IKEDBG، و IPSec، و IPSECDBG في المستوى 13 إلى syslog. تذكر أن تقوم بتعطيل تصحيح الأخطاء بعد اكتمال الاختبار.

تصحيح أخطاء عميل الأجهزة VPN 3002

```
    SEV=7 IPSECDBG/14 RPT=3 11:02:30.100 06/03/2002 297
 The VPN Client attempts to connect to the headend. ---!
 !--- In this case, it is Cisco IOS. Sending KEY_ACQUIRE
 to IKE for src 209.165.200.225, dst 209.165.202.129 298
 06/03/2002 11:02:30.100 SEV=8 IKEDBG/0 RPT=108 pitcher:
         received a key acquire message! 299 06/03/2002
   11:02:30.100 SEV=4 IKE/41 RPT=135 209.165.202.129 IKE
Initiator: New Phase 1, Intf 2, IKE Peer 209.165.202.129
       local Proxy Address 209.165.200.225, remote Proxy
          Address 209.165.202.129, SA (ESP-3DES-MD5) 302
          06/03/2002 11:02:30.100 SEV=9 IKEDBG/0 RPT=109
      209.165.202.129 constructing ISA_SA for isakmp 303
          06/03/2002 11:02:30.230 SEV=9 IKEDBG/0 RPT=110
  209.165.202.129 constructing ke payload 304 06/03/2002
      11:02:30.230 SEV=9 IKEDBG/1 RPT=30 209.165.202.129
  constructing nonce payload 305 06/03/2002 11:02:30.230
   SEV=9 IKEDBG/1 RPT=31 209.165.202.129 constructing ID
       306 06/03/2002 11:02:30.230 SEV=9 IKEDBG/46 RPT=4
   209.165.202.129 constructing xauth V6 VID payload 307
          06/03/2002 11:02:30.230 SEV=9 IKEDBG/46 RPT=5
 209.165.202.129 constructing VID payload 308 06/03/2002
 11:02:30.230 SEV=9 IKEDBG/48 RPT=2 209.165.202.129 Send
Cisco Unity client VID 309 06/03/2002 11:02:30.230 SEV=8
        IKEDBG/0 RPT=111 209.165.202.129 SENDING Message
 (msgid=0) with payloads : HDR + SA (1) + KE (4) + NONCE
   (10) + ID (5) + VENDOR (13) + VENDOR (13) + NONE ( 0)
... total length : 541 312 06/03/2002 11:02:30.520 SEV=8
       IKEDBG/0 RPT=112 209.165.202.129 RECEIVED Message
  (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) +
   VENDOR (13) + VENDOR (13) + VENDOR (13) + KE (4) + ID
 (5) + NONCE (10) + HASH (8) + NONE (0) ... total length
: 348 315 06/03/2002 11:02:30.530 SEV=8 IKEDBG/0 RPT=113
209.165.202.129 RECEIVED Message (msgid=0) with payloads
: HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13)
 + VENDOR (13) + KE (4) + ID (5) + NONCE (10) + HASH (8)
        + NONE (0) ... total length : 348 318 06/03/2002
     11:02:30.530 SEV=9 IKEDBG/0 RPT=114 209.165.202.129
 processing SA payload 319 06/03/2002 11:02:30.530 SEV=7
     IKEDBG/0 RPT=115 209.165.202.129 Oakley proposal is
  acceptable 320 06/03/2002 11:02:30.530 SEV=9 IKEDBG/47
        RPT=5 209.165.202.129 processing VID payload 321
           06/03/2002 11:02:30.530 SEV=9 IKEDBG/49 RPT=4
     209.165.202.129 Received Cisco Unity client VID 322
           06/03/2002 11:02:30.530 SEV=9 IKEDBG/47 RPT=6
   209.165.202.129 processing VID payload 323 06/03/2002
      11:02:30.530 SEV=9 IKEDBG/49 RPT=5 209.165.202.129
      Received DPD VID 324 06/03/2002 11:02:30.530 SEV=9
  IKEDBG/47 RPT=7 209.165.202.129 processing VID payload
