EzVPN مع NEM على موجه IOS مع مثال لتكوين مركز VPN 3000

المحتويات

المقدمة

يشرح هذا المستند الإجراء الذي تستخدمه لتكوين موجه Cisco IOS® على أنه EzVPN في وضع امتداد الشبكة (NEM) للاتصال بمركز Cisco VPN 3000. ميزة EzVPN Phase II جديدة هي دعم تكوين ترجمة عنوان الشبكة (NAT) الأساسي. يتم اشتقاق المرحلة الثانية من EzVPN من بروتوكول الوحدة (برنامج عميل شبكة VPN). الجهاز البعيد هو دائما بادئ نفق IPsec. ومع ذلك، فإن اقتراحات Internet Key Exchange (IKE) و IPsec غير قابلة للتكوين على عميل EzVPN. يتفاوض عميل الشبكة الخاصة الظاهرية (VPN) على الاقتراحات مع الخادم.

لتكوين IPsec بين PIX/ASA 7.x وموجه Cisco 871 باستخدام شبكة VPN سهلة، ارجع إلى PIX/ASA 7.x Easy VPN مع ASA 5500 كخادم و Cisco 871 كمثال التكوين عن بعد السهل ل VPN.

من أجل تكوين IPsec بين عميل الأجهزة البعيدة Easy VPN من Cisco IOS® وخادم PIX Easy VPN، ارجع إلى عميل الأجهزة البعيدة VPN سهل IOS إلى مثال تكوين خادم PIX Easy VPN.

أحلت in order to شكلت cisco 7200 مسحاج تخديد ك EzVPN و ال cisco 871 مسحاج تخديد ك ال VPN بعيد سهل، 7200 ييسر VPN نادل إلى 871 ييسر VPN تشكيل بعيد مثال.

المتطلبات الأساسية

المتطلبات

قبل أن تحاول إجراء إختبار التكوين هذا، يدعم موجه Cisco IOS ميزة EzVPN Phase II ويتميز باتصال IP مع الاتصالات من نهاية إلى نهاية لإنشاء نفق IPsec.

المكونات المستخدمة

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

- برنامج IOS الإصدار 12.2(8)II (EzVPN Phase II) YJ من Cisco
- مركز VPN 3000، الإصدار x.3.6
- موجّه Cisco 1700

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

ملاحظة: تم إختبار هذا التكوين مؤخرا باستخدام موجه Cisco 3640 مع البرنامج Cisco IOS Software، الإصدار 12.4(8) وإصدار مركز VPN 3000، الإصدار x.4.7.

الاصطلاحات

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

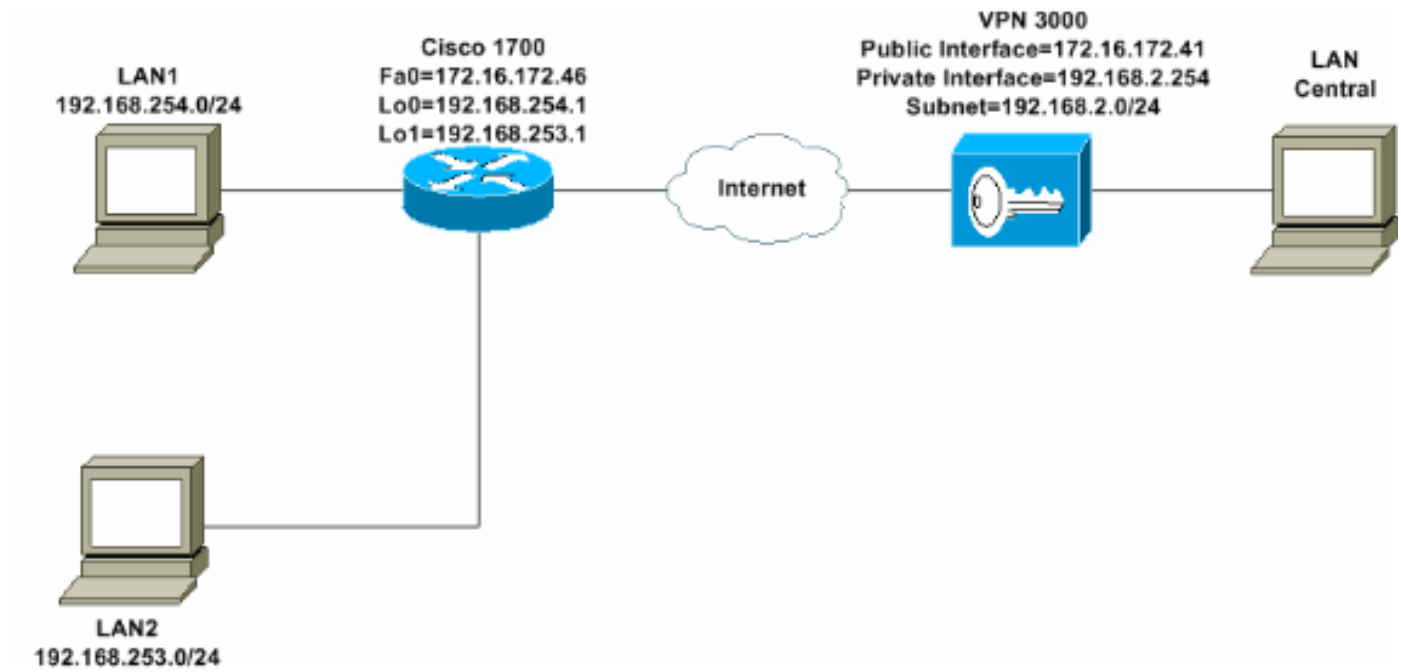
تكوين مركز VPN 3000

المهمة

في هذا القسم، تقدم لك معلومات تكوين مركز VPN 3000.

الرسم التخطيطي للشبكة

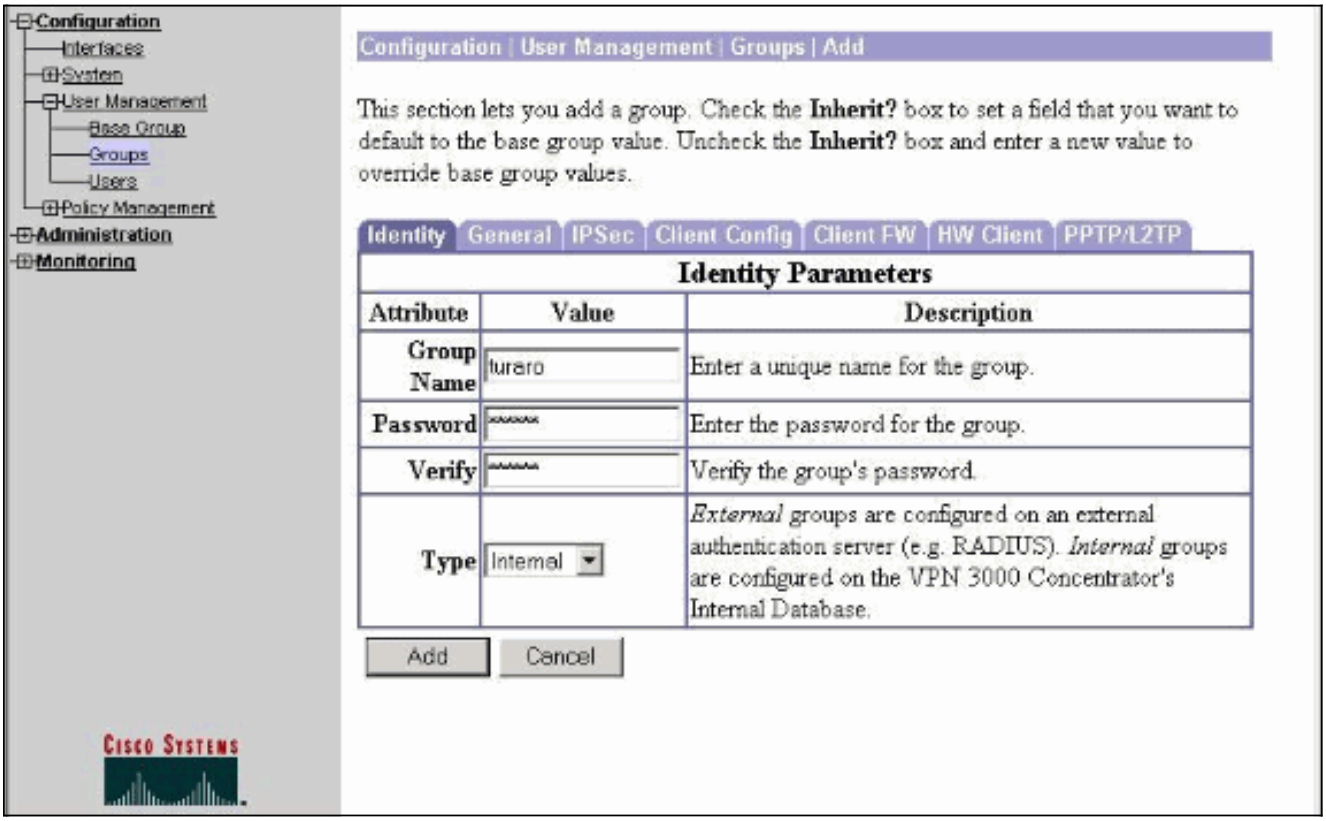
يستخدم هذا المستند إعداد الشبكة الموضح في هذا الرسم التخطيطي. يتم إستخدام واجهات الاسترجاع كشبكات فرعية داخلية، وبعد FastEthernet 0 هو الإعداد الافتراضي للإنترنت.



