# تكوين أمان RADIUS IPSec لمداخل WLCs و Microsoft Windows 2003 IAS

## المحتويات


المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
تكوين IPSec RADIUS
تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)
تكوين IAS
إعدادات أمان المجال ل Microsoft Windows 2003
أحداث سجل النظام ل Windows 2003
مثال تصحيح أخطاء نجاح IPSec لوحدة تحكم الشبكة المحلية اللاسلكية RADIUS
أسر إثربالي
معلومات ذات صلة


## المقدمة

يوثق هذا الدليل كيفية تكوين ميزة RADIUS IPSec التي يدعمها WCS ووحدات التحكم في الشبكة المحلية اللاسلكية (WLAN) التالية:

- السلسلة 4400
- WiSM
- 3750G

توجد ميزة RADIUS IPSec Controller على واجهة المستخدم الرسومية (GUI) لوحدة التحكم **ضمن قسم الأمان > AAA > خوادم مصادقة RADIUS**. توفر هذه الميزة طريقة لتشفير جميع إتصالات RADIUS بين وحدات التحكم وخوادم RADIUS (IAS) باستخدام IPSec.

## المتطلبات الأساسية

### المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة حول LWAPP
- معرفة مصادقة RADIUS و IPSec
- معرفة كيفية تكوين الخدمات على نظام تشغيل Windows 2003 Server

## المكونات المستخدمة

يجب تثبيت مكونات الشبكة والبرامج هذه وتكوينها من أجل نشر ميزة IPSec في بروتوكول RADIUS لوحدة التحكم:

- وحدات التحكم WLC 4400 أو WiSM أو 3750G. يستعمل هذا مثال WLC 4400 أن يركض برمجية صيغة 5.2.178.0
- نقاط الوصول Lightweight (LAPs). يستخدم هذا المثال نقطة الوصول في الوضع Lightweight من السلسلة 1231.
- التبديل باستخدام DHCP
- تم تكوين خادم Microsoft 2003 كوحدة تحكم بالمجال مثبتة بواسطة "مرجع شهادات Microsoft" و"خدمة مصادقة إنترنت (IAS) "Microsoft".
- أمان مجال Microsoft
- مهايئ عميل لاسلكي Cisco 802.11 a/b/g مع ADU الإصدار 3.6 مكون مع WPA2/ PEAP

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.

# تكوين IPSec RADIUS

لا يتناول دليل التكوين هذا تثبيت أو تكوين عميل Microsoft WinServer أو Certificate Authority أو Active Directory أو WLAN 802.1x. يجب تثبيت هذه المكونات وتكوينها قبل نشر ميزة IPSec RADIUS لوحدة التحكم. يوثق الجزء المتبقي من هذا الدليل كيفية تكوين IPSec RADIUS على هذه المكونات:

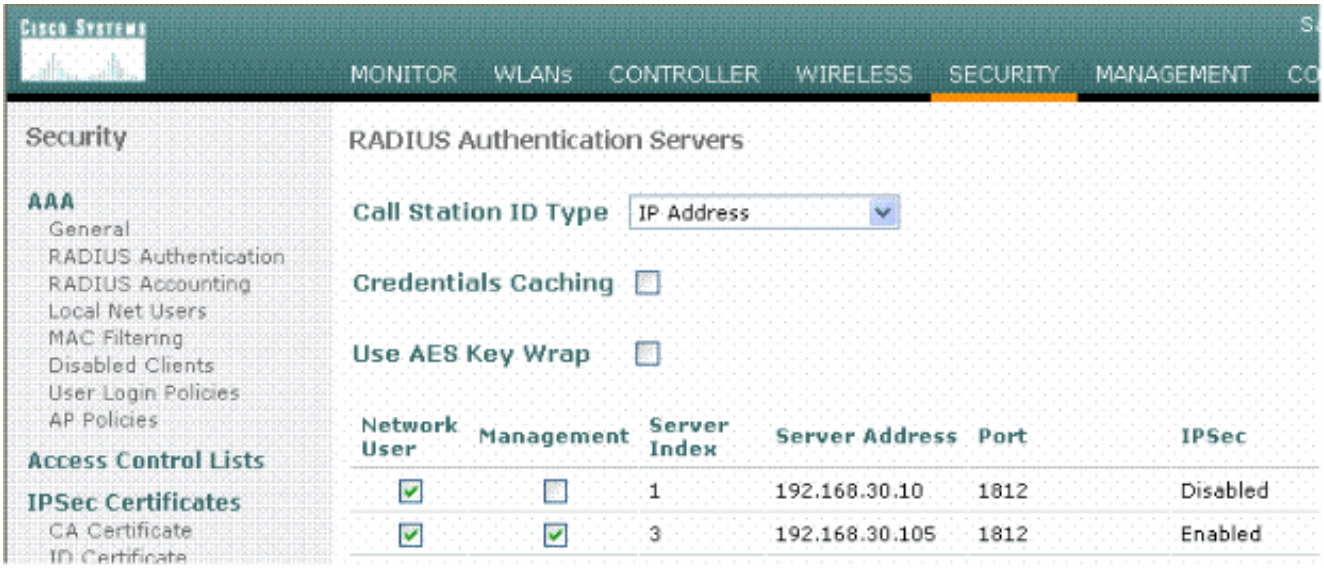
1. وحدات التحكم في الشبكة المحلية اللاسلكية (WLAN) من Cisco
2. Windows 2003 IAS
3. إعدادات أمان Microsoft Windows Domain

## تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)

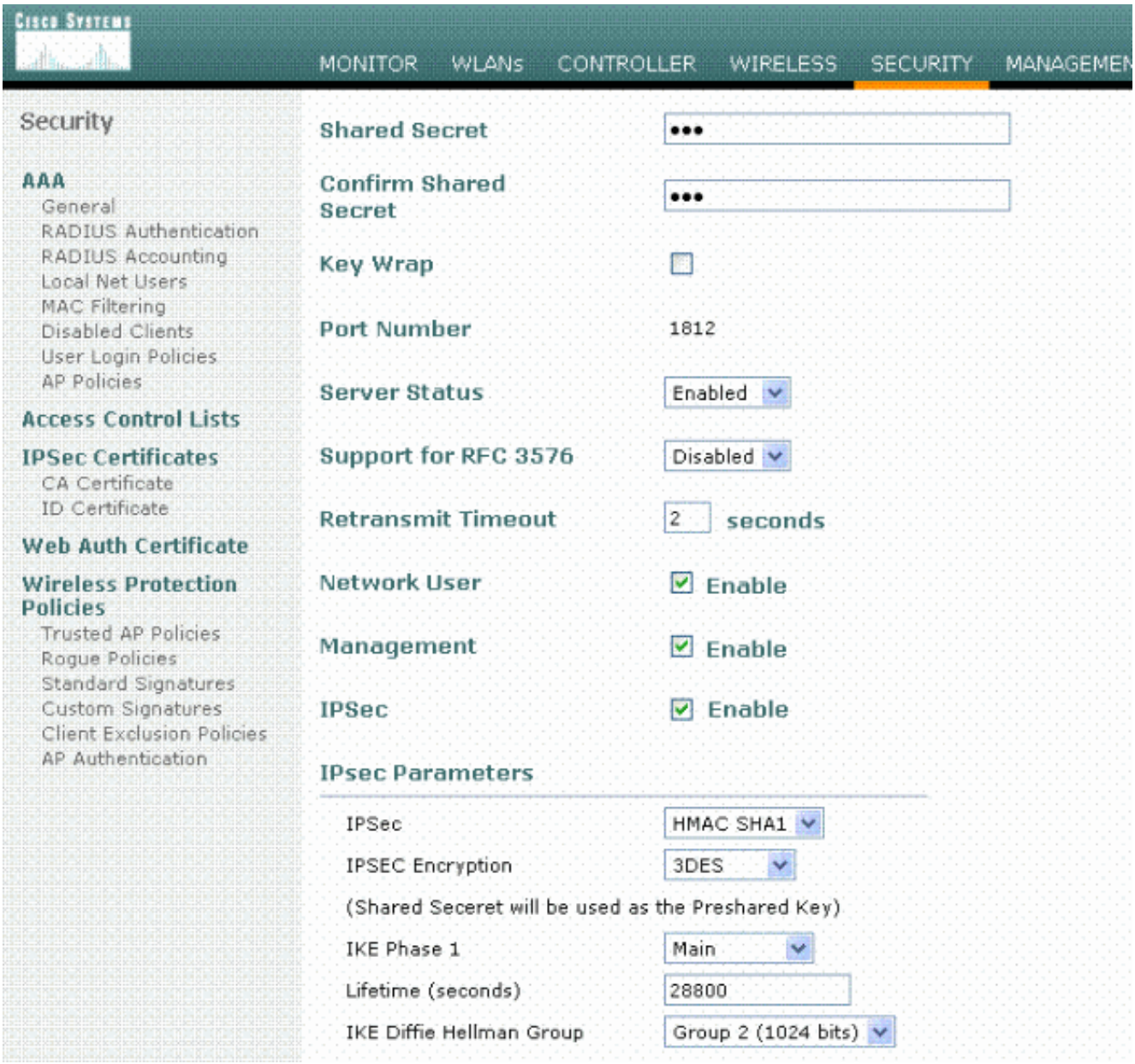
يشرح هذا القسم كيفية تكوين IPSec على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) من خلال واجهة المستخدم الرسومية (GUI).

من واجهة المستخدم الرسومية (GUI) لوحدة التحكم، أكمل الخطوات التالية.

1. انتقل إلى علامة التبويب **أمان > AAA > مصادقة RADIUS** في واجهة المستخدم الرسومية (GUI) لوحدة التحكم، وأضف خادم RADIUS جديد.



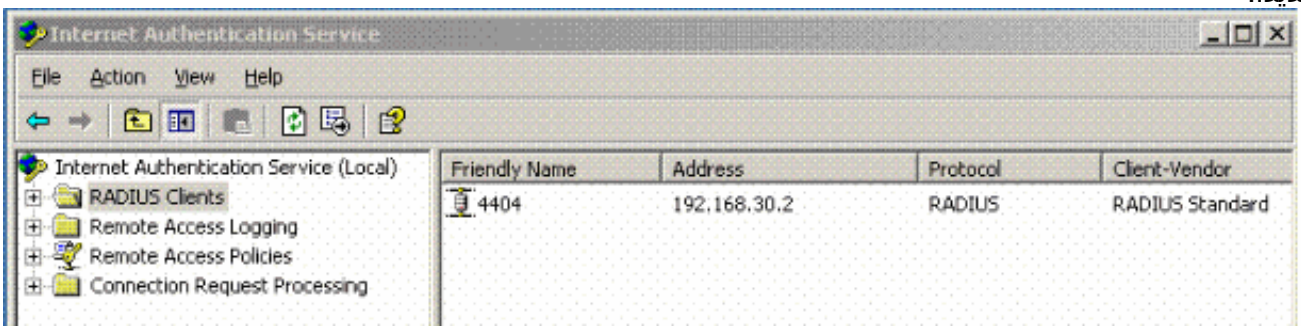

2. قم بتكوين عنوان IP، المنفذ 1812، وسر مشترك لخادم RADIUS الجديد. حدد خانة الاختيار **IPSec enable**-، وقم بتكوين معلمات IPSec هذه، ثم انقر فوق **تطبيق.ملاحظة:** يتم إستخدام السر المشترك لمصادقة خادم RADIUS وكمفتاح مشترك مسبقا (PSK) لمصادقة IPSec.