       325 06/03/2002 11:02:30.530 SEV=9 IKEDBG/38 RPT=2
    209.165.202.129 Processing IOS/PIX Vendor ID payload
 (version: 1.0.0, capabilities: 0000007f) 326 06/03/2002
      11:02:30.530 SEV=9 IKEDBG/47 RPT=8 209.165.202.129
processing VID payload 327 06/03/2002 11:02:30.530 SEV=9
     IKEDBG/49 RPT=6 209.165.202.129 !--- The VPN Client
    understands that it needs !--- to go through Extended
     authentication to !--- bring the tunnel up. Received
 xauth V6 VID 328 06/03/2002 11:02:30.530 SEV=9 IKEDBG/0
       RPT=116 209.165.202.129 processing ke payload 329
          06/03/2002 11:02:30.530 SEV=9 IKEDBG/0 RPT=117
        209.165.202.129 processing ISA_KE 330 06/03/2002
      11:02:30.530 SEV=9 IKEDBG/1 RPT=32 209.165.202.129
```

```
Processing ID 331 06/03/2002 11:02:30.530 SEV=9 IKEDBG/1
     RPT=33 209.165.202.129 processing nonce payload 332
          06/03/2002 11:02:30.660 SEV=9 IKEDBG/0 RPT=118
    209.165.202.129 Generating keys for Initiator... 333
          06/03/2002 11:02:30.670 SEV=9 IKEDBG/0 RPT=119
 209.165.202.129 Group [209.165.202.129] processing hash
      334 06/03/2002 11:02:30.670 SEV=9 IKEDBG/0 RPT=120
  209.165.202.129 Group [209.165.202.129] computing hash
335 06/03/2002 11:02:30.680 SEV=9 IKEDBG/0 RPT=121 Group
 [209.165.202.129] construct hash payload 336 06/03/2002
     11:02:30.680 SEV=9 IKEDBG/0 RPT=122 209.165.202.129
   Group [209.165.202.129] computing hash 337 06/03/2002
11:02:30.680 SEV=9 IKEDBG/46 RPT=6 209.165.202.129 Group
      [209.165.202.129] constructing dpd vid payload 338
          06/03/2002 11:02:30.680 SEV=8 IKEDBG/0 RPT=123
 209.165.202.129 SENDING Message (msgid=0) with payloads
 : HDR + HASH (8) + NOTIFY (11) + VENDOR (13) + NONE (0)
... total length : 100 340 06/03/2002 11:02:30.690 SEV=8
       IKEDBG/0 RPT=124 209.165.202.129 RECEIVED Message
(msgid=71c8c9fd) with payloads : HDR + HASH (8) + NOTIFY
    (11) + NONE (0) ... total length : 92 342 06/03/2002
     11:02:30.690 SEV=9 IKEDBG/0 RPT=125 209.165.202.129
  Group [209.165.202.129] processing hash 343 06/03/2002
     11:02:30.690 SEV=9 IKEDBG/0 RPT=126 209.165.202.129
   Group [209.165.202.129] Processing Notify payload 344
             06/03/2002 11:02:30.690 SEV=5 IKE/73 RPT=19
 209.165.202.129 Group [209.165.202.129] !--- As IOS has
    a default IKE time of 1 day (86400) seconds !--- and
forces the VPN Client to accept this value. !--- This is
because Cisco IOS responds and the VPN Client initiates.
  Responder forcing change of IKE rekeying duration from
 2147483647 to 86400 seconds 347 06/03/2002 11:02:30.690
    SEV=6 IKE/0 RPT=2 AM AM:843f96f6 received unexpected
   event EV_RESET_LIFETIME in state AM_RSND_LST_ MSG 349
          06/03/2002 11:02:30.700 SEV=8 IKEDBG/0 RPT=127
  209.165.202.129 RECEIVED Message (msgid=ecb5af46) with
    payloads : HDR + HASH (8) + ATTR (14) + NONE (0) ...