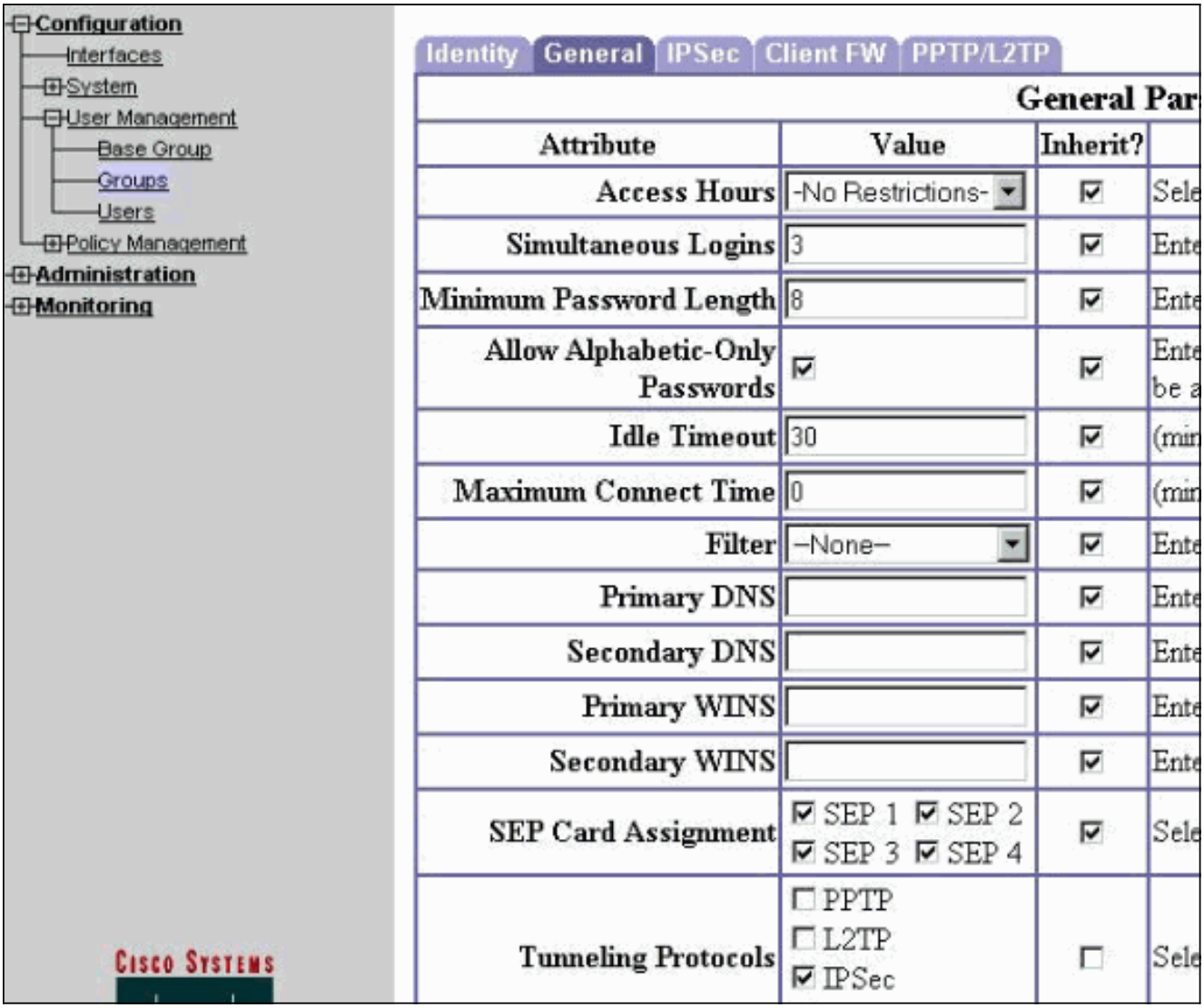
إرشادات خطوة بخطوة

أكمل الخطوات التالية:

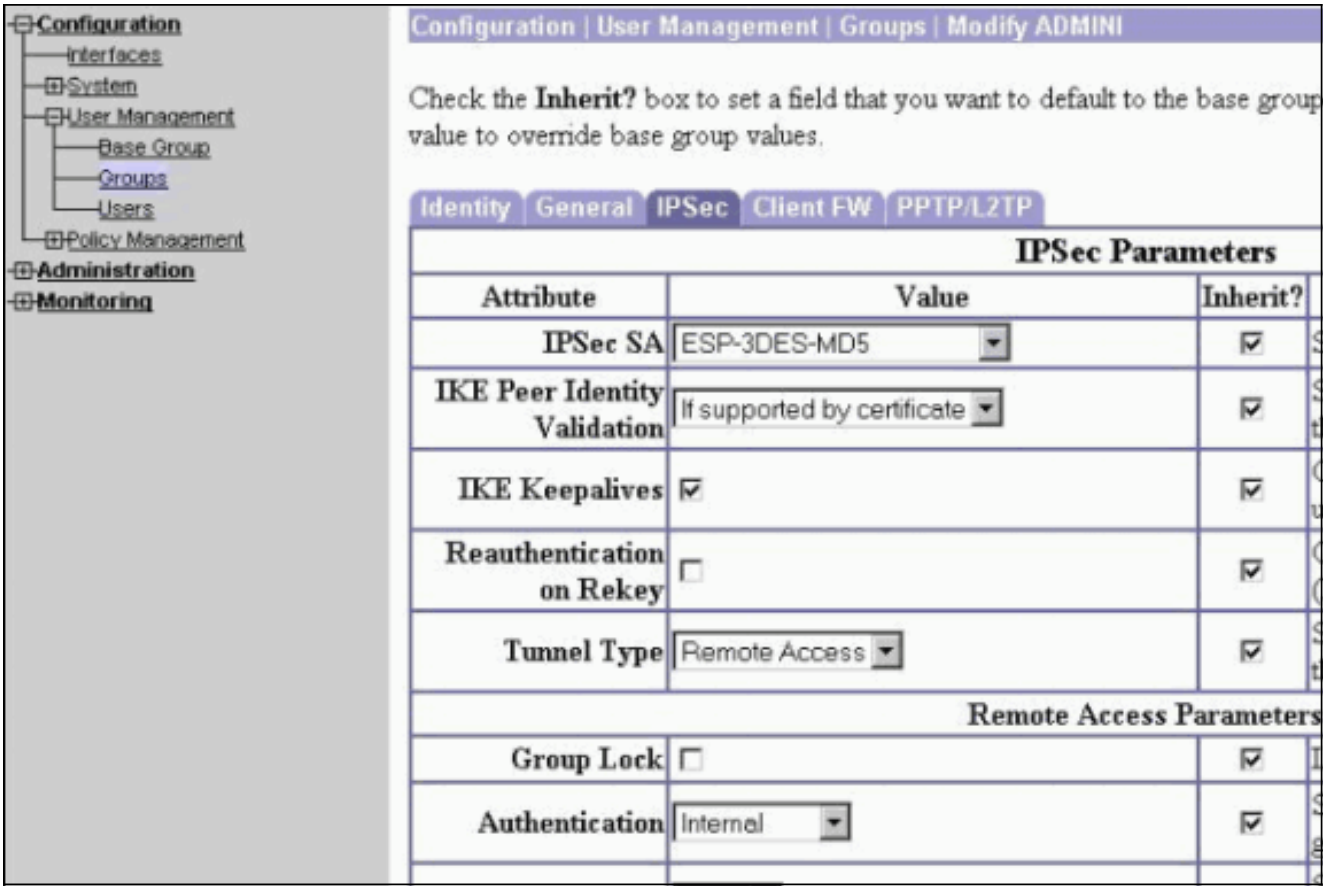
1. أخترت **تشكيل>مستعمل إدارة>مجموعة>يضيف>ويعين مجموعة إسم وكلمة** in order to **شكلت مجموعة IPsec للمستخدمين**.يستخدم هذا المثال اسم المجموعة Turaro مع كلمة المرور/التحقق من Olulo.



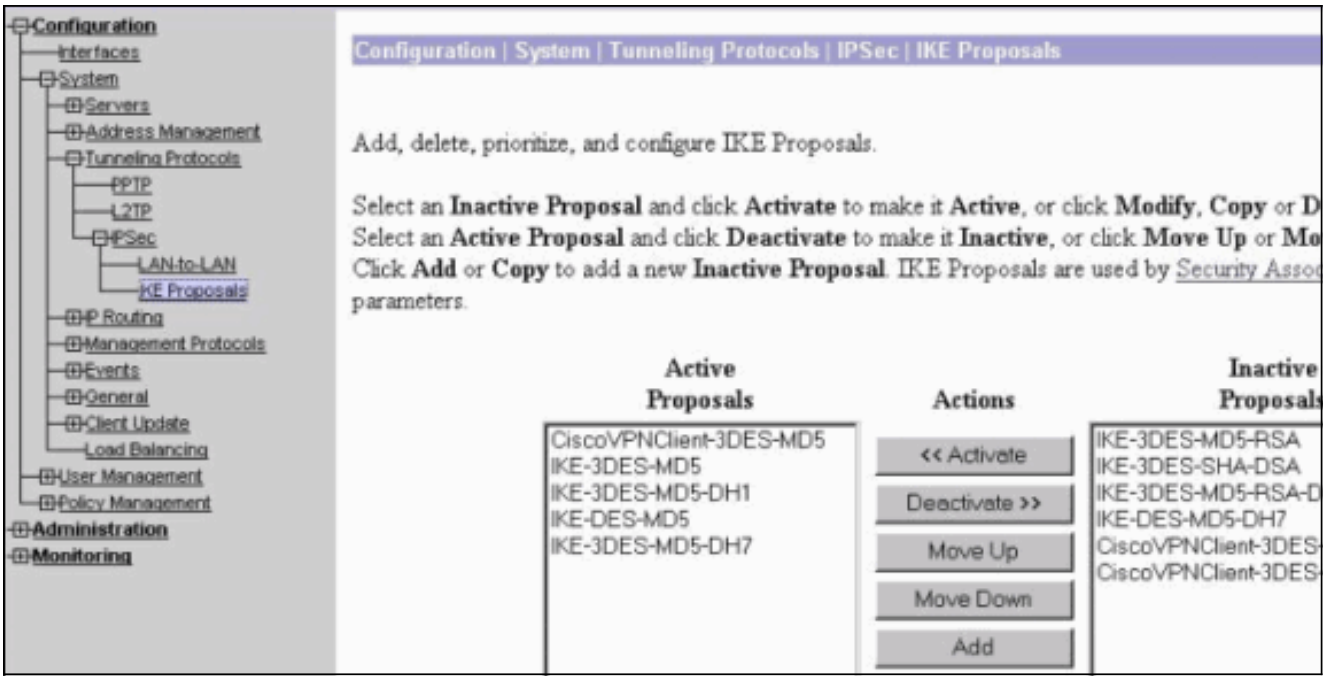
2. أخترت تشكيل>مستعمل إدارة>مجموعة>**turaro>عام** أن يمكن IPSec ويعجز نقطة أن يدل tunneling بروتوكول (PPTP) وطبقة 2 نفق بروتوكول (L2TP).قم بعمل التحديدات وانقر فوق **تطبيق**.