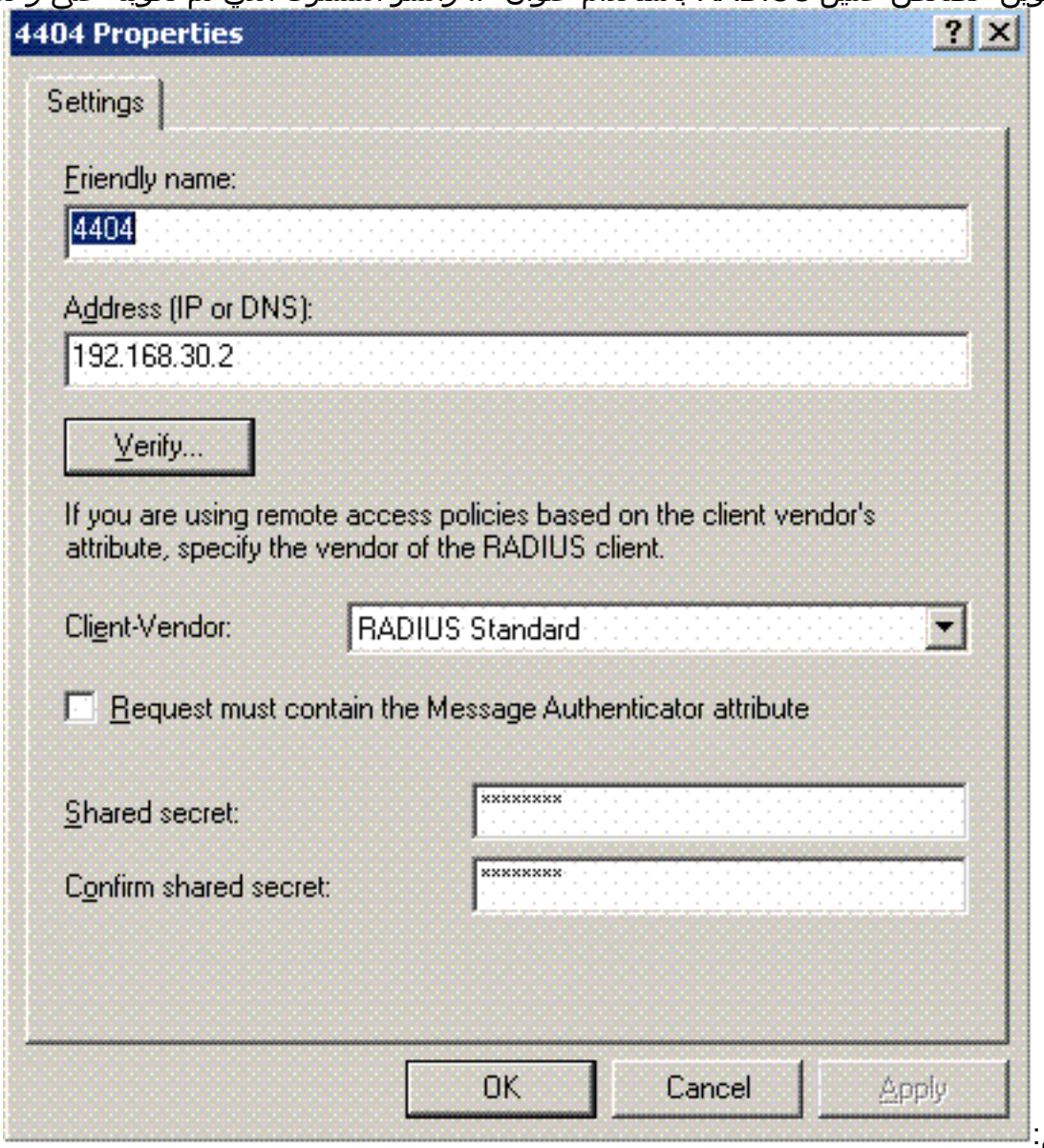
## تكوين IAS

أتمت هذا steps على ال IAS:

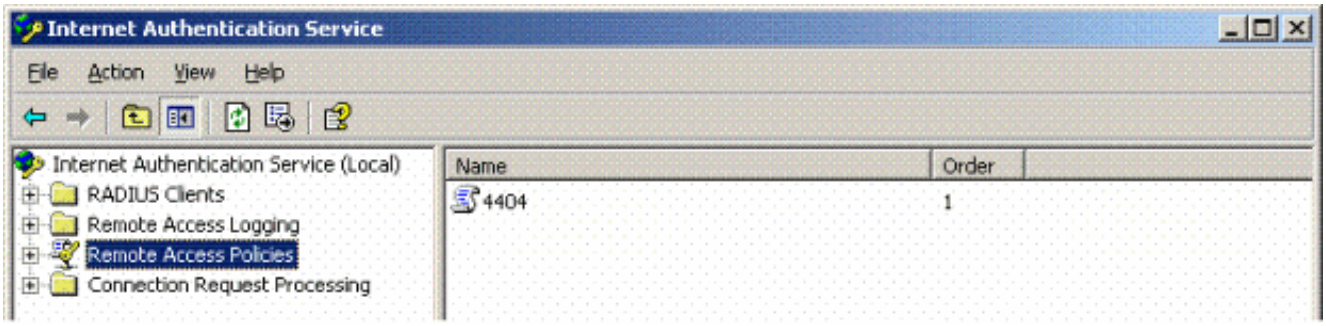
1. انتقل إلى مدير IAS في Win2003 وأضف عميل RADIUS جديدا.



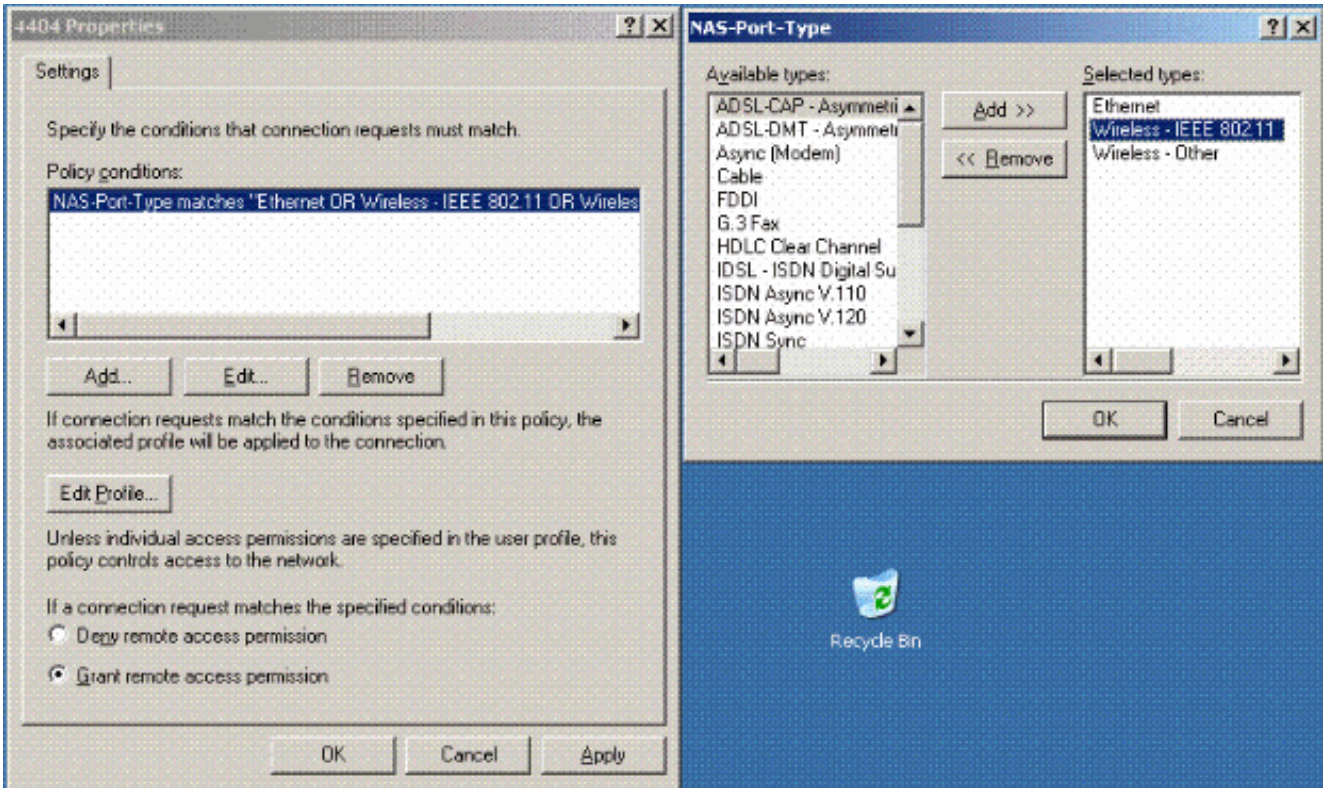

2. قم بتكوين خصائص عميل RADIUS باستخدام عنوان IP والسر المشترك الذي تم تكوينه على وحدة التحكم:



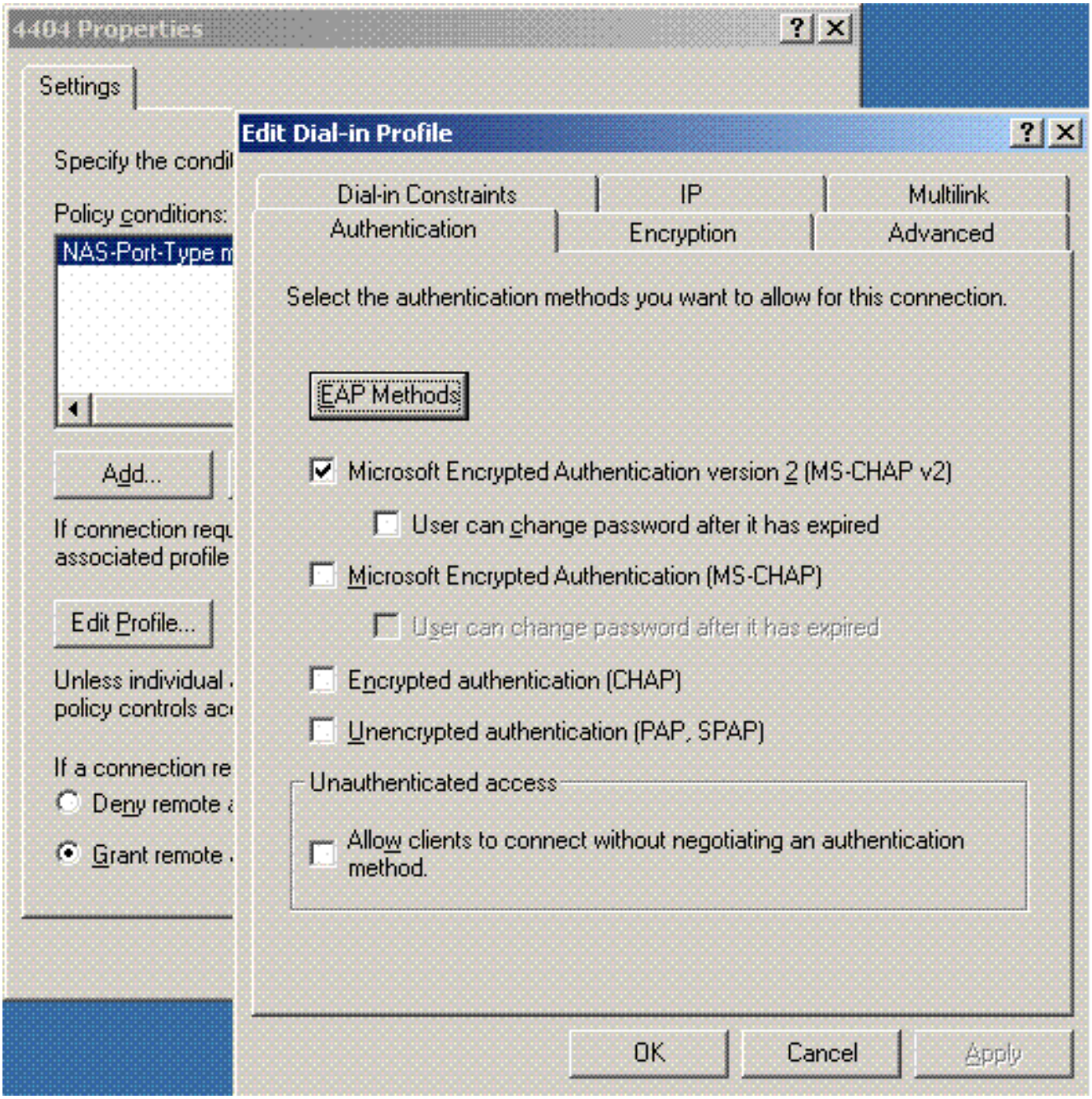

3. تكوين نهج وصول عن بعد جديد لوحدة التحكم:



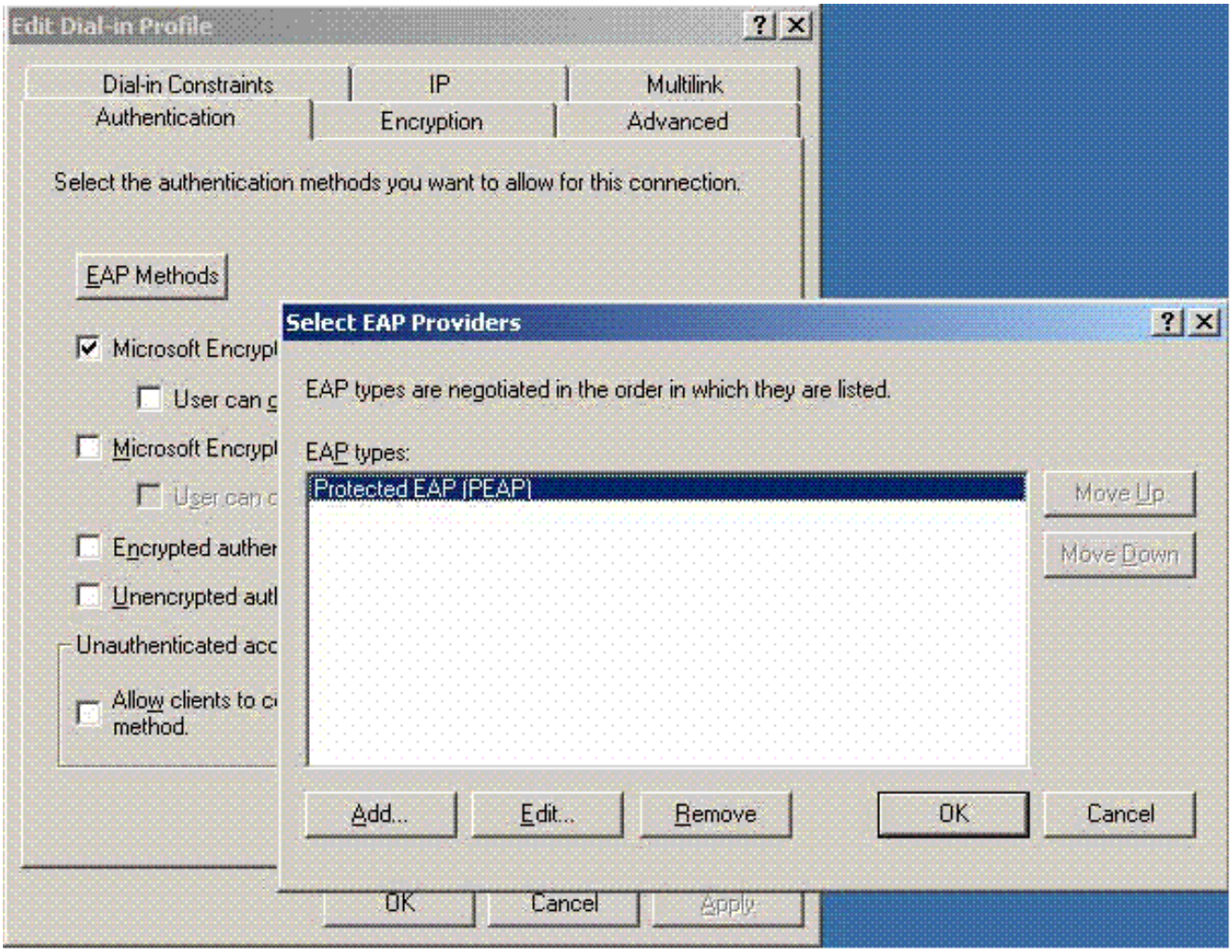

4. تحرير خصائص نهج الوصول عن بعد لوحدة التحكم. تأكد من إضافة نوع منفذ NAS - لاسلكي - IEEE 802.11:



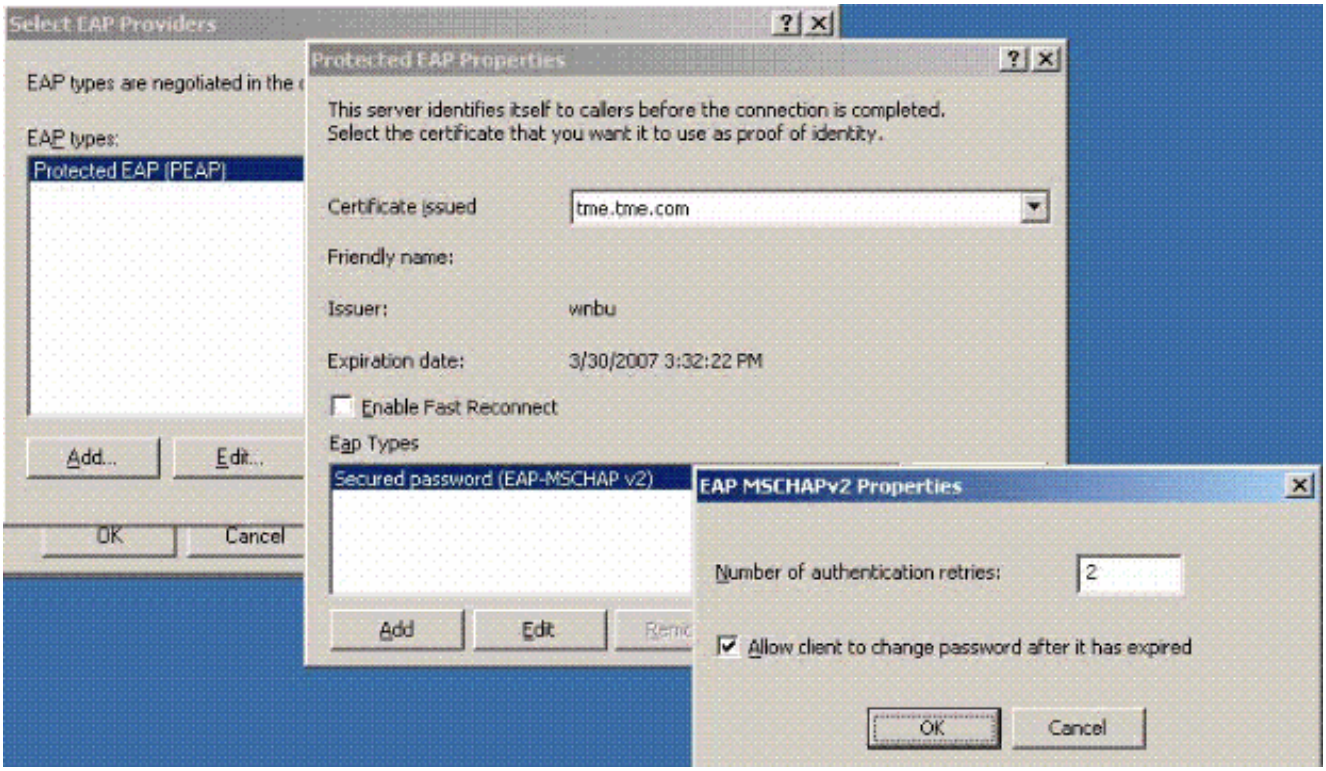

5. انقر على **تحرير ملف التعريف**، وانقر فوق علامة التبويب **المصادقة**، ثم تحقق من MS-CHAP V2 للمصادقة:



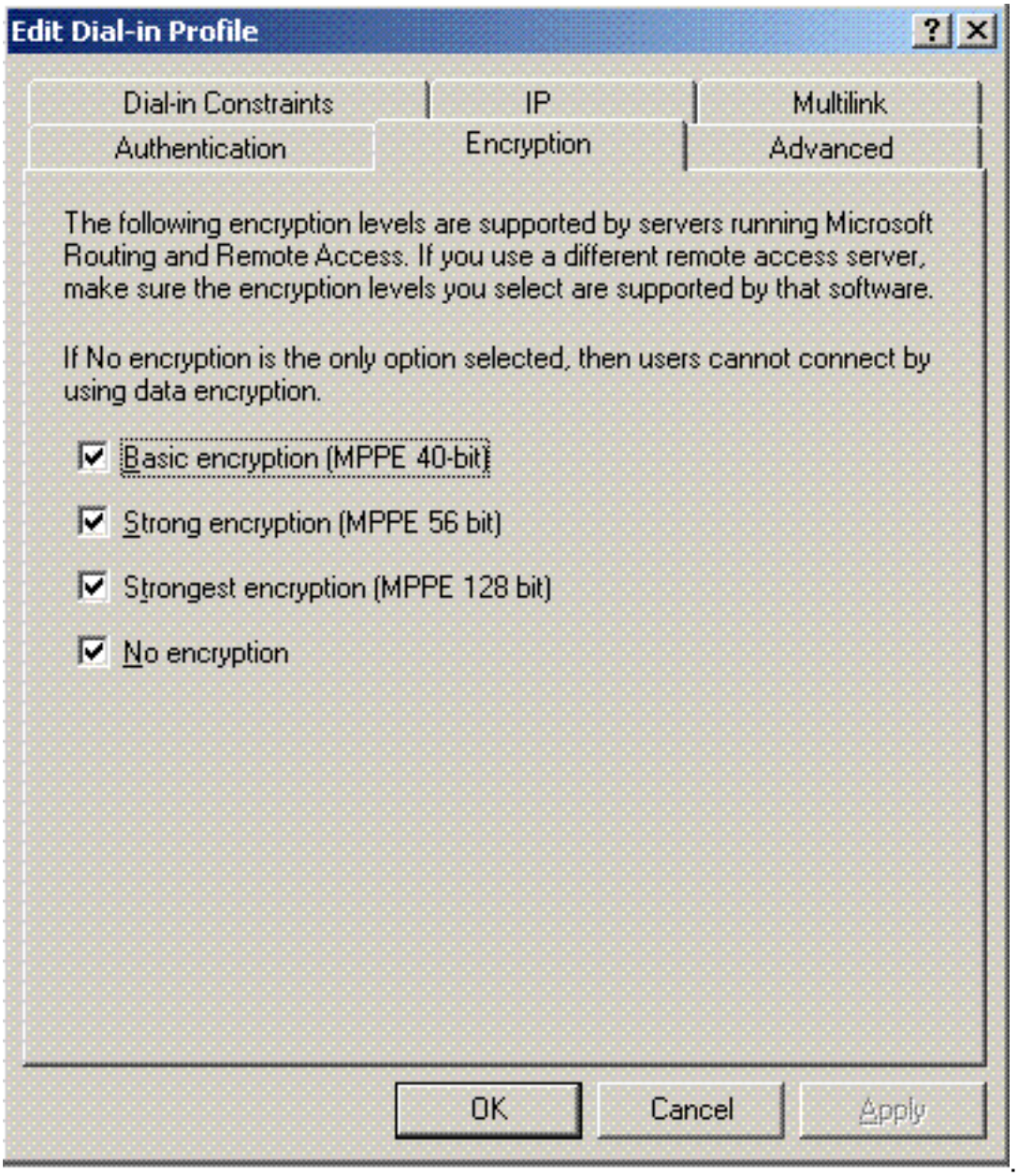

6. انقر على **أساليب EAP**، وحدد مزودي EAP، واضيف PEAP كنوع EAP:




7. انقر على **تحرير** في تحديد موفري EAP واختر من القائمة المنسدلة الخادم المقترن بحسابات مستخدمي Active Directory و CA (على سبيل المثال، tme.tme.com). إضافة نوع EAP MSCHAP v2:

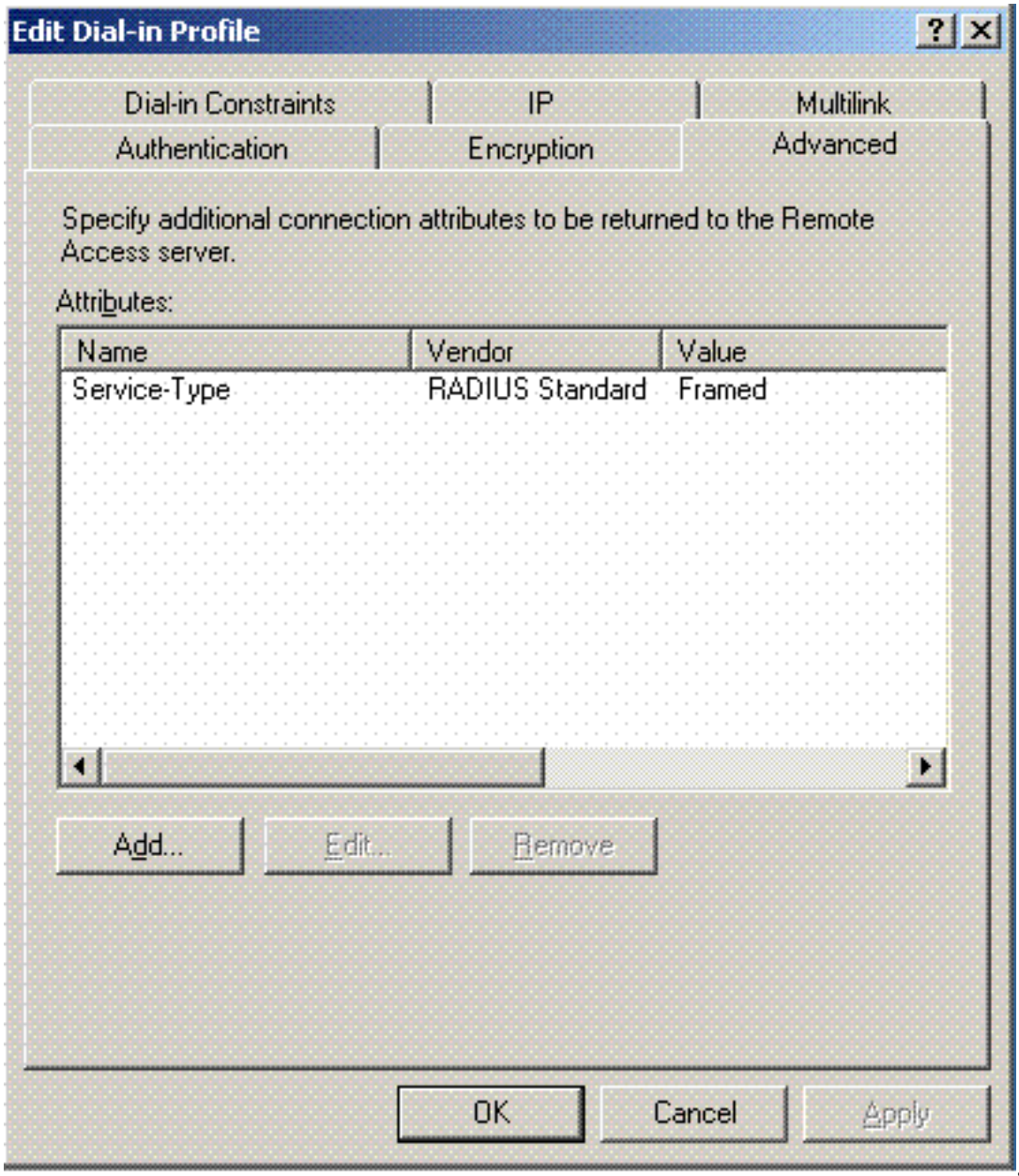



8. انقر فوق علامة التبويب **التشفير**، وفحص جميع أنواع التشفير للوصول عن



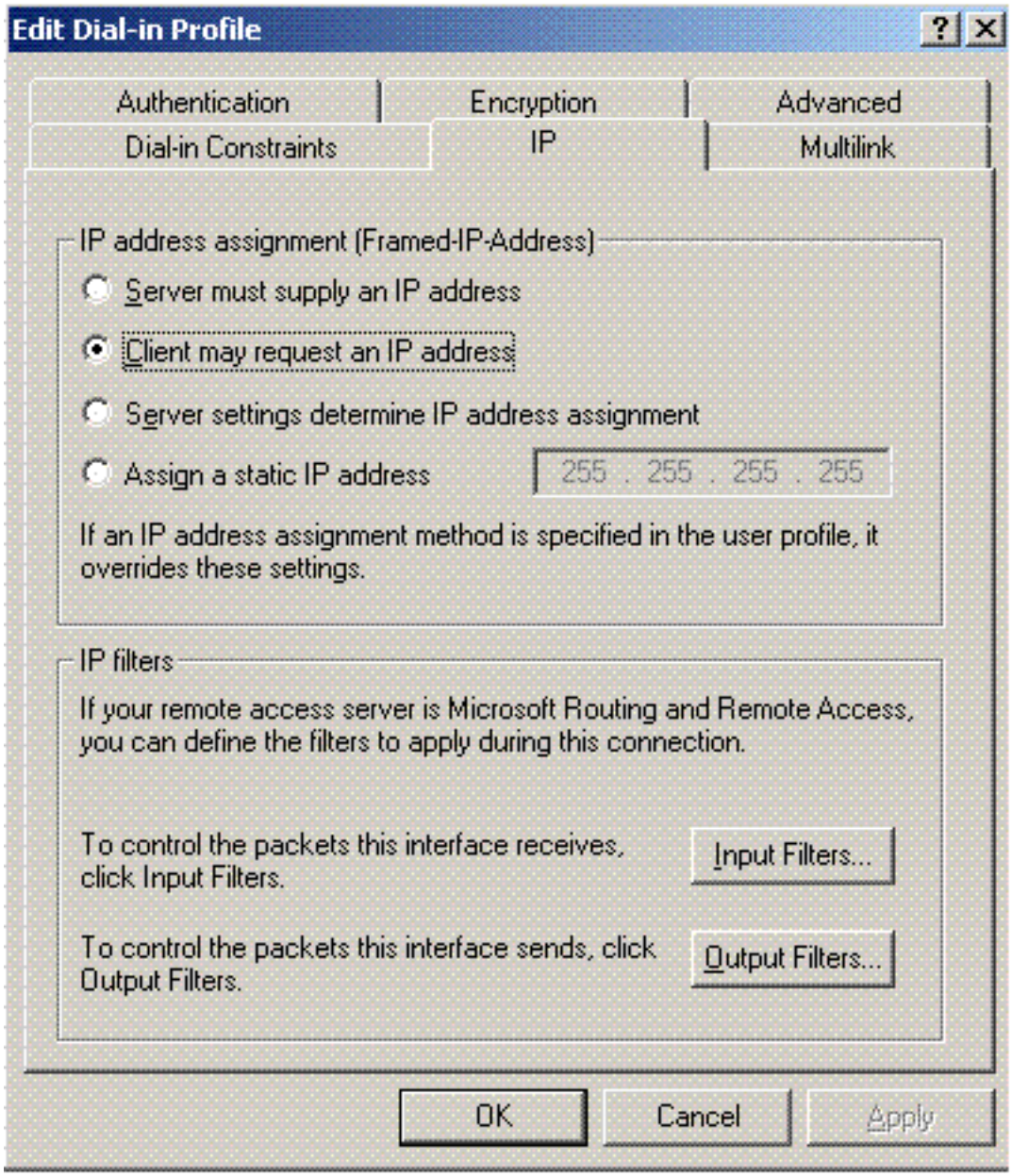

بعد:

9. انقر فوق علامة التبويب **خيارات متقدمة**، وقم بإضافة RADIUS Standard/Framed كنوع




الخدمة:

10. انقر فوق علامة التبويب **IP**، وتحقق من **إمكانية طلب العميل لعنوان IP**. هذا يفترض أن أنت تتلقى DHCP يمكن على مفتاح أو

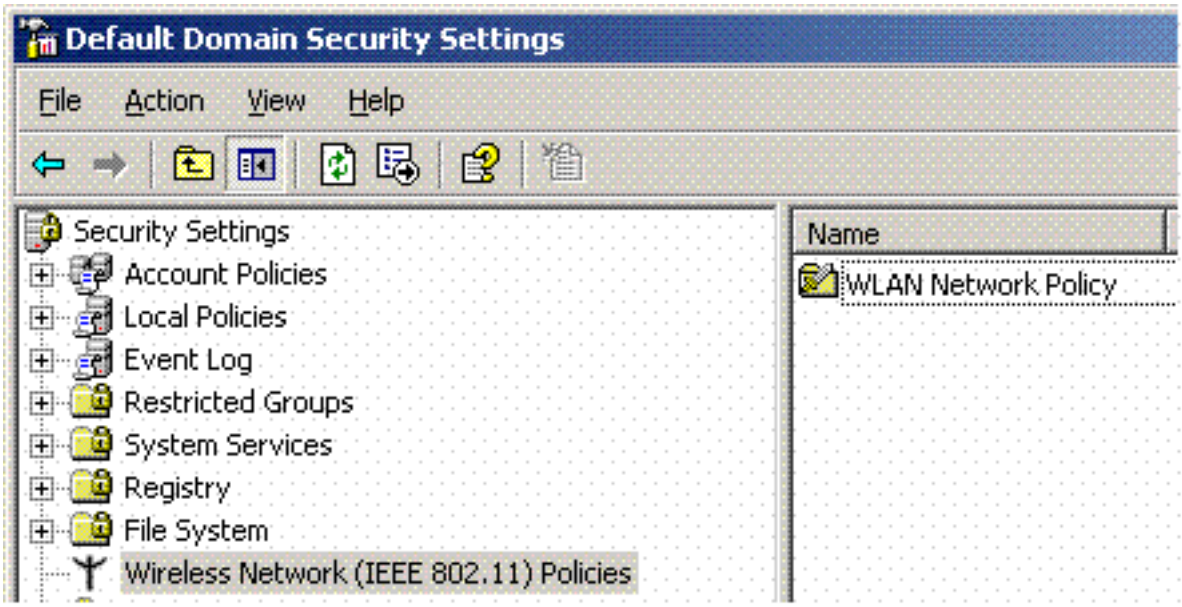


.WinServer

## [إعدادات أمان المجال ل Microsoft Windows 2003]

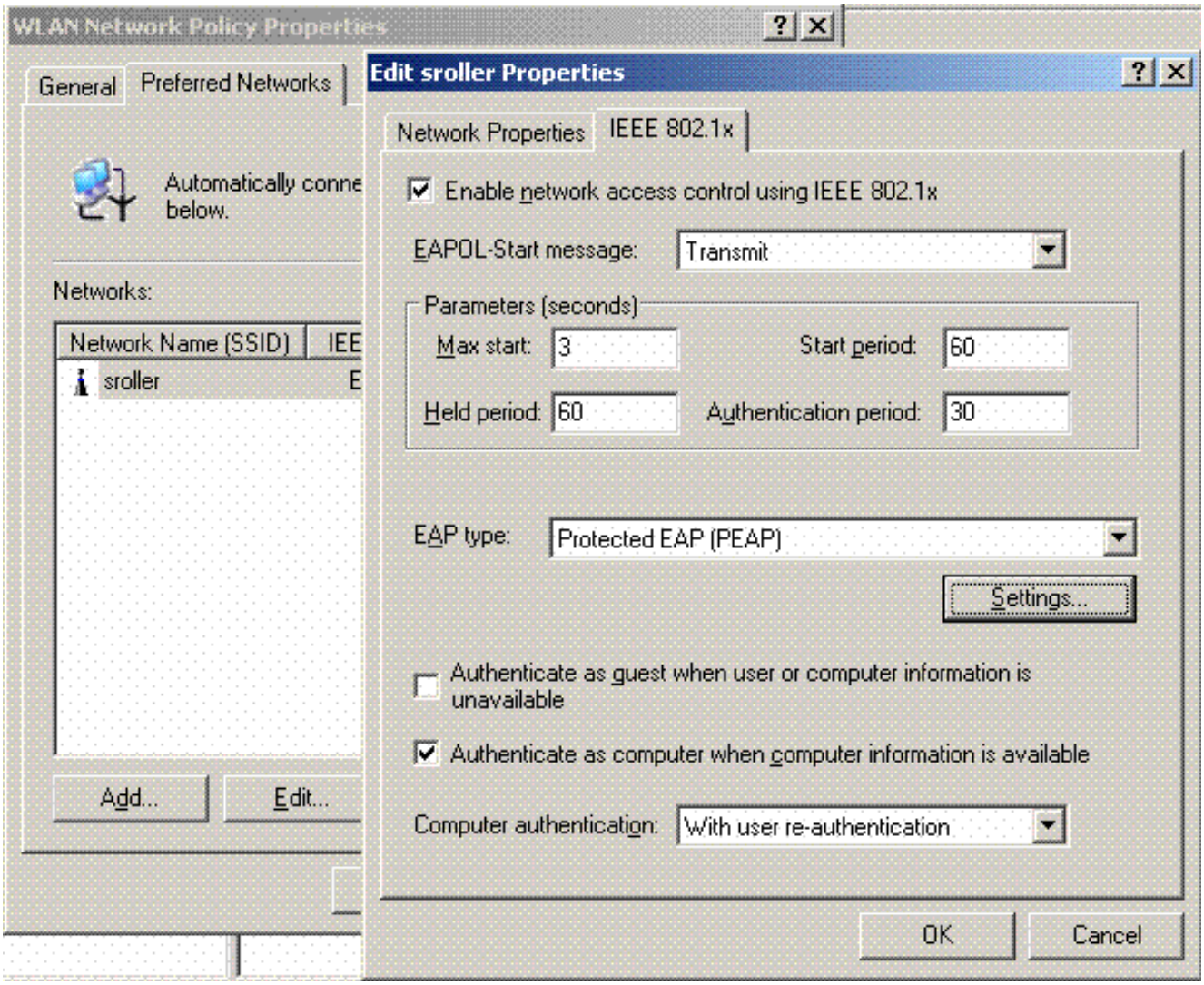
أكمل الخطوات التالية لتكوين إعدادات أمان مجال Windows 2003:

1. قم بتشغيل مدير إعدادات أمان المجال الافتراضية، وقم بإنشاء سياسة أمان جديدة لنهج الشبكة اللاسلكية IEEE)

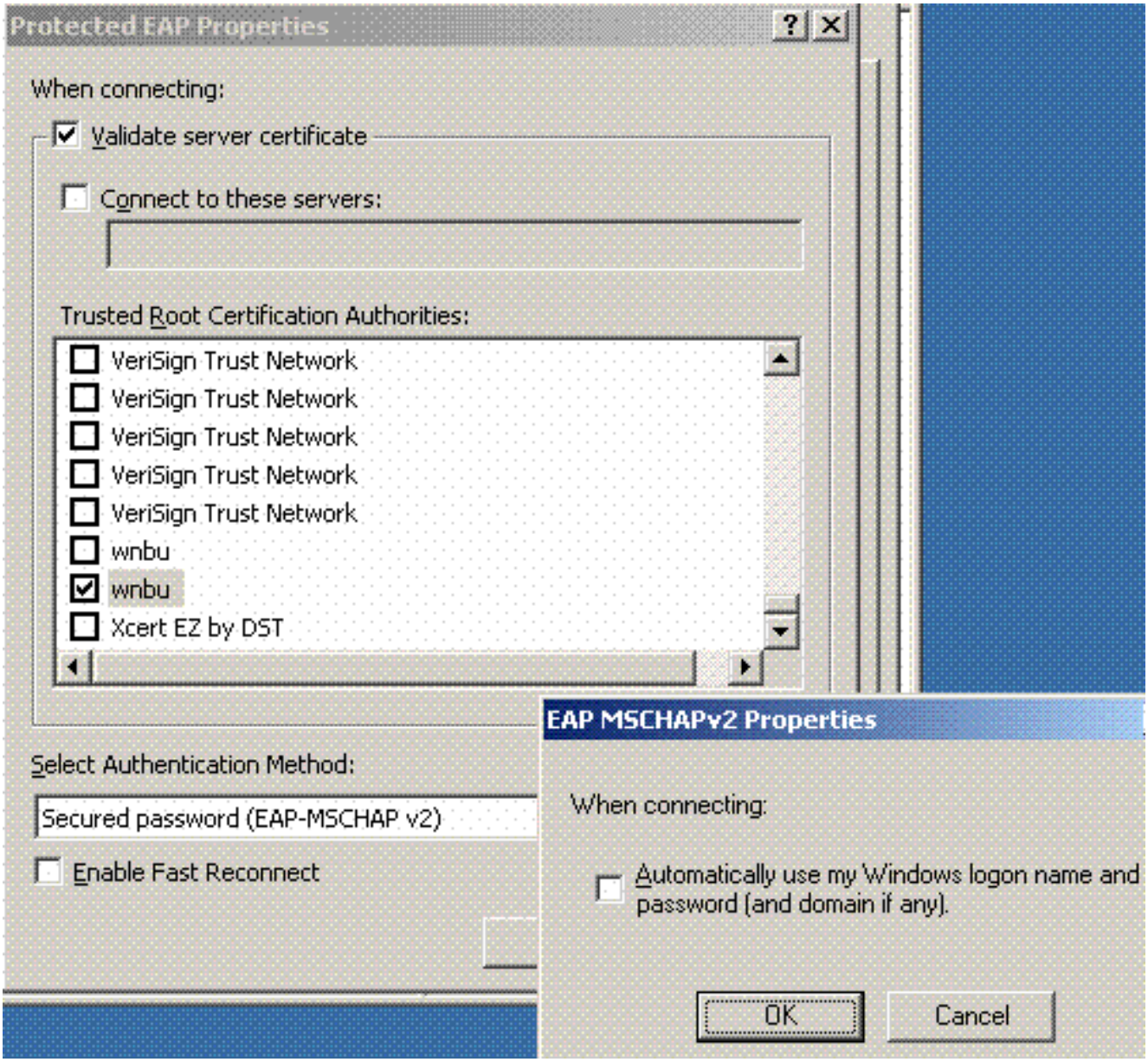



802.11).