     total length : 86 351 06/03/2002 11:02:30.700 SEV=9
   IKEDBG/1 RPT=34 process_attr(): Enter! 352 06/03/2002
       11:02:30.700 SEV=9 IKEDBG/1 RPT=35 Processing cfg
    Request attributes 353 06/03/2002 11:02:30.700 SEV=9
     IKEDBG/1 RPT=36 Received Xauth Type in request! 354
  06/03/2002 11:02:30.700 SEV=9 IKEDBG/1 RPT=37 Received
        Xauth Message! 355 06/03/2002 11:02:30.700 SEV=9
    IKEDBG/1 RPT=38 Received Xauth Username request! 356
  06/03/2002 11:02:30.700 SEV=9 IKEDBG/1 RPT=39 Received
     Xauth Password request! 357 06/03/2002 11:02:30.700
           SEV=9 IKEDBG/0 RPT=128 209.165.202.129 Group
[209.165.202.129] constructing blank hash 358 06/03/2002
     11:02:30.700 SEV=9 IKEDBG/0 RPT=129 209.165.202.129
        Group [209.165.202.129] constructing qm hash 359
          06/03/2002 11:02:30.700 SEV=8 IKEDBG/0 RPT=130
   209.165.202.129 SENDING Message (msgid=ecb5af46) with
    payloads : HDR + HASH (8) + ATTR (14) + NONE (0) ...
     total length : 77 361 06/03/2002 11:02:30.710 SEV=8
       IKEDBG/0 RPT=131 209.165.202.129 RECEIVED Message
  (msgid=ad808e58) with payloads : HDR + HASH (8) + ATTR
    (14) + NONE (0) ... total length : 64 363 06/03/2002
      11:02:30.710 SEV=9 IKEDBG/1 RPT=40 process_attr():
Enter! 364 06/03/2002 11:02:30.710 SEV=9 IKEDBG/1 RPT=41
        Processing cfg Request attributes 365 06/03/2002
11:02:30.710 SEV=9 IKEDBG/1 RPT=42 Received Xauth Status
 Set! 366 06/03/2002 11:02:30.710 SEV=9 IKEDBG/0 RPT=132
    209.165.202.129 Group [209.165.202.129] constructing
```

```
   blank hash 367 06/03/2002 11:02:30.710 SEV=9 IKEDBG/0
         RPT=133 209.165.202.129 Group [209.165.202.129]
  constructing qm hash 368 06/03/2002 11:02:30.710 SEV=8
        IKEDBG/0 RPT=134 209.165.202.129 SENDING Message
  (msgid=ad808e58) with payloads : HDR + HASH (8) + ATTR
    (14) + NONE (0) ... total length : 60 370 06/03/2002
     11:02:30.720 SEV=9 IKEDBG/0 RPT=135 209.165.202.129
     Group [209.165.202.129] constructing blank hash 371
          06/03/2002 11:02:30.720 SEV=9 IKEDBG/0 RPT=136
 209.165.202.129 Group [209.165.202.129] constructing qm
 hash 372 06/03/2002 11:02:30.720 SEV=8 IKEDBG/0 RPT=137
   209.165.202.129 SENDING Message (msgid=30ce63a8) with
    payloads : HDR + HASH (8) + ATTR (14) + NONE (0) ...
    total length : 231 374 06/03/2002 11:02:30.740 SEV=8
       IKEDBG/0 RPT=138 209.165.202.129 RECEIVED Message
  (msgid=30ce63a8) with payloads : HDR + HASH (8) + ATTR
   (14) + NONE (0) ... total length : 313 376 06/03/2002
      11:02:30.740 SEV=9 IKEDBG/1 RPT=43 process_attr():
Enter! 377 06/03/2002 11:02:30.740 SEV=9 IKEDBG/1 RPT=44
Processing MODE_CFG Reply attributes !--- The VPN Client
  processes the mode !--- configuration reply attributes
    sent by Cisco IOS. 378 06/03/2002 11:02:30.740 SEV=6
   IKE/130 RPT=2 209.165.202.129 Group [209.165.202.129]
  Received unsupported transaction mode attribute: 7 379
            06/03/2002 11:02:30.740 SEV=5 IKE/115 RPT=7
 209.165.202.129 Group [209.165.202.129] Client rejected
     NAT enabled IPSec request, falling back to standard