3. قم بتعيين المصادقة على **داخلي** للمصادقة الموسعة (Xauth) وتأكد من أن نوع النفق هو **الوصول عن بعد** و IPSec SA هو **ESP-3DES-MD5**.

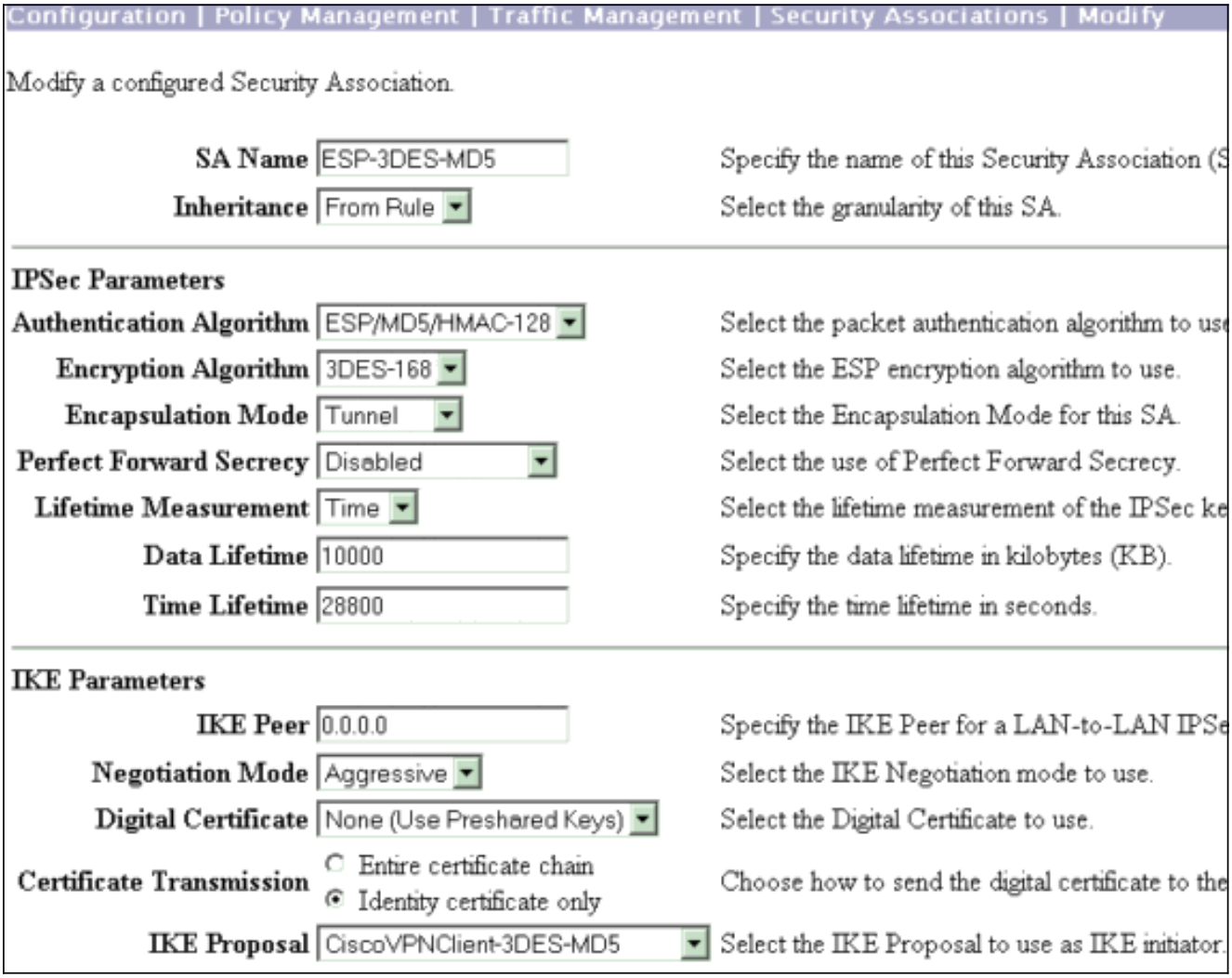


4. أخترت **تشكيل>نظام>tunneling بروتوكول>IKE > IPSec مقترح** in order to تأكدت أن ال cisco VPN زبون (CiscoVPNClient-3DES-MD5) في اقتراح نشط ل IKE (مرحلة 1).**ملاحظة:** من مركز الشبكة الخاصة الظاهرية (VPN) الإصدار x.4.1، يختلف الإجراء لضمان أن يكون عميل الشبكة الخاصة الظاهرية (VPN) من Cisco مدرجا في قائمة المقترحات النشطة للطراز IKE (المرحلة 1). أختر **التكوين > الاتصال النفقي والأمان > IPSec > مقترحات IKE.**



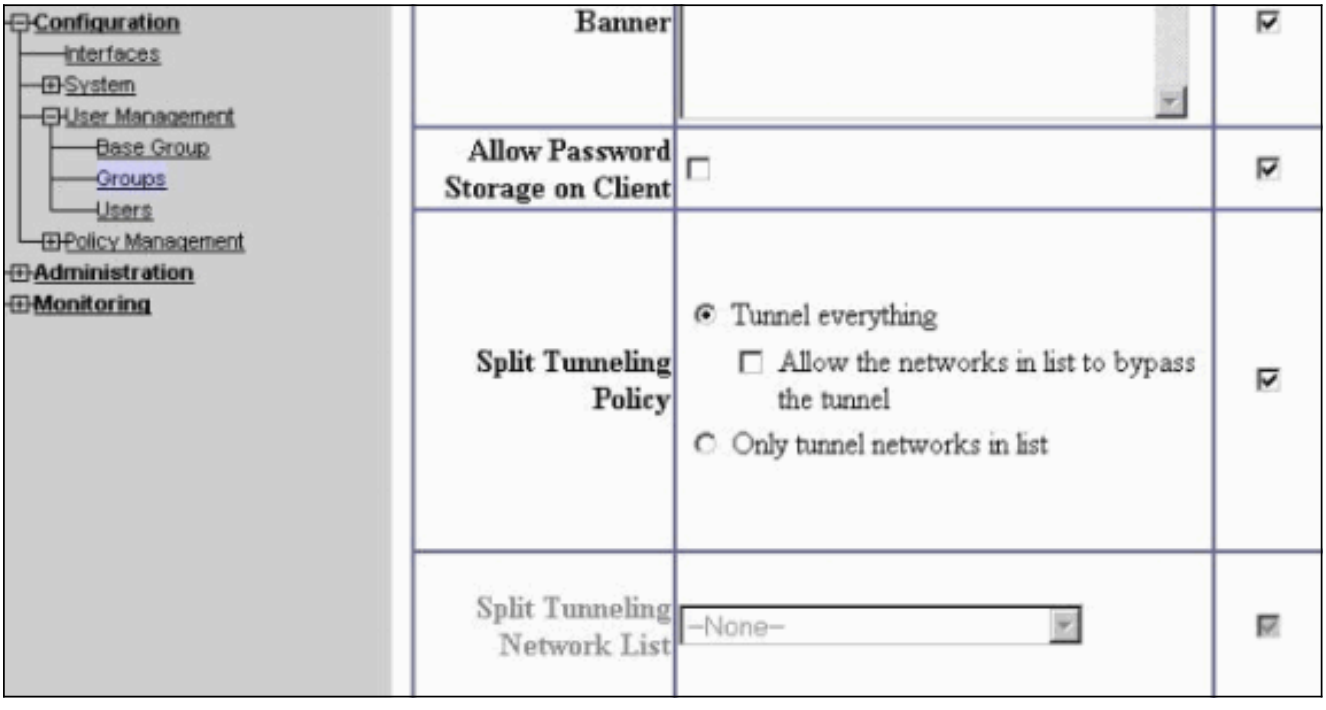
5. تحقق من اقتران أمان IPsec (SA).في الخطوة 3 يكون IPsec SA الخاص بك هو ESP-3DES-MD5. يمكنك إنشاء واحد جديد إذا كنت ترغب في ذلك ولكن تأكد من إستخدام IPsec SA الصحيح على مجموعتك. يجب تعطيل سرية إعادة التوجيه (PFS) المثالية ل IPsec SA التي تستخدمها. حدد عميل Cisco VPN كاقتراح IKE باختيار **التكوين>إدارة السياسة>إدارة حركة مرور البيانات>SAs**. اكتب اسم SA في مربع النص ثم قم بعمل التحديدات المناسبة كما هو موضح

هنا:

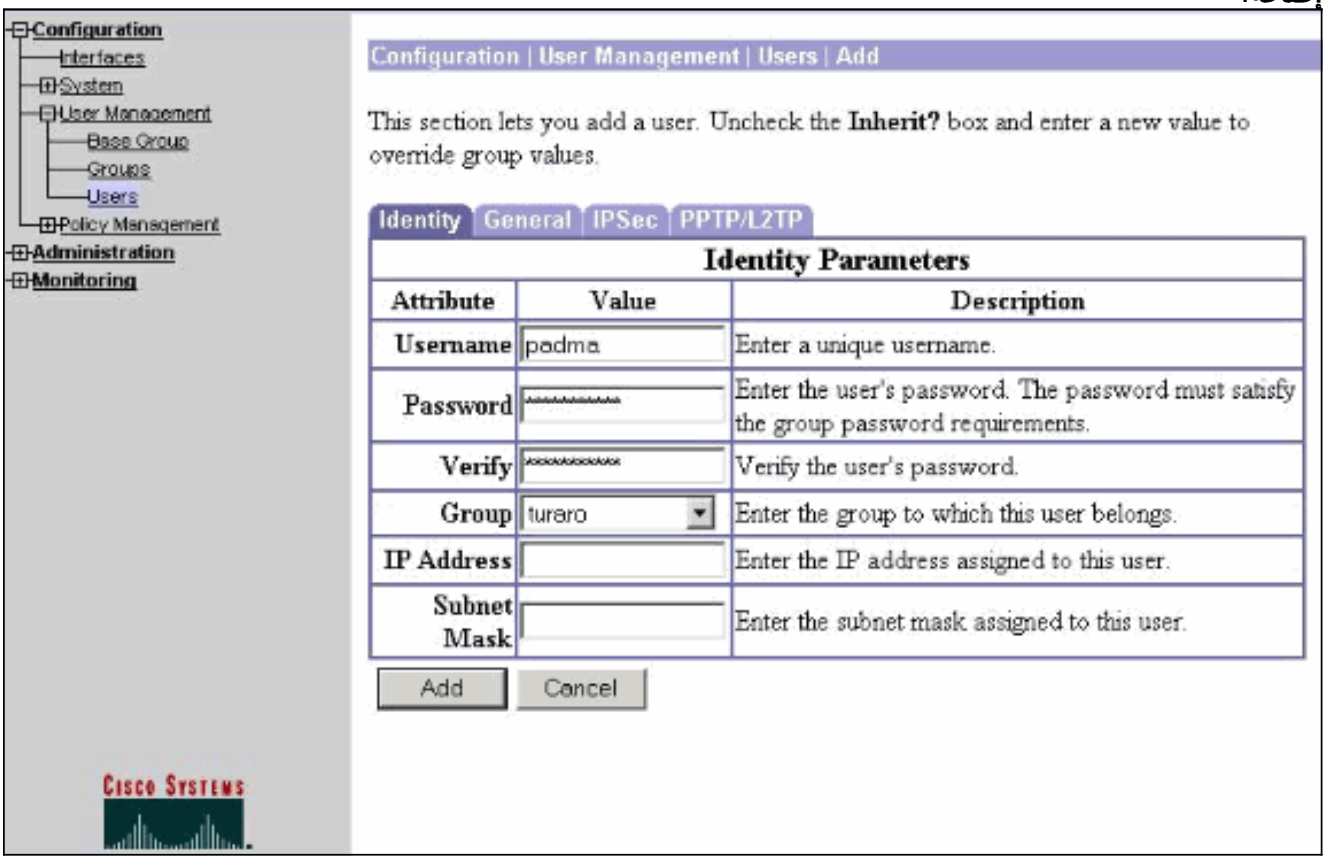


ملاحظة: تعد هذه الخطوة والخطوة التالية اختياريين إذا كنت تفضل إختيار منطقة وصول (SA) معرفة مسبقا. إذا كان لدى العميل عنوان IP معين بشكل ديناميكي، فاستخدم 0.0.0.0 في مربع نص نظير IKE. تأكد من تعيين اقتراح IKE على **CiscoVPNClient-3DES-MD5** كما يوضح هذا المثال.

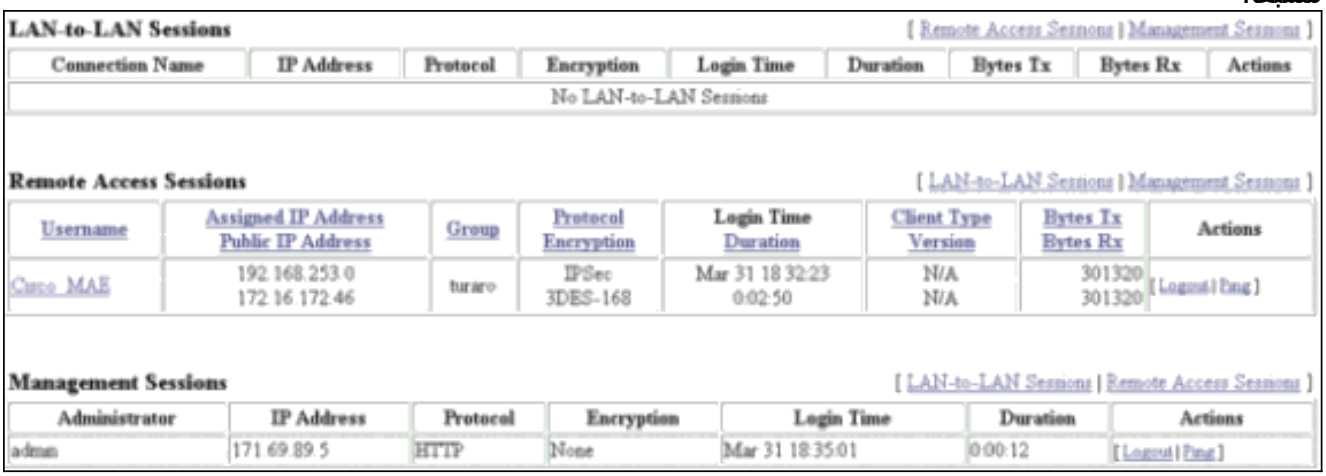
6. أنت ينبغي **لا** ينقر *يسمح الشبكات في القائمة أن يتجاوز النفق*. السبب أن تقسيم الاتصال النفقي مدعوم، غير أن ميزة التجاوز غير مدعومة مع ميزة عميل EzVPN.



7. أخترت **تشكيل>مستعمل إدارة>مستعمل** in order to أضفت مستعمل. قم بتعريف اسم مستخدم وكلمة مرور، وقم بتعيينها على مجموعة، وانقر فوق
إضافة.



8. أختر **إدارة > جلسات عمل المسؤول** وتحقق من اتصال المستخدم. في NEM، لا يعين مركز الشبكة الخاصة الظاهرية (VPN) عنوان IP من المجموعة.**ملاحظة:** تكون هذه الخطوة إختيارية إذا كنت تفضل إختيار وسيلة مساعدة (SA) معرفة
مسبقا.



9. انقر إما على أيقونة **حفظ مطلوب** أو **حفظ** لحفظ التكوين.

تكوين الموجّه

show version output

```
show version
Cisco Internetwork Operating System Software
```

,IOS (tm) C1700 Software (C1700-BK9NO3R2SY7-M), Version 12.2(8)YJ
(EARLY DEPLOYMENT RELEASE SOFTWARE (fc1

ADSL) uptime is 4 days, 5 hours, 33 minutes)1721-1
System returned to ROM by reload
"System image file is "flash:**c1700-bk9no3r2sy7-mz.122-8.YJ.bin**
cisco 1721 (MPC860P) processor (revision 0x100) with 88474K/9830K bytes
(16384K bytes of processor board System flash (Read/Write

1721-1

ADSL)#**show run**)1721-1
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
(hostname 1721-1(ADSL
!
Specify the configuration name !--- to be assigned ---!
to the interface. **crypto ipsec client ezvpn SJVPN**
Tunnel control; automatic is the default. **connect** *---!*
auto
The group name and password should be the same as ---!
given in the VPN Concentrator. **group turaro key tululo**
The mode that is chosen as the network extension. ---!
mode network-extension
The tunnel peer end (VPN Concentrator public ---!
interface IP address). **peer 172.16.172.41**
!
interface Loopback0
ip address 192.168.254.1 255.255.255.0
Configure the Loopback interface !--- as the inside ---!
interface. **ip nat inside**
Specifies the Cisco EzVPN Remote configuration name ---!
.*!--- to be assigned to the* **inside** interface

crypto ipsec client ezvpn SJVPN inside
!
interface Loopback1
ip address 192.168.253.1 255.255.255.0
ip nat inside
crypto ipsec client ezvpn SJVPN inside
!
interface FastEthernet0
ip address 172.16.172.46 255.255.255.240
Configure the FastEthernet interface !--- as the ---!
outside interface. **ip nat outside**
Specifies the Cisco EzVPN Remote configuration name ---!
!--- to be assigned to the first outside interface,
because !--- **outside** is not specified for the interface.
.!--- The default is outside

crypto ipsec client ezvpn SJVPN
!
Specify the **overload** option with the **ip nat** command *---!*
!--- in global configuration mode in order to enable !--
- Network Address Translation (NAT) of the inside source
address !--- so that multiple PCs can use the single IP
.address

ip nat inside source route-map EZVPN interface
FastEthernet0 overload
ip classless

```
ip route 0.0.0.0 0.0.0.0 172.16.172.41
!
access-list 177 deny   ip 192.168.254.0 0.0.0.255
                          192.168.2.0 0.0.0.255
access-list 177 deny   ip 192.168.253.0 0.0.0.255
                          192.168.2.0 0.0.0.255
access-list 177 permit ip 192.168.253.0 0.0.0.255 any
access-list 177 permit ip 192.168.254.0 0.0.0.255 any
!
route-map EZVPN permit 10
    match ip address 177
!
!
line con 0
line aux 0
line vty 0 4
 password cisco
 login
!
no scheduler allocate
end
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

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

بمجرد تكوين كلا الجهازين، يحاول الموجه Cisco 3640 إعداد نفق VPN من خلال الاتصال بموجه VPN تلقائيا باستخدام عنوان IP للنظير. بعد تبادل معلمات ISAKMP الأولية، يعرض الموجه هذه الرسالة:

```
Pending XAuth Request, Please enter the
following command: crypto ipsec client ezvpn xauth
```

يجب إدخال الأمر **crypto ipSec client ezVPN xauth** الذي يطالبك باسم مستخدم وكلمة مرور. يجب أن يتطابق هذا مع اسم المستخدم وكلمة المرور اللذين تم تكوينهما على مركز VPN (الخطوة 7). بمجرد الموافقة على اسم المستخدم وكلمة المرور من قبل كلا النظيرين، يتم الاتفاق على باقي المعلمات ويتم ظهور نفق IPsec VPN.