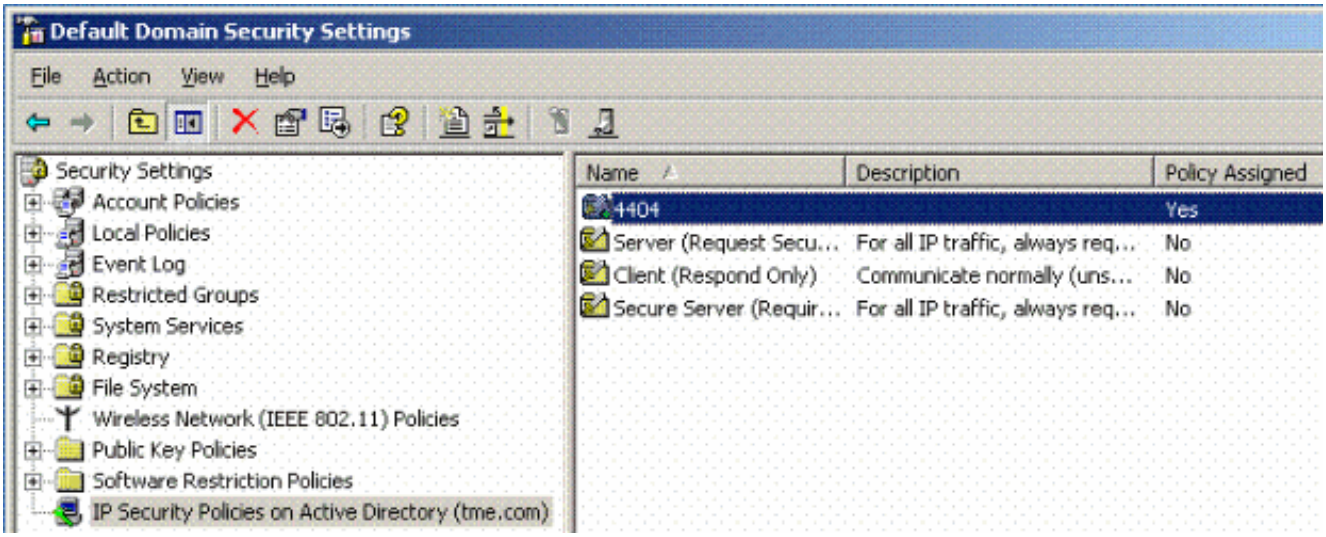
2. افتح خصائص نهج شبكة WLAN، وانقر فوق **الشبكات المفضلة**. أضف شبكة WLAN جديدة مفضلة واكتب اسم WLAN SSID، مثل . انقر نقرا مزدوجا على الشبكة المفضلة الجديدة ثم انقر على علامة التبويب **IEEE 802.1x**. أختر PEAP ليكون هو النوع EAP:



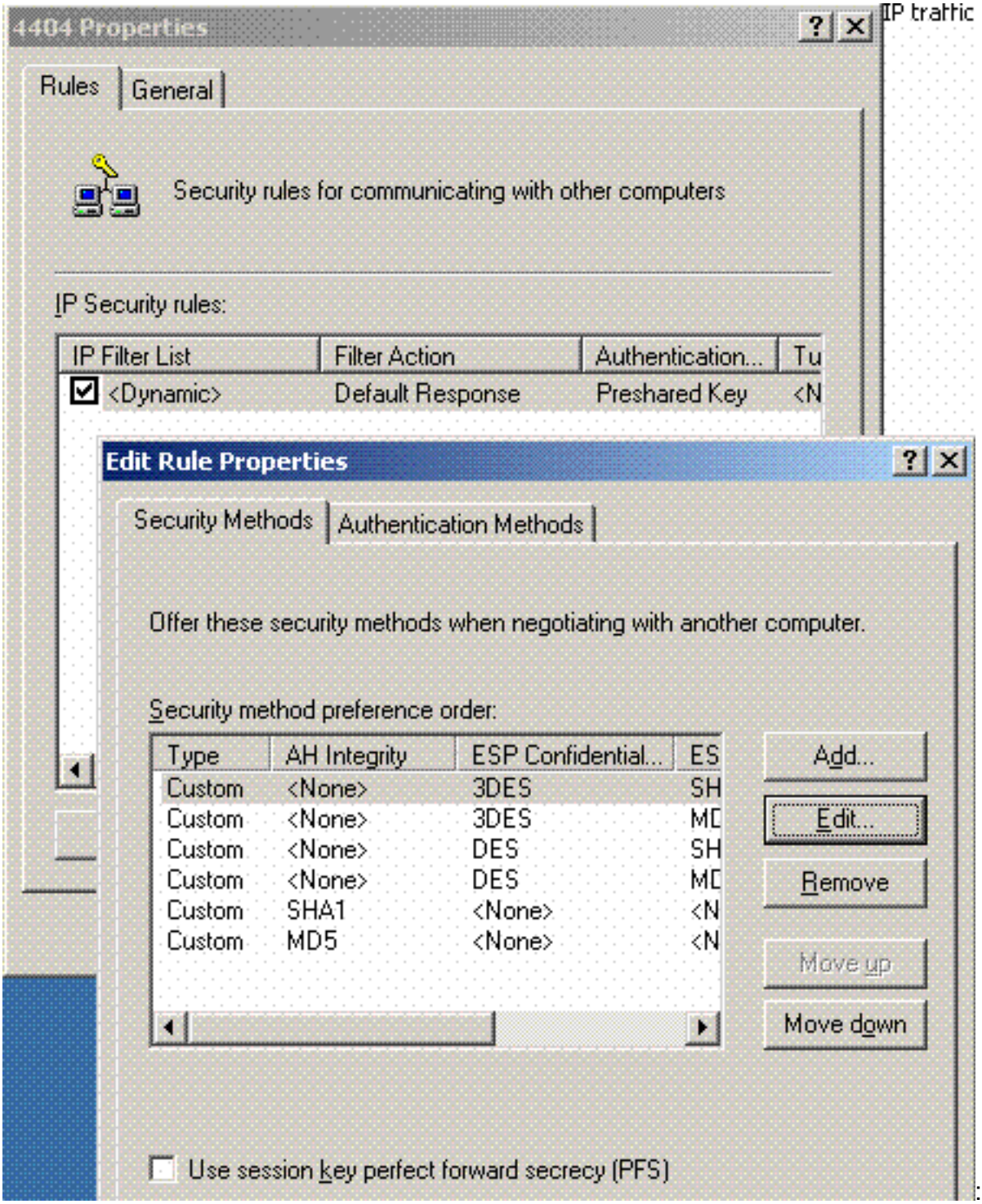

3. انقر على **إعدادات PEAP**، وتحقق من **التحقق من شهادة الخادم**، وحدد شهادة الجذر الموثوق بها المثبتة على المرجع المصدق. لأغراض الاختبار، قم بإلغاء تحديد مربع MS CHAP V2 لاستخدام تسجيل الدخول إلى Windows وكلمة المرور الخاصة بي تلقائيا.




4. في إطار إدارة إعدادات أمان المجال الافتراضية ل Windows 2003، قم بإنشاء نهج أمان IP جديدة أخرى على نهج Active Directory، مثل **4404**.

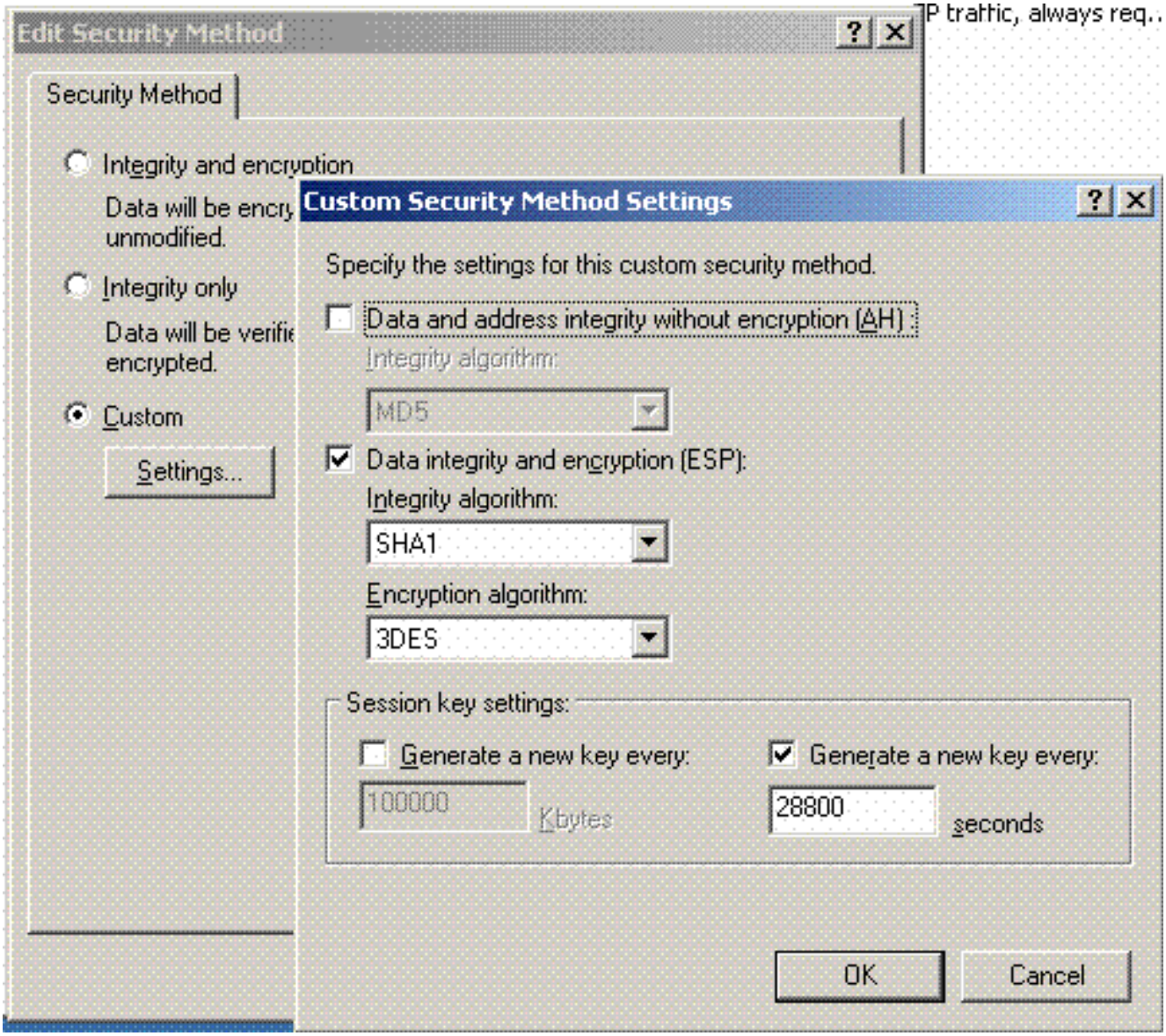



5. قم بتحرير خصائص نهج 4404 الجديدة، وانقر فوق علامة التبويب **قواعد**. إضافة قاعدة تصفية جديدة - قائمة ملفات IP (ديناميكية)؛ إجراء التصفية (الاستجابة الافتراضية)؛ المصادقة (PSK)؛ النفق (بلا). انقر نقرا مزدوجا على قاعدة المرشح التي تم إنشاؤها حديثا وحدد طرق