   IPSec 381 06/03/2002 11:02:30.740 SEV=3 AUTH/24 RPT=7
  Tunnel to headend device 209.165.202.129 connected 382
          06/03/2002 11:02:30.740 SEV=9 IKEDBG/0 RPT=139
    209.165.202.129 Group [209.165.202.129] Oakley begin
    quick mode 383 06/03/2002 11:02:30.740 SEV=4 IKE/119
RPT=7 209.165.202.129 Group [209.165.202.129] !--- Phase
1 is complete. 384 06/03/2002 11:02:30.740 SEV=6 IKE/121
          RPT=2 209.165.202.129 Keep-alive type for this
       connection: DPD 385 06/03/2002 11:02:30.740 SEV=7
IKEDBG/0 RPT=140 209.165.202.129 Group [209.165.202.129]
         Starting phase 1 rekey timer: 73440000 (ms) 386
   06/03/2002 11:02:30.740 SEV=9 IPSECDBG/6 RPT=15 IPSEC
     key message parse - msgtype 6, len 200, vers 1, pid
00000000, seq 13, err 0, type 2, mode 0, state 32, label
    0, pad 0, spi 00000000, encrKeyLen 0, hashKey Len 0,
ivlen 0, alg 0, hmacAlg 0, lifetype 0, lifetime1 662488,
lifetime2 0, dsI d 300 390 06/03/2002 11:02:30.740 SEV=9
        IPSECDBG/1 RPT=47 Processing KEY_GETSPI msg! 391
06/03/2002 11:02:30.740 SEV=7 IPSECDBG/13 RPT=3 Reserved
        SPI 1608220759 392 06/03/2002 11:02:30.740 SEV=8
       IKEDBG/6 RPT=3 IKE got SPI from key engine: SPI =
   0x5fdb8057 393 06/03/2002 11:02:30.750 SEV=9 IKEDBG/0
  RPT=141 209.165.202.129 Group [209.165.202.129] oakley
constucting quick mode 394 06/03/2002 11:02:30.750 SEV=9
IKEDBG/0 RPT=142 209.165.202.129 Group [209.165.202.129]
     constructing blank hash 395 06/03/2002 11:02:30.750
           SEV=9 IKEDBG/0 RPT=143 209.165.202.129 Group
     [209.165.202.129] constructing ISA_SA for ipsec 396
          06/03/2002 11:02:30.750 SEV=9 IKEDBG/1 RPT=45
    209.165.202.129 Group [209.165.202.129] constructing
   ipsec nonce payload 397 06/03/2002 11:02:30.750 SEV=9
 IKEDBG/1 RPT=46 209.165.202.129 Group [209.165.202.129]
 constructing proxy ID 398 06/03/2002 11:02:30.750 SEV=7
IKEDBG/0 RPT=144 209.165.202.129 Group [209.165.202.129]
         Transmitting Proxy Id: !--- This is the SA for
   management between !--- the VPN Client and Cisco IOS.
       Local host:  209.165.200.225  Protocol 0  Port 0
```

```
      Remote host: 209.165.202.129  Protocol 0  Port 0
      SEV=9 IKEDBG/0 RPT=145 11:02:30.750 06/03/2002 402
                                              209.165.202.129
                                    [Group [209.165.202.129
                                       constructing qm hash
      SEV=8 IKEDBG/0 RPT=146 11:02:30.750 06/03/2002 403
                                              209.165.202.129
        : SENDING Message (msgid=e429a70e) with payloads
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) +
                                    NONE (0) ... total leng
                                                  th : 292
      SEV=8 IKEDBG/0 RPT=147 11:02:31.010 06/03/2002 406
                                              209.165.202.129
       : RECEIVED Message (msgid=e429a70e) with payloads
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) +
                                     (NOTIFY (11) + NONE (0
                                     total length : 192 ...