```
:EZVPN(SJVPN): Pending XAuth Request, Please enter the following command

EZVPN: crypto ipsec client ezvpn xauth

.Enter the crypto ipsec client ezvpn xauth command ---!


crypto ipsec client ezvpn xauth

Enter Username and Password.: padma
Password: : password
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

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

- **debug crypto ipSec client ezVPN**—يعرض المعلومات التي تظهر تكوين ميزة عميل EzVPN وتنفيذها.
- **debug crypto ipSec**—يعرض معلومات تصحيح الأخطاء حول إتصالات IPsec.
- **debug crypto isakmp**— يعرض معلومات تصحيح الأخطاء حول إتصالات IPsec، ويبدي المجموعة الأولى من السمات التي يتم رفضها بسبب عدم التوافق على كلا النهايتين.
- **show debug**—يعرض حالة كل خيار تصحيح.

مخرجات من أوامر التصحيح

بمجرد إدخال الأمر **crypto ipSec client ezVPN SJVPN**، يحاول عميل EzVPN الاتصال بالخادم. إذا قمت بتغيير الأمر **connect manual** ضمن تكوين المجموعة، فأدخل الأمر **crypto ipSec client ezVPN connect sjvpn** لبدء تبادل الاقتراحات إلى الخادم.

```
                                4d05h: ISAKMP (0:3): beginning Aggressive Mode exchange
                   4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) AG_INIT_EXCH
                4d05h: ISAKMP (0:3): received packet from 172.16.172.41 (I) AG_INIT_EXCH
                             4d05h: ISAKMP (0:3): processing SA payload. message ID = 0
                             4d05h: ISAKMP (0:3): processing ID payload. message ID = 0
                                      4d05h: ISAKMP (0:3): processing vendor id payload
                                               4d05h: ISAKMP (0:3): vendor ID is Unity
                                      4d05h: ISAKMP (0:3): processing vendor id payload
                           4d05h: ISAKMP (0:3): vendor ID seems Unity/DPD but bad major
                                               4d05h: ISAKMP (0:3): vendor ID is XAUTH
                                      4d05h: ISAKMP (0:3): processing vendor id payload
                                                 4d05h: ISAKMP (0:3): vendor ID is DPD
                                    4d05h: ISAKMP (0:3) local preshared key found
                                 4d05h: ISAKMP (0:3) Authentication by xauth preshared
              4d05h: ISAKMP (0:3): Checking ISAKMP transform 6 against priority 65527 policy
                                               4d05h: ISAKMP:      encryption 3DES-CBC
                                                         4d05h: ISAKMP:      hash MD5
                                                      4d05h: ISAKMP:      default group 2
                                                4d05h: ISAKMP:      auth XAUTHInitPreShared
                                                   4d05h: ISAKMP:      life type in seconds
                                 4d05h: ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
                       !4d05h: ISAKMP (0:3): Encryption algorithm offered does not match policy
                                4d05h: ISAKMP (0:3): atts are not acceptable. Next payload is 0
              4d05h: ISAKMP (0:3): Checking ISAKMP transform 6 against priority 65528 policy
                                               4d05h: ISAKMP:      encryption 3DES-CBC
                                                         4d05h: ISAKMP:      hash MD5
                                                      4d05h: ISAKMP:      default group 2
                                                4d05h: ISAKMP:      auth XAUTHInitPreShared
                                                   4d05h: ISAKMP:      life type in seconds
                                 4d05h: ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
                       !4d05h: ISAKMP (0:3): Encryption algorithm offered does not match policy
                                4d05h: ISAKMP (0:3): atts are not acceptable. Next payload is 0
              4d05h: ISAKMP (0:3): Checking ISAKMP transform 6 against priority 65529 policy
                                               4d05h: ISAKMP:      encryption 3DES-CBC
                                                         4d05h: ISAKMP:      hash MD5
```

4d05h: ISAKMP: default group 2
4d05h: ISAKMP: auth XAUTHInitPreShared
4d05h: ISAKMP: life type in seconds
4d05h: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
!4d05h: ISAKMP (0:3): Encryption algorithm offered does not match policy
4d05h: ISAKMP (0:3): atts are not acceptable. Next payload is 0
4d05h: ISAKMP (0:3): Checking ISAKMP transform 6 against priority 65530 policy
4d05h: ISAKMP: encryption 3DES-CBC
4d05h: ISAKMP: hash MD5
4d05h: ISAKMP: default group 2
4d05h: ISAKMP: auth XAUTHInitPreShared
4d05h: ISAKMP: life type in seconds
4d05h: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
!4d05h: ISAKMP (0:3): Encryption algorithm offered does not match policy
4d05h: ISAKMP (0:3): atts are not acceptable. Next payload is 0
4d05h: ISAKMP (0:3): Checking ISAKMP transform 6 against priority 65531 policy
4d05h: ISAKMP: encryption 3DES-CBC
4d05h: ISAKMP: hash MD5
4d05h: ISAKMP: default group 2
4d05h: ISAKMP: auth XAUTHInitPreShared
4d05h: ISAKMP: life type in seconds
4d05h: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
!4d05h: ISAKMP (0:3): Hash algorithm offered does not match policy
4d05h: ISAKMP (0:3): atts are not acceptable. Next payload is 0
4d05h: ISAKMP (0:3): Checking ISAKMP transform 6 against priority 65532 policy
4d05h: ISAKMP: encryption 3DES-CBC
4d05h: ISAKMP: hash MD5
4d05h: ISAKMP: default group 2
4d05h: ISAKMP: auth XAUTHInitPreShared
4d05h: ISAKMP: life type in seconds
4d05h: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
4d05h: ISAKMP (0:3): **atts are acceptable.** Next payload is 0
4d05h: ISAKMP (0:3): processing KE payload. message ID = 0
4d05h: ISAKMP (0:3): processing NONCE payload. message ID = 0
4d05h: ISAKMP (0:3): SKEYID state generated
4d05h: ISAKMP (0:3): processing HASH payload. message ID = 0
4d05h: ISAKMP (0:3): **SA has been authenticated with 172.16.172.41**
4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) AG_INIT_EXCH
4d05h: ISAKMP (0:3): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
Old State = IKE_I_AM1 New State = IKE_P1_COMPLETE

...4d05h: IPSEC(key_engine): got a queue event

4d05h: IPSec: Key engine got KEYENG_IKMP_MORE_SAS message

4d05h: ISAKMP (0:3): Need XAUTH

4d05h: ISAKMP (0:3): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE

Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE

Phase 1 (ISAKMP) is complete. 4d05h: ISAKMP: received ke message (6/1) 4d05h: ISAKMP: *---!* received KEYENG_IKMP_MORE_SAS message 4d05h: ISAKMP: set new node -857862190 to CONF_XAUTH *!--- Initiate extended authentication.* 4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) CONF_XAUTH 4d05h: ISAKMP (0:3): purging node -857862190 4d05h: ISAKMP (0:3): Sending initial contact. 4d05h: ISAKMP (0:3): received packet from 172.16.172.41 (I) CONF_XAUTH 4d05h: ISAKMP: set new node -1898481791 to CONF_XAUTH 4d05h: ISAKMP (0:3): processing transaction payload from 172.16.172.41. message ID = -1898481791 4d05h: ISAKMP: Config payload REQUEST 4d05h: ISAKMP (0:3): checking request: 4d05h: ISAKMP: XAUTH_TYPE_V2 4d05h: ISAKMP: XAUTH_USER_NAME_V2 4d05h: ISAKMP: XAUTH_USER_PASSWORD_V2 4d05h: ISAKMP: XAUTH_MESSAGE_V2 4d05h: ISAKMP (0:3): Xauth process request 4d05h: ISAKMP (0:3): Input = IKE_MESG_FROM_PEER, IKE_CFG_REQUEST Old State = IKE_P1_COMPLETE New State = IKE_XAUTH_REPLY_AWAIT 4d05h: EZVPN(SJVPN): Current State: READY 4d05h: EZVPN(SJVPN): Event: XAUTH_REQUEST 4d05h: EZVPN(SJVPN): ezvpn_xauth_request 4d05h: EZVPN(SJVPN): ezvpn_parse_xauth_msg 4d05h: EZVPN: Attributes sent in xauth request message:

4d05h: XAUTH_TYPE_V2(SJVPN): 0 4d05h: XAUTH_USER_NAME_V2(SJVPN): 4d05h: XAUTH_USER_PASSWORD_V2(SJVPN): 4d05h: XAUTH_MESSAGE_V2(SJVPN) <Enter Username and Password.> 4d05h: EZVPN(SJVPN): New State: XAUTH_REQ 4d05h: ISAKMP (0:3): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE Old State = IKE_XAUTH_REPLY_AWAIT New State = IKE_XAUTH_REPLY_AWAIT 4d05h: EZVPN(SJVPN): Pending XAuth Request, Please enter the following command: 4d05h: EZVPN: **crypto ipsec client ezvpn xauth**