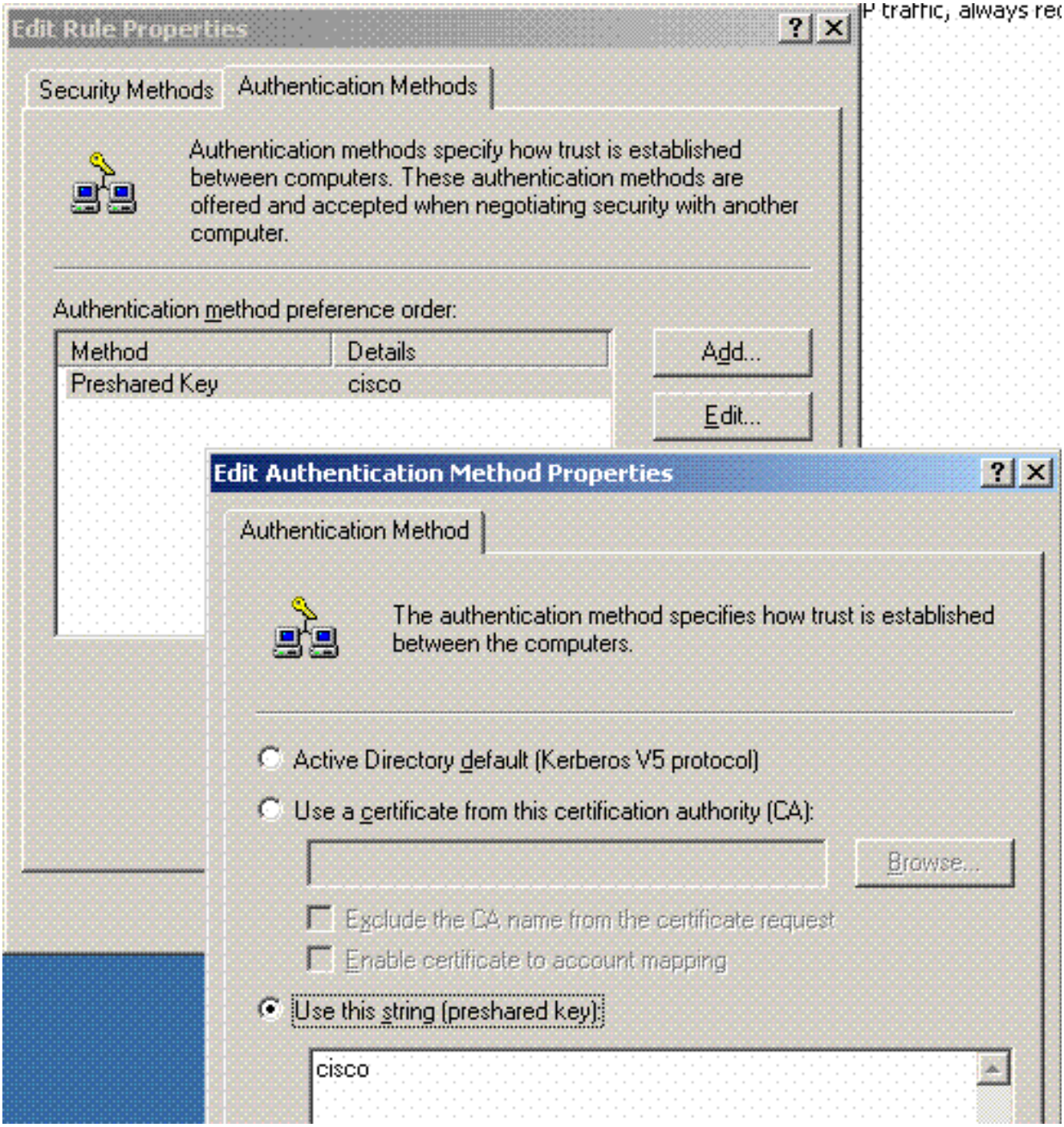



التأمين:

6. انقر **تحرير أسلوب التأمين**، وانقر زر انتقاء **الإعدادات المخصصة**. أخترت هذا عملية إعداد.**ملاحظة:** يجب أن تتطابق هذه الإعدادات مع إعدادات أمان IPSec الخاصة بوحدة التحكم RADIUS.




7. انقر فوق علامة التبويب **أسلوب المصادقة** ضمن خصائص قاعدة التحرير. أدخل نفس السر المشترك الذي أدخلته سابقا في تكوين RADIUS لوحدة التحكم.



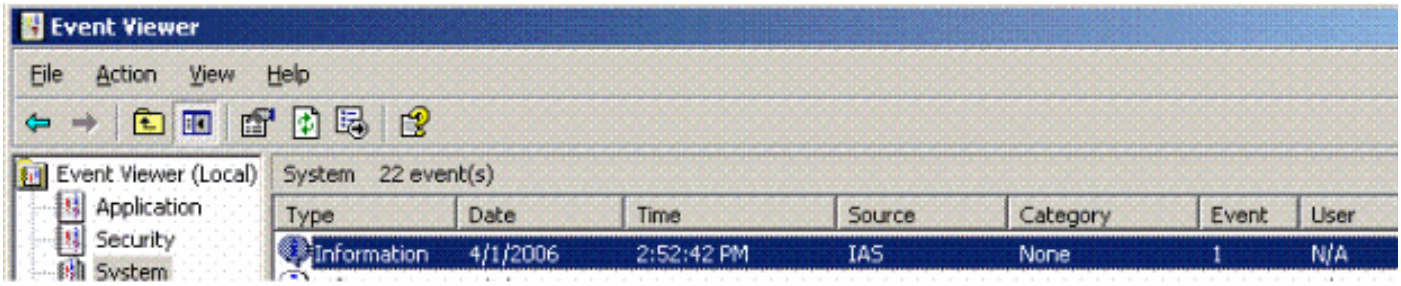

وعند هذه النقطة، يتم إكمال جميع التكوينات الخاصة بإعدادات وحدة التحكم و IAS وأمان المجال. قم بحفظ جميع التكوينات على كل من وحدة التحكم ونظام التشغيل WinServer وإعادة تمهيد جميع الأجهزة. على عميل WLAN الذي يتم إستخدامه للاختبار، قم بتثبيت الجذر والتكوين ل WPA2/PEAP. بعد تثبيت شهادة الجذر على العميل، أعد تشغيل جهاز العميل. بعد إعادة تمهيد جميع الأجهزة، قم بتوصيل العميل بالشبكة المحلية اللاسلكية (WLAN) والتقاط أحداث السجل هذه.

**ملاحظة:** يلزم اتصال عميل لإعداد اتصال IPSec بين وحدة التحكم و WinServer RADIUS.

## أحداث سجل النظام ل Windows 2003

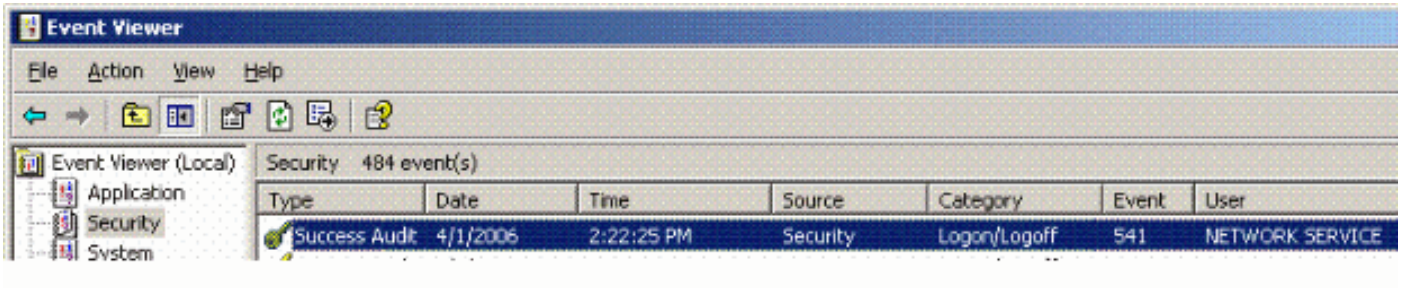
يقوم اتصال عميل شبكة WLAN الناجح الذي تم تكوينه ل WPA2/PEAP مع تمكين IPSec RADIUS بتوليد حدث النظام هذا على WinServer:

```
WinServer = 192.168.30.105
WLAN Controller = 192.168.30.2
```




```
.User TME0\Administrator was granted access
Fully-Qualified-User-Name = tme.com/Users/Administrator
NAS-IP-Address = 192.168.30.2
NAS-Identifier = Cisco_40:5f:23
Client-Friendly-Name = 4404
Client-IP-Address = 192.168.30.2
Calling-Station-Identifier = 00-40-96-A6-D4-6D
NAS-Port-Type = Wireless - IEEE 802.11
NAS-Port = 1
Proxy-Policy-Name = Use Windows authentication for all users
Authentication-Provider = Windows
<Authentication-Server = <undetermined
Policy-Name = 4404
Authentication-Type = PEAP
(EAP-Type = Secured password (EAP-MSCHAP v2
```