      SEV=9 IKEDBG/0 RPT=148 11:02:31.010 06/03/2002 409
                                              209.165.202.129
                                    [Group [209.165.202.129
                                              processing hash
      SEV=9 IKEDBG/0 RPT=149 11:02:31.010 06/03/2002 410
                                              209.165.202.129
                                    [Group [209.165.202.129
                                       processing SA payload
       SEV=9 IKEDBG/1 RPT=47 11:02:31.020 06/03/2002 411
                                              209.165.202.129
                                    [Group [209.165.202.129
                                   processing nonce payload
       SEV=9 IKEDBG/1 RPT=48 11:02:31.020 06/03/2002 412
                                              209.165.202.129
                                    [Group [209.165.202.129
                                                Processing ID
       SEV=9 IKEDBG/1 RPT=49 11:02:31.020 06/03/2002 413
                                              209.165.202.129
                                    [Group [209.165.202.129
                                                Processing ID
      SEV=9 IKEDBG/0 RPT=150 11:02:31.020 06/03/2002 414
                                              209.165.202.129
                                    [Group [209.165.202.129
                                  Processing Notify payload
         SEV=5 IKE/73 RPT=20 11:02:31.020 06/03/2002 415
                                              209.165.202.129
                                    [Group [209.165.202.129
Responder forcing change of IPSec rekeying duration from
                                    2147483647 to 3600 seco
                                                        nds
      SEV=9 IKEDBG/0 RPT=151 11:02:31.020 06/03/2002 418
                                              209.165.202.129
                                    [Group [209.165.202.129
                                      loading all IPSEC SAs
       SEV=9 IKEDBG/1 RPT=50 11:02:31.020 06/03/2002 419
                                              209.165.202.129
                                    [Group [209.165.202.129
                                 !Generating Quick Mode Key
       SEV=9 IKEDBG/1 RPT=51 11:02:31.020 06/03/2002 420
                                              209.165.202.129
                                    [Group [209.165.202.129
                                 !Generating Quick Mode Key
      SEV=7 IKEDBG/0 RPT=152 11:02:31.020 06/03/2002 421
                                              209.165.202.129
                                    [Group [209.165.202.129
                                                :Loading host
                                     Dst: 209.165.202.129
```

```
                                        Src: 209.165.200.225
        SEV=4 IKE/49 RPT=13 11:02:31.020 06/03/2002 423
                                                209.165.202.129
                                    [Group [209.165.202.129
(Security negotiation complete for peer (209.165.202.129
     Initiator, Inbound SPI = 0x5fdb8057, Outbound SPI =
                                                0xa088f2dc
      SEV=9 IKEDBG/0 RPT=153 11:02:31.020 06/03/2002 426
                                                209.165.202.129
                                    [Group [209.165.202.129
                    oakley constructing final quick mode
      SEV=8 IKEDBG/0 RPT=154 11:02:31.030 06/03/2002 427
                                                209.165.202.129
        : SENDING Message (msgid=e429a70e) with payloads
         HDR + HASH (8) + NONE (0) ... total length : 76
     SEV=9 IPSECDBG/6 RPT=16 11:02:31.030 06/03/2002 429
   IPSEC key message parse - msgtype 1, len 612, vers 1,
                                 pid 00000000, seq 0, err 0
         type 2, mode 1, state 64, label 0, pad 0, spi ,
                             a088f2dc, encrKeyLen 24, hashKey
Len 20, ivlen 8, alg 2, hmacAlg 4, lifetype 0, lifetime1
                                    662488, lifetime2 0, ds
                                                Id -378167296
     SEV=9 IPSECDBG/1 RPT=48 11:02:31.030 06/03/2002 433
                                    !Processing KEY_ADD msg
     SEV=9 IPSECDBG/1 RPT=49 11:02:31.030 06/03/2002 434
                                key_msghdr2secassoc(): Enter
     SEV=7 IPSECDBG/1 RPT=50 11:02:31.030 06/03/2002 435
                                  No USER filter configured
     SEV=9 IPSECDBG/1 RPT=51 11:02:31.030 06/03/2002 436
                                       KeyProcessAdd: Enter