.*Enter the* **crypto ipsec client ezvpn xauth** command *---!*

crypto ipsec client ezvpn xauth

Enter Username and Password.: **padma**

Password: : **password**

The router requests your username and password that is !--- configured on the server. ---!
4d05h: EZVPN(SJVPN): Current State: XAUTH_REQ 4d05h: EZVPN(SJVPN): Event: XAUTH_PROMPTING 4d05h: EZVPN(SJVPN): New State: XAUTH_PROMPT 1721-1(ADSL)# 4d05h: EZVPN(SJVPN): Current State: XAUTH_PROMPT 4d05h: EZVPN(SJVPN): Event: XAUTH_REQ_INFO_READY 4d05h: EZVPN(SJVPN): ezvpn_xauth_reply 4d05h: XAUTH_TYPE_V2(SJVPN): 0 4d05h: XAUTH_USER_NAME_V2(SJVPN): Cisco_MAE 4d05h: XAUTH_USER_PASSWORD_V2(SJVPN): <omitted> 4d05h: EZVPN(SJVPN): New State: XAUTH_REPLIED 4d05h: xauth-type: 0 4d05h: username: Cisco_MAE 4d05h: password: <omitted> 4d05h: message <Enter Username and Password.> 4d05h: ISAKMP (0:3): responding to peer config from 172.16.172.41. ID = -1898481791 4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) CONF_XAUTH 4d05h: ISAKMP (0:3): deleting node -1898481791 error FALSE reason "done with xauth request/reply exchange" 4d05h: ISAKMP (0:3): Input = IKE_MESG_INTERNAL, IKE_XAUTH_REPLY_ATTR Old State = IKE_XAUTH_REPLY_AWAIT New State = IKE_XAUTH_REPLY_SENT 4d05h: ISAKMP (0:3): received packet from 172.16.172.41 (I) CONF_XAUTH 4d05h: ISAKMP: set new node -1602220489 to CONF_XAUTH 4d05h: ISAKMP (0:3): processing transaction payload from 172.16.172.41. message ID = -1602220489 4d05h: ISAKMP: Config payload SET 4d05h: ISAKMP (0:3): Xauth process set, status = 1 4d05h: ISAKMP (0:3): checking SET: 4d05h: ISAKMP: XAUTH_STATUS_V2 XAUTH-OK 4d05h: ISAKMP (0:3): attributes sent in message: 4d05h: Status: 1 4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) CONF_XAUTH 4d05h: ISAKMP (0:3): deleting node -1602220489 error FALSE reason "" 4d05h: ISAKMP (0:3): Input = IKE_MESG_FROM_PEER, IKE_CFG_SET Old State = IKE_XAUTH_REPLY_SENT New State = IKE_P1_COMPLETE 4d05h: EZVPN(SJVPN): Current State: XAUTH_REPLIED 4d05h: EZVPN(SJVPN): Event: XAUTH_STATUS 4d05h: EZVPN(SJVPN): New State: READY 4d05h: ISAKMP (0:3): Need config/address 4d05h: ISAKMP (0:3): Need config/address 4d05h: ISAKMP: set new node 486952690 to CONF_ADDR 4d05h: ISAKMP (0:3): initiating peer config to 172.16.172.41. ID = 486952690 4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) CONF_ADDR 4d05h: ISAKMP (0:3): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE Old State = IKE_P1_COMPLETE New State = IKE_CONFIG_MODE_REQ_SENT 4d05h: ISAKMP (0:3): received packet from 172.16.172.41 (I) CONF_ADDR 4d05h: ISAKMP (0:3): processing transaction payload from 172.16.172.41. message ID = 486952690 4d05h: ISAKMP: Config payload REPLY 4d05h: ISAKMP(0:3) process config reply 4d05h: ISAKMP (0:3): deleting node 486952690 error FALSE reason "done with transaction" 4d05h: ISAKMP (0:3): Input = IKE_MESG_FROM_PEER, IKE_CFG_REPLY Old State = IKE_CONFIG_MODE_REQ_SENT New State = IKE_P1_COMPLETE 4d05h: EZVPN(SJVPN): Current State: READY 4d05h: EZVPN(SJVPN): Event: MODE_CONFIG_REPLY 4d05h: EZVPN(SJVPN): ezvpn_mode_config 4d05h: EZVPN(SJVPN): ezvpn_parse_mode_config_msg 4d05h: EZVPN: Attributes sent in message 4d05h: ip_ifnat_modified: old_if 0, new_if 2 4d05h: ip_ifnat_modified: old_if 0, new_if 2 4d05h: ip_ifnat_modified: old_if 1, new_if 2 4d05h: EZVPN(SJVPN): New State: SS_OPEN 4d05h: ISAKMP (0:3): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE 4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.254.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-sha-hmac , lifedur= 2147483s and 4608000kb, spi= 0xE6DB9372(3873149810), conn_id= 0, keysize= 0, flags= 0x400C 4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.254.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 2147483s and 4608000kb, spi= 0x3C77C53D(1014482237), conn_id= 0, keysize= 0, flags= 0x400C 4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.254.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-sha-hmac , lifedur= 2147483s and 4608000kb, spi= 0x79BB8DF4(2042334708), conn_id= 0, keysize= 0, flags= 0x400C 4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41,

local_proxy= 192.168.254.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 2147483s and 4608000kb, spi= 0x19C3A5B2(432252338), conn_id= 0, keysize= 0, flags= 0x400C 4d05h: ISAKMP: received ke message (1/4) 4d05h: ISAKMP: set new node 0 to QM_IDLE 4d05h: EZVPN(SJVPN): Current State: SS_OPEN 4d05h: EZVPN(SJVPN): Event: SOCKET_READY 4d05h: EZVPN(SJVPN): No state change 4d05h: ISAKMP (0:3): sitting IDLE. Starting QM immediately (QM_IDLE) 4d05h: ISAKMP (0:3): beginning Quick Mode exchange, M-ID of -1494477527 4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.253.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-sha-hmac , lifedur= 2147483s and 4608000kb, spi= 0xB18CF11E(2978803998), conn_id= 0, keysize= 0, flags= 0x400C 4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.253.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 2147483s and 4608000kb, spi= 0xA8C469EC(2831444460), conn_id= 0, keysize= 0, flags= 0x400C 4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.253.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-sha-hmac , lifedur= 2147483s and 4608000kb, spi= 0xBC5AD5EE(3160069614), conn_id= 0, keysize= 0, flags= 0x400C 4d05h: IPSEC(sa_request): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.253.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 2147483s and 4608000kb, spi= 0x8C34C692(2352268946), conn_id= 0, keysize= 0, flags= 0x400C 4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) QM_IDLE 4d05h: ISAKMP (0:3): Node -1494477527, Input = IKE_MESG_INTERNAL, IKE_INIT_QM Old State = IKE_QM_READY New State = IKE_QM_I_QM1 4d05h: ISAKMP: received ke message (1/4) 4d05h: ISAKMP: set new node 0 to QM_IDLE 4d05h: ISAKMP (0:3): sitting IDLE. Starting QM immediately (QM_IDLE) 4d05h: ISAKMP (0:3): beginning Quick Mode exchange, M-ID of -1102788797 4d05h: EZVPN(SJVPN): Current State: SS_OPEN 4d05h: EZVPN(SJVPN): Event: SOCKET_READY 4d05h: EZVPN(SJVPN): No state change 4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) QM_IDLE 4d05h: ISAKMP (0:3): Node -1102788797, Input = IKE_MESG_INTERNAL, IKE_INIT_QM Old State = IKE_QM_READY New State = IKE_QM_I_QM1 4d05h: ISAKMP (0:3): received packet from 172.16.172.41 (I) QM_IDLE 4d05h: ISAKMP: set new node 733055375 to QM_IDLE 4d05h: ISAKMP (0:3): processing HASH payload. message ID = 733055375 4d05h: ISAKMP (0:3): processing NOTIFY RESPONDER_LIFETIME protocol 1 spi 0, message ID = 733055375, sa = 820ABFA0 4d05h: ISAKMP (0:3): processing responder lifetime 4d05h: ISAKMP (0:3): start processing isakmp responder lifetime 4d05h: ISAKMP (0:3): restart ike sa timer to 86400 secs 4d05h: ISAKMP (0:3): deleting node 733055375 error FALSE reason "informational (in) state 1" 4d05h: ISAKMP (0:3): Input = IKE_MESG_FROM_PEER, IKE_INFO_NOTIFY Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE 4d05h: ISAKMP (0:3): received packet from 172.16.172.41 (I) QM_IDLE 4d05h: ISAKMP (0:3): processing HASH payload. message ID = -1494477527 4d05h: ISAKMP (0:3): processing SA payload. message ID = -1494477527 4d05h: ISAKMP (0:3): Checking IPSec proposal 1 4d05h: ISAKMP: transform 1, ESP_3DES 4d05h: ISAKMP: attributes in transform: 4d05h: ISAKMP: SA life type in seconds 4d05h: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B 4d05h: ISAKMP: SA life type in kilobytes 4d05h: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 4d05h: ISAKMP: encaps is 1 4d05h: ISAKMP: authenticator is HMAC-MD5 4d05h: ISAKMP (0:3): atts are acceptable. 4d05h: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.254.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 4d05h: ISAKMP (0:3): processing NONCE payload. message ID = -1494477527 4d05h: ISAKMP (0:3): processing ID payload. message ID = -1494477527 4d05h: ISAKMP (0:3): processing ID payload. message ID = -1494477527 4d05h: ISAKMP (0:3): processing NOTIFY RESPONDER_LIFETIME protocol 3 spi 1344958901, message ID = -1494477527, sa = 820ABFA0 4d05h: ISAKMP (0:3): processing responder lifetime 4d05h: ISAKMP (3): responder lifetime of 28800s 4d05h: ISAKMP (3): responder lifetime of 0kb 4d05h: ISAKMP (0:3): Creating IPSec SAs 4d05h: inbound SA from 172.16.172.41 to 172.16.172.46 (proxy 0.0.0.0 to 192.168.254.0) 4d05h: has spi 0x3C77C53D and conn_id 2000 and flags 4 4d05h: lifetime of 28800 seconds 4d05h: outbound SA from 172.16.172.46 to 172.16.172.41 (proxy 192.168.254.0 to 0.0.0.0) 4d05h: has spi 1344958901 and conn_id 2001 and flags C 4d05h: lifetime of 28800 seconds 4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) QM_IDLE 4d05h: ISAKMP (0:3): deleting node -1494477527 error FALSE reason "" 4d05h: ISAKMP (0:3): Node -1494477527, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH Old State = IKE_QM_I_QM1 New State = IKE_QM_PHASE2_COMPLETE 4d05h: ISAKMP (0:3): received packet from 172.16.172.41 (I) QM_IDLE 4d05h: ISAKMP (0:3): processing HASH payload. message ID = -1102788797 4d05h: ISAKMP (0:3): processing SA payload. message ID = -1102788797 4d05h: ISAKMP (0:3): Checking IPSec proposal 1 4d05h: ISAKMP: transform 1, ESP_3DES 4d05h: ISAKMP: attributes in transform: 4d05h: ISAKMP: SA life type in seconds