يقوم اتصال IPSec الخاص بوحدة التحكم الناجحة <> بإنشاء حدث الأمان هذا على سجلات WinServer:




```
.IKE security association established
(Mode: Data Protection Mode (Quick Mode
.Peer Identity: Preshared key ID
Peer IP Address: 192.168.30.2
:Filter
Source IP Address 192.168.30.105
Source IP Address Mask 255.255.255.255
Destination IP Address 192.168.30.2
Destination IP Address Mask 255.255.255.255
Protocol 17
Source Port 1812
Destination Port 0
IKE Local Addr 192.168.30.105
IKE Peer Addr 192.168.30.2
IKE Source Port 500
IKE Destination Port 500
Peer Private Addr
:Parameters
ESP Algorithm Triple DES CBC
HMAC Algorithm SHA
AH Algorithm None
Encapsulation Transport Mode
(InboundSpi 3531784413 (0xd282c0dd
```

```
(OutBoundSpi 4047139137 (0xf13a7141
Lifetime (sec) 28800
Lifetime (kb) 100000
QM delta time (sec) 0
Total delta time (sec) 0
```

## مثال تصحيح أخطاء نجاح IPSec لوحدة تحكم الشبكة المحلية اللاسلكية RADIUS

يمكنك إستخدام الأمر **debug pm ikemsg enable** على وحدة التحكم للتحقق من هذا التكوين. فيما يلي مثال.

```
Cisco Controller) >debug pm ikemsg enable)
Cisco Controller) >****** ERR: Connection timed out or error, calling callback)
TX MM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
ookie=0x0000000000000000
SA: doi=1 situation=0x1
[Proposal 0, proto=ISAKMP, # transforms=1, SPI[0
Transform#=0 TransformId=1, # SA Attributes = 6
EncrAlgo = 3DES-CBC
HashAlgo = SHA
AuthMethod = Pre-shared Key
GroupDescr =2
LifeType = secs
LifeDuration =28800
VID: vendor id[16] = 0x8f9cc94e 01248ecd f147594c 284b213b
VID: vendor id[16] = 0x27bab5dc 01ea0760 ea4e3190 ac27c0d0
VID: vendor id[16] = 0x6105c422 e76847e4 3f968480 1292aecd
VID: vendor id[16] = 0x4485152d 18b6bbcd 0be8a846 9579ddcc
VID: vendor id[16] = 0xcd604643 35df21f8 7cfdb2fc 68b6a448
VID: vendor id[16] = 0x90cb8091 3ebb696e 086381b5 ec427b1f
VID: vendor id[16] = 0x7d9419a6 5310ca6f 2c179d92 15529d56
VID: vendor id[16] = 0x12f5f28c 457168a9 702d9fe2 74cc0100
RX MM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
ookie=0x064bdcaf50d5f555
SA: doi=1 situation=0x1
[Proposal 1, proto=ISAKMP, # transforms=1 SPI[0
Transform payload: transf#=1 transfId=1, # SA Attributes = 6
EncrAlgo= 3DES-CBC
HashAlgo= SHA
GroupDescr=2
AuthMethod= Pre-shared Key
LifeType= secs
LifeDuration=28800
VENDOR ID: data[20] = 0x1e2b5169 05991c7d 7c96fcbf b587e461 00000004
VENDOR ID: data[16] = 0x4048b7d5 6ebce885 25e7de7f 00d6c2d3
VENDOR ID: data[16] = 0x90cb8091 3ebb696e 086381b5 ec427b1f
TX MM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
ookie=0x064bdcaf50d5f555
...KE: ke[128] = 0x9644af13 b4275866 478d294f d5408dc5 e243fc58
NONCE: nonce [16] = 0xede8dc12 c11be7a7 aa0640dd 4cd24657
PRV[payloadId=130]: data[20] = 0x1628f4af 61333b10 13390df8 85a0c0c2 93db6
c67
PRV[payloadId=130]: data[20] = 0xcf0bbd1c 55076966 94bccf4f e05e1533 191b1
378
RX MM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
ookie=0x064bdcaf50d5f555
...KE: ke[128] = 0x9f0420e5 b13adb04 a481e91c 8d1c4267 91c8b486
NONCE: nonce[20] = 0x011a4520 04e31ba1 6089d2d6 347549c3 260ad104
PRV payloadId=130: data[20] = 0xcf0bbd1c 55076966 94bccf4f e05e1533 191b13
78
PRV payloadId=130: data[20] = 0x1628f4af 61333b10 13390df8 85a0c0c2 93db6c
67
TX MM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
```

```
                                                ookie=0x064bdcaf50d5f555
                                            ID: packet[8] = 0x01000000 c0a81e69
                    HASH: hash[20] = 0x04814190 5d87caa1 221928de 820d9f6e ac2ef809
                            [NOTIFY: doi=1 proto=ISAKMP type=INITIAL_CONTACT, spi[0
                                                                [NOTIFY: data[0
RX MM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
                                                ookie=0x064bdcaf50d5f555
                                            ID: packet[8] = 0x01000000 c0a81e69
                    HASH: hash[20] = 0x3b26e590 66651f13 2a86f62d 1b1d1e71 064b43f6
TX QM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
                                        ookie=0x064bdcaf50d5f555 msgid=0x73915967
                    HASH: hash[20] = 0x00000000 00000000 00000000 00000000 00000000
                                                    SA: doi=1 situation=0x1
                         Proposal 1, proto=ESP, # transforms=1, SPI[4] = 0xbb243261
                                    Transform#=1 TransformId=3, # SA Attributes = 4
                                                        AuthAlgo = HMAC-SHA
                                                            LifeType = secs
                                                        LifeDuration =28800
                                                    EncapMode = Transport
                      NONCE: nonce [16] = 0x48a874dd 02d91720 29463981 209959bd
                                            ID: packet[8] = 0x01110000 c0a81e02
                                            ID: packet[8] = 0x01110714 c0a81e69
RX QM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
                                        ookie=0x064bdcaf50d5f555 msgid=0x73915967
                    HASH: hash[20] = 0x2228d010 84c6014e dd04ee05 4d15239a 32a9e2ba
                                                    SA: doi=1 situation=0x1
                        Proposal 1, proto=ESP, # transforms=1 SPI[4] = 0x7d117296
                   Transform payload: transf#=1 transfId=3, # SA Attributes = 4
                                                        LifeType= secs
                                                    LifeDuration=28800
                                                    EncapMode= Transport
                                                        AuthAlgo= HMAC-SHA
                  NONCE: nonce[20] = 0x5c4600e4 5938cbb0 760d47f4 024a59dd 63d7ddce
                                            ID: packet[8] = 0x01110000 c0a81e02
                                            ID: packet[8] = 0x01110714 c0a81e69
TX QM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
                                        ookie=0x064bdcaf50d5f555 msgid=0x73915967
                    HASH: hash[20] = 0x0e81093e bc26ebf3 d367297c d9f7c000 28a3662d
RX QM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rc
                                        ookie=0x064bdcaf50d5f555 msgid=0x73915967
                    HASH: hash[20] = 0xcb862635 2b30202f 83fc5d7a 2264619d b09faed2
                        NOTIFY: doi=1 proto=ESP type=CONNECTED, spi[4] = 0xbb243261
                                                    data[8] = 0x434f4e4e 45435431
```

## أسر إثريالي

هنا عينة إلتقاط ثري.

```
                                                    WinServer = 192.168.30.105
                                                WLAN Controller = 192.168.30.2
                                        Authenticated WLAN client = 192.168.30.107
                                        No. Time Source Destination Protocol Info
                .Cisco_42:d3:03 Spanning-tree-(for-bridges)_00 STP Conf 0.000000 1
                          Root = 32769/00:14:a9:76:d7:c0 Cost = 4 Port = 0x8003
                   (ESP ESP (SPI=0x7d117296 192.168.30.105 192.168.30.2 1.564706 2
                   (ESP ESP (SPI=0xbb243261 192.168.30.2 192.168.30.105 1.591426 3
                   (ESP ESP (SPI=0x7d117296 192.168.30.105 192.168.30.2 1.615600 4
                   (ESP ESP (SPI=0xbb243261 192.168.30.2 192.168.30.105 1.617243 5
                   (ESP ESP (SPI=0x7d117296 192.168.30.105 192.168.30.2 1.625168 6
                   (ESP ESP (SPI=0xbb243261 192.168.30.2 192.168.30.105 1.627006 7
                   (ESP ESP (SPI=0x7d117296 192.168.30.105 192.168.30.2 1.638414 8
```

```
(ESP ESP (SPI=0xbb243261 192.168.30.2 192.168.30.105 1.639673 9
(ESP ESP (SPI=0x7d117296 192.168.30.105 192.168.30.2 1.658440 10
(ESP ESP (SPI=0xbb243261 192.168.30.2 192.168.30.105 1.662462 11
(ESP ESP (SPI=0x7d117296 192.168.30.105 192.168.30.2 1.673782 12
(ESP ESP (SPI=0xbb243261 192.168.30.2 192.168.30.105 1.674631 13
(ESP ESP (SPI=0x7d117296 192.168.30.105 192.168.30.2 1.687892 14
(ESP ESP (SPI=0xbb243261 192.168.30.2 192.168.30.105 1.708082 15
;Broadcast LLC U, func=XID 192.168.30.107 1.743648 16
DSAP NULL LSAP Individual, SSAP NULL LSAP Command
.Cisco_42:d3:03 Spanning-tree-(for-bridges)_00 STP Conf 2.000073 17
Root = 32769/00:14:a9:76:d7:c0 Cost = 4 Port = 0x8003
.Cisco_42:d3:03 Spanning-tree-(for-bridges)_00 STP Conf 4.000266 18
Root = 32769/00:14:a9:76:d7:c0 Cost = 4 Port = 0x8003
Cisco_42:d3:03 Cisco_42:d3:03 LOOP Reply 5.062531 19
<NBNS Name query NB PRINT.CISCO.COM<00 192.168.30.255 192.168.30.101 5.192104 20
<NBNS Name query NB PRINT.CISCO.COM<00 192.168.30.255 192.168.30.101 5.942171 21
.Cisco_42:d3:03 Spanning-tree-(for-bridges)_00 STP Conf 6.000242 22
Root = 32769/00:14:a9:76:d7:c0 Cost = 4 Port = 0x8003
ARP Who has 192.168.30.105? Tell 192.168.30.2 192.168.30.105 192.168.30.2 6.562944 23
ARP 192.168.30.105 is at 00:40:63:e3:19:c9 192.168.30.2 192.168.30.105 6.562982 24
Broadcast ARP 192.168.30.107 is at 00:13:ce:67:ae:d2 192.168.30.107 6.596937 25
```

## معلومات ذات صلة

- دليل تكوين وحدة تحكم شبكة LAN اللاسلكية من Cisco، الإصدار 5.2
- 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).