     SEV=8 IPSECDBG/1 RPT=52 11:02:31.030 06/03/2002 437
                          KeyProcessAdd: Adding outbound SA
     SEV=8 IPSECDBG/1 RPT=53 11:02:31.030 06/03/2002 438
    KeyProcessAdd: src 209.165.200.225 mask 0.0.0.0, dst
                               .209.165.202.129 mask 0.0.0
                                                          0
     SEV=8 IPSECDBG/1 RPT=54 11:02:31.030 06/03/2002 440
              KeyProcessAdd: FilterIpsecAddIkeSa success
     SEV=9 IPSECDBG/6 RPT=17 11:02:31.030 06/03/2002 441
   IPSEC key message parse - msgtype 3, len 332, vers 1,
                                 pid 00000000, seq 0, err 0
         type 2, mode 1, state 32, label 0, pad 0, spi ,
                             5fdb8057, encrKeyLen 24, hashKey
Len 20, ivlen 8, alg 2, hmacAlg 4, lifetype 0, lifetime1
                                    662488, lifetime2 0, ds
                                                Id -378167296
     SEV=9 IPSECDBG/1 RPT=55 11:02:31.030 06/03/2002 445
                                    !Processing KEY_UPDATE msg
     SEV=9 IPSECDBG/1 RPT=56 11:02:31.030 06/03/2002 446
                                  Update inbound SA addresses
     SEV=9 IPSECDBG/1 RPT=57 11:02:31.030 06/03/2002 447
                                key_msghdr2secassoc(): Enter
     SEV=7 IPSECDBG/1 RPT=58 11:02:31.030 06/03/2002 448
                                  No USER filter configured
     SEV=9 IPSECDBG/1 RPT=59 11:02:31.030 06/03/2002 449
                                    KeyProcessUpdate: Enter
     SEV=8 IPSECDBG/1 RPT=60 11:02:31.030 06/03/2002 450
                                  KeyProcessUpdate: success
        SEV=8 IKEDBG/7 RPT=3 11:02:31.030 06/03/2002 451
          IKE got a KEY_ADD msg for SA: SPI = 0xa088f2dc
      SEV=8 IKEDBG/0 RPT=155 11:02:31.030 06/03/2002 452
                  pitcher: rcv KEY_UPDATE, spi 0x5fdb8057
        SEV=4 IKE/120 RPT=13 11:02:31.040 06/03/2002 453
```

```
                                                    209.165.202.129
                                                [Group [209.165.202.129
                                    (PHASE 2 COMPLETED (msgid=e429a70e
 This line indicates that SA establishment !--- for ---!
      management between the VPN Client and Cisco IOS is
 complete. 454 06/03/2002 11:02:35.040 SEV=7 IPSECDBG/10
       RPT=4 IPSEC ipsec_output() can call key_acquire()
           because 4 seconds have elapsed since last IKE
  negotiation began (src 0x0a3042b9, dst 0x00a66e24) 456
 06/03/2002 11:02:35.040 SEV=7 IPSECDBG/14 RPT=4 Sending
KEY_ACQUIRE to IKE for src 10.48.66.185, dst 0.0.0.0 457
 06/03/2002 11:02:35.040 SEV=8 IKEDBG/0 RPT=156 pitcher:
          received a key acquire message! 458 06/03/2002
    11:02:35.040 SEV=4 IKE/41 RPT=136 IKE Initiator: New
   Phase 2, Intf 2, IKE Peer 209.165.202.129 local Proxy
    Address 10.48.66.0, remote Proxy Address 0.0.0.0, SA
        (ESP-3DES-MD5) 460 06/03/2002 11:02:35.040 SEV=9
IKEDBG/0 RPT=157 209.165.202.129 Group [209.165.202.129]
     Oakley begin quick mode 461 06/03/2002 11:02:35.040
       SEV=9 IPSECDBG/6 RPT=18 IPSEC key message parse -
msgtype 6, len 200, vers 1, pid 00000000, seq 14, err 0,
 type 2, mode 0, state 32, label 0, pad 0, spi 00000000,
 encrKeyLen 0, hashKey Len 0, ivlen 0, alg 0, hmacAlg 0,
lifetype 0, lifetime1 662488, lifetime2 0, dsI d 300 465
         06/03/2002 11:02:35.040 SEV=9 IPSECDBG/1 RPT=61
  Processing KEY_GETSPI msg! 466 06/03/2002 11:02:35.040
     SEV=7 IPSECDBG/13 RPT=4 Reserved SPI 1819592269 467
06/03/2002 11:02:35.040 SEV=8 IKEDBG/6 RPT=4 IKE got SPI
        from key engine: SPI = 0x6c74c64d 468 06/03/2002
     11:02:35.040 SEV=9 IKEDBG/0 RPT=158 209.165.202.129
   Group [209.165.202.129] oakley constucting quick mode
      469 06/03/2002 11:02:35.040 SEV=9 IKEDBG/0 RPT=159
    209.165.202.129 Group [209.165.202.129] constructing
   blank hash 470 06/03/2002 11:02:35.040 SEV=9 IKEDBG/0
         RPT=160 209.165.202.129 Group [209.165.202.129]
            constructing ISA_SA for ipsec 471 06/03/2002
11:02:35.040 SEV=9 IKEDBG/1 RPT=52 209.165.202.129 Group
  [209.165.202.129] constructing ipsec nonce payload 472
          06/03/2002 11:02:35.040 SEV=9 IKEDBG/1 RPT=53
    209.165.202.129 Group [209.165.202.129] constructing
     proxy ID 473 06/03/2002 11:02:35.040 SEV=7 IKEDBG/0
         RPT=161 209.165.202.129 Group [209.165.202.129]
  Transmitting Proxy Id: Local subnet:  10.48.66.0  mask
                         255.255.254.0 Protocol 0  Port 0
 Remote subnet: 0.0.0.0  Mask 0.0.0.0 Protocol 0  Port
                                                        0
 This line indicates the SA for the traffic between ---!