4d05h: ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B 4d05h: ISAKMP: SA life type in kilobytes 4d05h: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 4d05h: ISAKMP: encaps is 1 4d05h: ISAKMP: authenticator is HMAC-MD5 4d05h: ISAKMP (0:3): atts are acceptable. 4d05h: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.253.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 4d05h: ISAKMP (0:3): processing NONCE payload. message ID = -1102788797 4d05h: ISAKMP (0:3): processing ID payload. message ID = -1102788797 4d05h: ISAKMP (0:3): processing ID payload. message ID = -1102788797 4d05h: ISAKMP (0:3): processing NOTIFY RESPONDER_LIFETIME protocol 3 spi 653862918, message ID = -1102788797, sa = 820ABFA0 4d05h: ISAKMP (0:3): processing responder lifetime 4d05h: ISAKMP (3): responder lifetime of 28800s 4d05h: ISAKMP (3): responder lifetime of 0kb 4d05h: IPSEC(key_engine): got a queue event... 4d05h: IPSEC(initialize_sas): , (key eng. msg.) INBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.254.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 28800s and 0kb, spi= 0x3C77C53D(1014482237), conn_id= 2000, keysize= 0, flags= 0x4 4d05h: IPSEC(initialize_sas): , (key eng. msg.) OUTBOUND local= 172.16.172.46, ,(remote= 172.16.172.41, local_proxy= **192.168.254.0**/255.255.255.0/0/0 (type=4 ,(remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4 , protocol= ESP, transform= esp-3des esp-md5-hmac ,lifedur= 28800s and 0kb spi= 0x502A71B5(1344958901), conn_id= 2001, keysize= 0, flags= 0xC ,4d05h: IPSEC(create_sa): sa created ,sa) sa_dest= 172.16.172.46, sa_prot= 50) ,(sa_spi= **0x3C77C53D(1014482237**

SPI that is used on inbound SA. sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2000 4d05h: *---!* IPSEC(create_sa): sa created, (sa) sa_dest= 172.16.172.41, sa_prot= 50, sa_spi= **,(0x502A71B5(1344958901**

SPI that is used on outbound SA. sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2001 4d05h: *---!* ISAKMP (0:3): Creating IPSec SAs 4d05h: inbound SA from 172.16.172.41 to 172.16.172.46 (proxy 0.0.0.0 to 192.168.253.0) 4d05h: has spi 0xA8C469EC and conn_id 2002 and flags 4 4d05h: lifetime of 28800 seconds 4d05h: outbound SA from 172.16.172.46 to 172.16.172.41 (proxy 192.168.253.0 to 0.0.0.0) 4d05h: has spi 653862918 and conn_id 2003 and flags C 4d05h: lifetime of 28800 seconds 4d05h: ISAKMP (0:3): sending packet to 172.16.172.41 (I) QM_IDLE 4d05h: ISAKMP (0:3): deleting node -1102788797 error FALSE reason "" 4d05h: ISAKMP (0:3): Node -1102788797, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH Old State = IKE_QM_I_QM1 New State = IKE_QM_PHASE2_COMPLETE 4d05h: ISAKMP: received ke message (4/1) 4d05h: ISAKMP: Locking CONFIG struct 0x81F433A4 for crypto_ikmp_config_handle_kei_mess, count 3 4d05h: EZVPN(SJVPN): Current State: SS_OPEN 4d05h: EZVPN(SJVPN): Event: MTU_CHANGED 4d05h: EZVPN(SJVPN): No state change 4d05h: IPSEC(key_engine): got a queue event... 4d05h: IPSEC(initialize_sas): , (key eng. msg.) INBOUND local= 172.16.172.46, remote= 172.16.172.41, local_proxy= 192.168.253.0/255.255.255.0/0/0 (type=4), remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 28800s and 0kb, spi= 0xA8C469EC(2831444460), conn_id= 2002, keysize= 0, flags= 0x4 4d05h: IPSEC(initialize_sas): , (key eng. msg.) OUTBOUND local= 172.16.172.46, remote= ,(172.16.172.41, local_proxy= **192.168.253.0**/255.255.255.0/0/0 (type=4 ,(remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4 , protocol= ESP, transform= esp-3des esp-md5-hmac ,lifedur= 28800s and 0kb spi= 0x26F92806(653862918), conn_id= 2003, keysize= 0, flags= 0xC ,4d05h: IPSEC(create_sa): sa created ,sa) sa_dest= 172.16.172.46, sa_prot= 50) ,(sa_spi= **0xA8C469EC(2831444460** sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2002 ,4d05h: IPSEC(create_sa): sa created ,sa) sa_dest= 172.16.172.41, sa_prot= 50) ,(sa_spi= **0x26F92806(653862918** sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2003 (4d05h: ISAKMP: received ke message (4/1 4d05h: ISAKMP: Locking CONFIG struct 0x81F433A4 for crypto_ikmp_config_handle_kei_mess, count 4 4d05h: EZVPN(SJVPN): Current State: SS_OPEN 4d05h: EZVPN(SJVPN): Event: SOCKET_UP 4d05h: ezvpn_socket_up 4d05h: EZVPN(SJVPN): New State: IPSEC_ACTIVE

```
4d05h: EZVPN(SJVPN): Current State: IPSEC_ACTIVE
4d05h: EZVPN(SJVPN): Event: MTU_CHANGED
4d05h: EZVPN(SJVPN): No state change
4d05h: EZVPN(SJVPN): Current State: IPSEC_ACTIVE
4d05h: EZVPN(SJVPN): Event: SOCKET_UP
4d05h: ezvpn_socket_up
4d05h: EZVPN(SJVPN): No state change
```

أوامر عرض IOS ذات الصلة لاستكشاف الأخطاء وإصلاحها من Cisco

```
ADSL)#show crypto ipsec client  ezvpn)1721-1
Tunnel name : SJVPN
,Inside interface list: Loopback0, Loopback1
Outside interface: FastEthernet0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
ADSL)#show  crypto  isakmp  sa)1721-1

dst     src         state         conn-id    slot

QM_IDLE          3       0   172.16.172.46   172.16.172.41

ADSL)#show crypto  ipsec sa)1721-1

interface: FastEthernet0
    Crypto map tag: FastEthernet0-head-0, local addr. 172.16.172.46
   (local  ident (addr/mask/prot/port): (192.168.253.0/255.255.255.0/0/0
   (remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0

current_peer: 172.16.172.41
{,PERMIT, flags={origin_is_acl
  pkts encaps: 100, #pkts encrypt: 100, #pkts digest 100#
  pkts decaps: 100, #pkts decrypt: 100, #pkts verify 100#
  pkts compressed: 0, #pkts decompressed: 0#
pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0#
  send errors 0, #recv errors 0#


  local crypto endpt.: 172.16.172.46, remote crypto endpt.: 172.16.172.41
  path mtu 1500, media mtu 1500
  current outbound spi: 26F92806


:inbound esp sas
(spi: 0xA8C469EC(2831444460
, transform: esp-3des esp-md5-hmac
{ ,in use settings ={Tunnel
slot: 0, conn id: 2002, flow_id: 3, crypto map: FastEthernet0-head-0
(sa timing: remaining key lifetime (k/sec): (4607848/28656
IV size: 8 bytes
replay detection support: Y
:inbound ah sas
:inbound pcp sas
:outbound esp sas
(spi: 0x26F92806(653862918
, transform: esp-3des esp-md5-hmac
{ ,in use settings ={Tunnel
slot: 0, conn id: 2003, flow_id: 4, crypto map: FastEthernet0-head-0
(sa timing: remaining key lifetime (k/sec): (4607848/28647
IV size: 8 bytes
replay detection support: Y
```

```
:outbound ah sas

:outbound pcp sas

(local  ident (addr/mask/prot/port): (192.168.254.0/255.255.255.0/0/0
(remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0
current_peer: 172.16.172.41
{,PERMIT, flags={origin_is_acl
pkts encaps: 105, #pkts encrypt: 105, #pkts digest 105#
pkts decaps: 105, #pkts decrypt: 105, #pkts verify 105#
pkts compressed: 0, #pkts decompressed: 0#
pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0#
send errors 0, #recv errors 0#
local crypto endpt.: 172.16.172.46, remote crypto endpt.: 172.16.172.41
path mtu 1500, media mtu 1500
current outbound spi: 502A71B5

:inbound esp sas
(spi: 0x3C77C53D(1014482237
, transform: esp-3des esp-md5-hmac
{ ,in use settings ={Tunnel
slot: 0, conn id: 2000, flow_id: 1, crypto map: FastEthernet0-head-0
(sa timing: remaining key lifetime (k/sec): (4607847/28644
IV size: 8 bytes
replay detection support: Y

:inbound ah sas

:inbound pcp sas

:outbound esp sas
(spi: 0x502A71B5(1344958901
, transform: esp-3des esp-md5-hmac
{ ,in use settings ={Tunnel
slot: 0, conn id: 2001, flow_id: 2, crypto map: FastEthernet0-head-0
(sa timing: remaining key lifetime (k/sec): (4607847/28644
IV size: 8 bytes
replay detection support: Y

:outbound ah sas

:outbound pcp sas
```

مسح نفق نشط

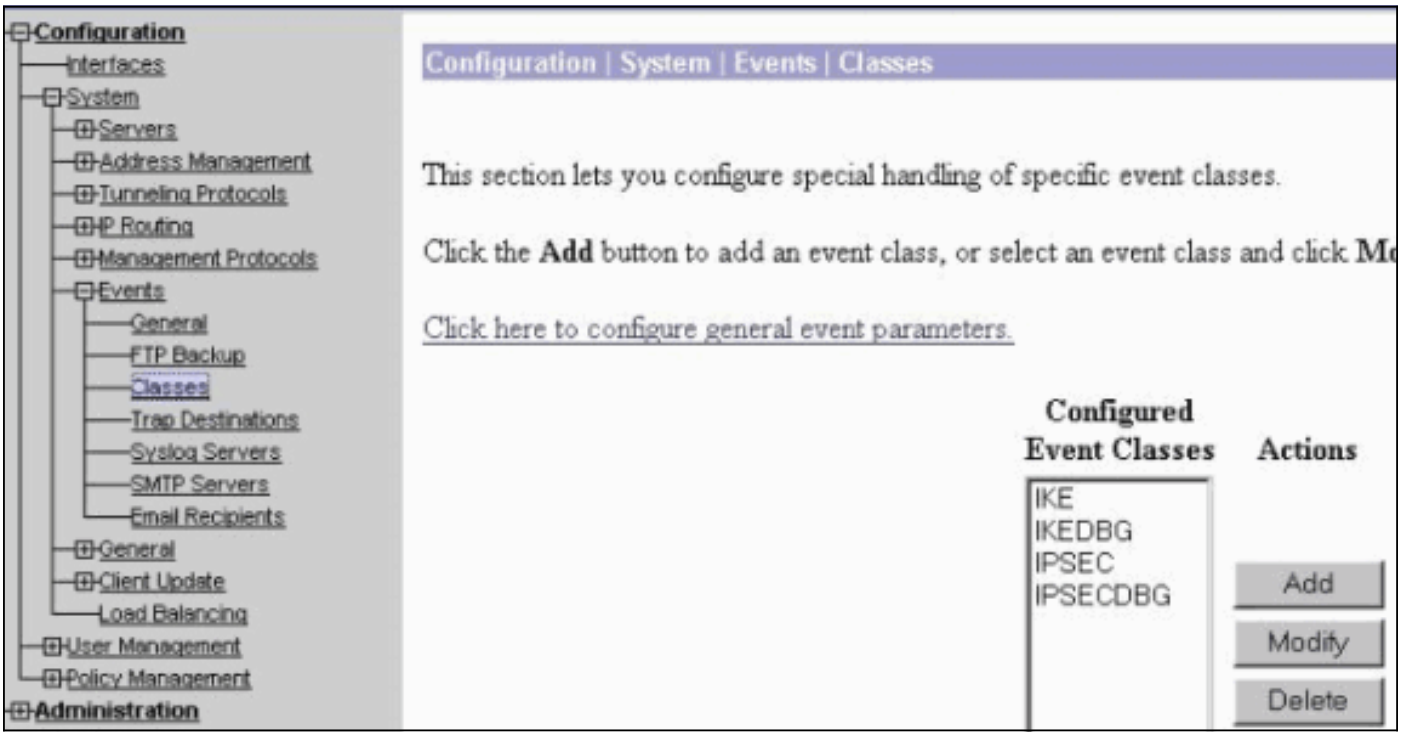
يمكنك مسح الأنفاق باستخدام هذه الأوامر:

- **مسح التشفير ISAKMP**
- **مسح التشفير(أ)**
- **مسح crypto ipSec client ezVPN**

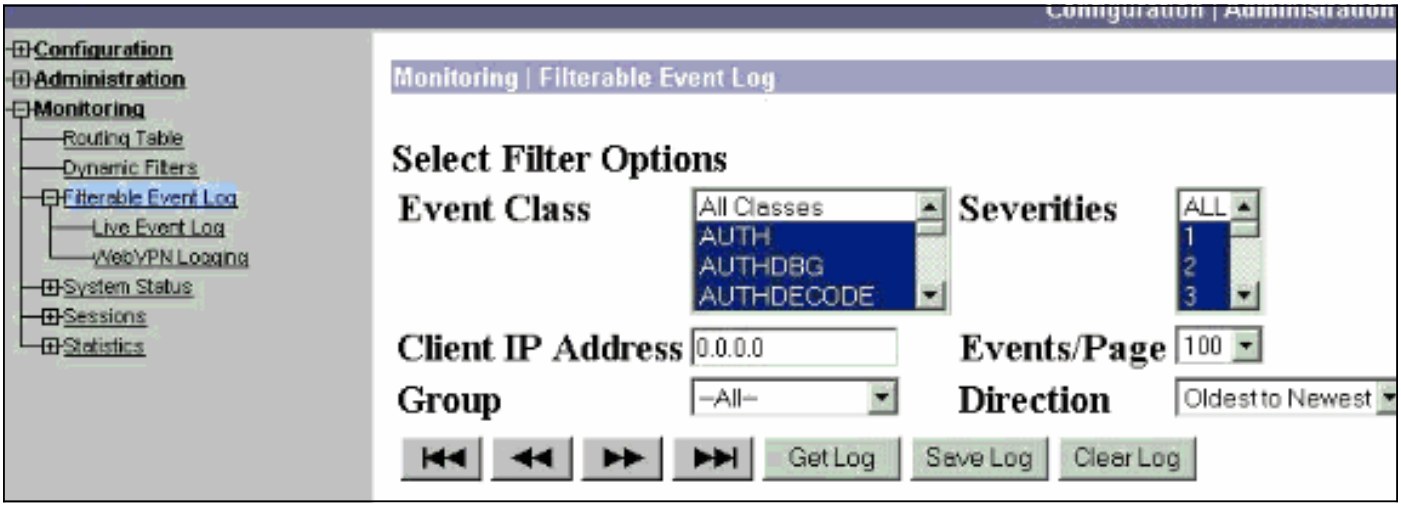
ملاحظة: يمكنك إستخدام مركز VPN لتسجيل الخروج من جلسة العمل عند إختيار **إدارة > جلسات عمل المسؤول**، وحدد المستخدم في **جلسة عمل الوصول عن بعد** وانقر فوق **تسجيل الخروج**.

تصحيح أخطاء مركز VPN 3000

أخترت **تشكيل>نظام>أحداث>صنف** in order to مكنت هذا تصحيح إن هناك حدث توصيل إخفاق. يمكنك دائما إضافة المزيد من الفئات إذا كانت الفئات المعروضة لا تساعدك على تحديد المشكلة.



لعرض سجل الأحداث الحالي في الذاكرة، قابل للتصفية حسب فئة الحدث وخطورته وعنوان IP وما إلى ذلك، أختر **المراقبة > سجل الأحداث القابل للتصفية**.



لعرض إحصائيات بروتوكول IPsec، أختر **مراقبة > إحصائيات > IPSec**. يوضح هذا الإطار إحصائيات نشاط IPsec، بما في ذلك أنفاق IPsec الحالية، على مركز VPN منذ آخر تمهيد أو إعادة تعيين له. تتوافق هذه الإحصائيات مع مسودة IETF لقاعدة معلومات الإدارة (MIB) الخاصة بمراقبة تدفق IPsec. يعرض نافذة **المراقبة > جلسات العمل > التفاصيل** أيضا بيانات IPsec.

Monitoring | Statistics | IPSec   Friday, 28 July 2006 10:00:1

Reset Refresh

IKE (Phase 1) Statistics

Active Tunnels	1
Total Tunnels	122
Received Bytes	2057442
Sent Bytes	332256
Received Packets	3041
Sent Packets	2128
Received Packets Dropped	1334
Sent Packets Dropped	0
Received Notifies	15
Sent Notifies	254
Received Phase-2 Exchanges	362

IPSec (Phase 2) Statistics

Active Tunnels	2
Total Tunnels	362
Received Bytes	0
Sent Bytes	1400
Received Packets	0
Sent Packets	5
Received Packets Dropped	0
Received Packets Dropped (Anti-Replay)	0
Sent Packets Dropped	0
Inbound Authentications	0

ما الذي يمكن أن يحدث بشكل خاطئ

- يعلق موجه Cisco IOS في حالة AG_INIT_EXCH. أثناء أستكشاف أخطاء IPsec و ISAKMP وإصلاحها، قم بتشغيل تصحيح الأخطاء باستخدام الأوامر التالية:**debug crypto ipSecdebug crypto isakmpdebug crypto ezVPN**على موجه Cisco IOS، ترى ما يلي:

```
5d16h: ISAKMP (0:9): beginning Aggressive Mode exchange
5d16h: ISAKMP (0:9): sending packet to 10.48.66.115 (I) AG_INIT_EXCH
...5d16h: ISAKMP (0:9): retransmitting phase 1 AG_INIT_EXCH
5d16h: ISAKMP (0:9): incrementing error counter on sa: retransmit phase 1
5d16h: ISAKMP (0:9): retransmitting phase 1 AG_INIT_EXCH
5d16h: ISAKMP (0:9): sending packet to 10.48.66.115 (I) AG_INIT_EXCH
...5d16h: ISAKMP (0:9): retransmitting phase 1 AG_INIT_EXCH
5d16h: ISAKMP (0:9): incrementing error counter on sa: retransmit phase 1
5d16h: ISAKMP (0:9): retransmitting phase 1 AG_INIT_EXCH
5d16h: ISAKMP (0:9): sending packet to 10.48.66.115 (I) AG_INIT_EXCH
...5d16h: ISAKMP (0:9): retransmitting phase 1 AG_INIT_EXCH
5d16h: ISAKMP (0:9): incrementing error counter on sa: retransmit phase 1
5d16h: ISAKMP (0:9): retransmitting phase 1 AG_INIT_EXCH
5d16h: ISAKMP (0:9): sending packet to 10.48.66.115 (I) AG_INIT_EXCH
```

  على مركز VPN 3000، يلزم توفر Xauth. ومع ذلك، لا يدعم الاقتراح المحدد Xauth. تحقق من تحديد المصادقة الداخلية لـ Xauth. قم بتمكين المصادقة الداخلية وتأكد من أن اقتراحات IKE لها وضع المصادقة المعين على **المفاتيح المعينة مسبقا (Xauth)**، كما هو الحال في لقطة الشاشة السابقة. طقطقة **يعدل** in order to حررت المقترح.
- كلمة المرور غير صحيحة.لا ترى رسالة **كلمة المرور غير الصالحة** على موجه Cisco IOS. على مركز VPN، قد ترى **الحدث غير المتوقع الذي تم تلقيه EV_ACTIVATE_NEW_SA في الحالة AM_TM_INIT_XAUTH**.تأكد من صحة كلمة المرور.
- اسم المستخدم غير صحيح.على موجه Cisco IOS، ترى تصحيح أخطاء مماثلا لهذا إذا كانت لديك كلمة المرور الخطأ. على مركز الشبكة الخاصة الظاهرية (VPN) ترى **رفض المصادقة: السبب = المستخدم لم يتم العثور عليه.**

معلومات ذات صلة

- صفحة دعم مركز Cisco VPN 3000 Series
- المرحلة الثانية البعيدة البسيطة لشبكة VPN من Cisco
- صفحة دعم عميل Cisco VPN 3000 Series
- صفحة 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).