  !--- the networks behind the VPN Client and Cisco IOS.
      477 06/03/2002 11:02:35.040 SEV=9 IKEDBG/0 RPT=162
 209.165.202.129 Group [209.165.202.129] constructing qm
 hash 478 06/03/2002 11:02:35.040 SEV=8 IKEDBG/0 RPT=163
   209.165.202.129 SENDING Message (msgid=a809c6b4) with
payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5)
         + ID (5) + NONE (0) ... total leng th : 300 481
          06/03/2002 11:02:35.310 SEV=8 IKEDBG/0 RPT=164
  209.165.202.129 RECEIVED Message (msgid=a809c6b4) with
payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5)
+ ID (5) + NOTIFY (11) + NONE (0) ... total length : 200
      484 06/03/2002 11:02:35.310 SEV=9 IKEDBG/0 RPT=165
 209.165.202.129 Group [209.165.202.129] processing hash
      485 06/03/2002 11:02:35.310 SEV=9 IKEDBG/0 RPT=166
   209.165.202.129 Group [209.165.202.129] processing SA
      payload 486 06/03/2002 11:02:35.310 SEV=9 IKEDBG/1
          RPT=54 209.165.202.129 Group [209.165.202.129]
```

```
    processing nonce payload 487 06/03/2002 11:02:35.310
            SEV=9 IKEDBG/1 RPT=55 209.165.202.129 Group
          [209.165.202.129] Processing ID 488 06/03/2002
11:02:35.310 SEV=9 IKEDBG/1 RPT=56 209.165.202.129 Group
          [209.165.202.129] Processing ID 489 06/03/2002
     11:02:35.310 SEV=9 IKEDBG/0 RPT=167 209.165.202.129
   Group [209.165.202.129] Processing Notify payload 490
            06/03/2002 11:02:35.310 SEV=5 IKE/73 RPT=21
       209.165.202.129 Group [209.165.202.129] Responder
          forcing change of IPSec rekeying duration from
 2147483647 to 3600 seco nds 493 06/03/2002 11:02:35.310
           SEV=9 IKEDBG/0 RPT=168 209.165.202.129 Group
  [209.165.202.129] loading all IPSEC SAs 494 06/03/2002
11:02:35.310 SEV=9 IKEDBG/1 RPT=57 209.165.202.129 Group
        [209.165.202.129] Generating Quick Mode Key! 495
          06/03/2002 11:02:35.320 SEV=9 IKEDBG/1 RPT=58
209.165.202.129 Group [209.165.202.129] Generating Quick
    Mode Key! 496 06/03/2002 11:02:35.320 SEV=7 IKEDBG/0
 RPT=169 209.165.202.129 Group [209.165.202.129] Loading
subnet: Dst: 0.0.0.0 mask: 0.0.0.0 Src: 10.48.66.0 mask:
  255.255.254.0 499 06/03/2002 11:02:35.320 SEV=4 IKE/49
 RPT=14 209.165.202.129 Group [209.165.202.129] Security
         negotiation complete for peer (209.165.202.129)
     Initiator, Inbound SPI = 0x6c74c64d, Outbound SPI =
   0x8e34d356 502 06/03/2002 11:02:35.320 SEV=9 IKEDBG/0
  RPT=170 209.165.202.129 Group [209.165.202.129] oakley
           constructing final quick mode 503 06/03/2002
     11:02:35.320 SEV=8 IKEDBG/0 RPT=171 209.165.202.129
  SENDING Message (msgid=a809c6b4) with payloads : HDR +
HASH (8) + NONE (0) ... total length : 76 505 06/03/2002
  11:02:35.320 SEV=9 IPSECDBG/6 RPT=19 IPSEC key message
parse - msgtype 1, len 612, vers 1, pid 00000000, seq 0,
   err 0 , type 2, mode 1, state 64, label 0, pad 0, spi
8e34d356, encrKeyLen 24, hashKey Len 20, ivlen 8, alg 2,
hmacAlg 4, lifetype 0, lifetime1 662488, lifetime2 0, ds
         Id -378167296 509 06/03/2002 11:02:35.330 SEV=9
IPSECDBG/1 RPT=62 Processing KEY_ADD msg! 510 06/03/2002
                   11:02:35.330 SEV=9 IPSECDBG/1 RPT=63
key_msghdr2secassoc(): Enter 511 06/03/2002 11:02:35.330
   SEV=7 IPSECDBG/1 RPT=64 No USER filter configured 512
         06/03/2002 11:02:35.330 SEV=9 IPSECDBG/1 RPT=65
  KeyProcessAdd: Enter 513 06/03/2002 11:02:35.330 SEV=8
 IPSECDBG/1 RPT=66 KeyProcessAdd: Adding outbound SA 514
         06/03/2002 11:02:35.330 SEV=8 IPSECDBG/1 RPT=67
       KeyProcessAdd: src 10.48.66.0 mask 0.0.1.255, dst
0.0.0.0 mask 255.255.255.255 515 06/03/2002 11:02:35.330
                  SEV=8 IPSECDBG/1 RPT=68 KeyProcessAdd:
 FilterIpsecAddIkeSa success 516 06/03/2002 11:02:35.330
       SEV=9 IPSECDBG/6 RPT=20 IPSEC key message parse -
msgtype 3, len 332, vers 1, pid 00000000, seq 0, err 0 ,
 type 2, mode 1, state 32, label 0, pad 0, spi 6c74c64d,
  encrKeyLen 24, hashKey Len 20, ivlen 8, alg 2, hmacAlg
   4, lifetype 0, lifetime1 662488, lifetime2 0, ds Id -
  378167296 520 06/03/2002 11:02:35.330 SEV=9 IPSECDBG/1
        RPT=69 Processing KEY_UPDATE msg! 521 06/03/2002
  11:02:35.330 SEV=9 IPSECDBG/1 RPT=70 Update inbound SA
  addresses 522 06/03/2002 11:02:35.330 SEV=9 IPSECDBG/1
      RPT=71 key_msghdr2secassoc(): Enter 523 06/03/2002
     11:02:35.330 SEV=7 IPSECDBG/1 RPT=72 No USER filter
 configured 524 06/03/2002 11:02:35.330 SEV=9 IPSECDBG/1
           RPT=73 KeyProcessUpdate: Enter 525 06/03/2002
  11:02:35.330 SEV=8 IPSECDBG/1 RPT=74 KeyProcessUpdate:
success 526 06/03/2002 11:02:35.330 SEV=8 IKEDBG/7 RPT=4
      IKE got a KEY_ADD msg for SA: SPI = 0x8e34d356 527
```

```
06/03/2002 11:02:35.330 SEV=8 IKEDBG/0 RPT=172 pitcher:
          rcv KEY_UPDATE, spi 0x6c74c64d 528 06/03/2002
11:02:35.330 SEV=4 IKE/120 RPT=14 209.165.202.129 Group
[209.165.202.129] PHASE 2 COMPLETED (msgid=a809c6b4) !--
   - This line indicates that SA establishment !--- for
       networks between the VPN Client and Cisco IOS is
                                                .complete
```

معلومات ذات صلة

- دعم مركز Cisco VPN 3000
- دعم عميل أجهزة Cisco VPN 3002
- دعم مفاوضة IPSec/بروتوكولات IKE
- 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).