WLC 用および Microsoft Windows 2003 IAS サーバ用に RADIUS IPSec セキュリティを設定する

目次

概要

このガイド 文書 WCS およびこれらの WLAN コントローラがサポートする RADIUS IPSec 機能を設定する方法を:

- 4400 シリーズ
- WiSM
- 3750G

コントローラ RADIUS IPSec 機能は**セキュリティ > AAA > RADIUS認証サーバ** セクションの下のコントローラ GUI にあります。 機能はあなたが IPSec のコントローラと RADIUSサーバ（IAS）間のすべての RADIUS 通信を暗号化することができるように方式を提供します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- LWAPP のナレッジ
- RADIUS認証および IPSec のナレッジ
- Windows 2003 サーバ オペレーティング システムのサービスを設定する方法の知識

使用するコンポーネント

これらのネットワークおよびソフトウェアコンポーネントはインストールされ、コントローラ RADIUS IPSec 機能を展開するために設定する必要があります:

- WLC 4400、WiSM、または 3750G コントローラ。 この例はソフトウェア バージョン 5.2.178.0 を実行する WLC 4400 を使用します
- Lightweight アクセスポイント（LAP）。 この例は 1231 シリーズ LAP を使用します。
- DHCP と切り替えて下さい
- Microsoft Certificate Authority と Microsoft Internet Authentication Service（IAS）とインストールされるドメインコントローラとして構成されたサーバー Microsoft 2003。
- Microsoft ドメイン セキュリティ
- WPA2/ PEAP で ADU バージョン 3.6 が設定されている Cisco 802.11 a/b/g ワイヤレスクライアントアダプタ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

IPSec RADIUSコンフィギュレーション

このコンフィギュレーション ガイドは Microsoft WinServer のインストールか設定を、認証局（CA）、アクティブ ディレクトリか WLAN 802.1X クライアント説明しません。 これらのコンポーネントはコントローラ IPSec RADIUS 機能の配備前にインストールされ、設定する必要があります。 このの残り ガイド 文書これらのコンポーネントの IPSec RADIUS を設定する方法を:

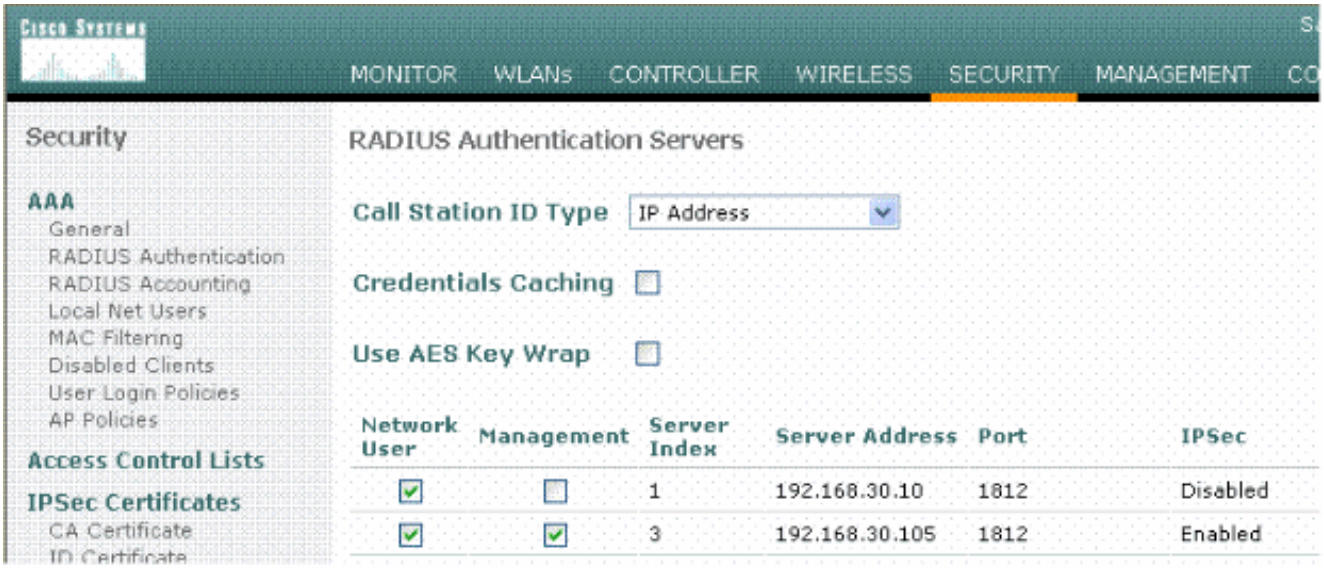
1. Cisco WLAN コントローラ
2. Windows 2003 IAS
3. Microsoft Windows ドメイン セキュリティ設定

WLC の設定

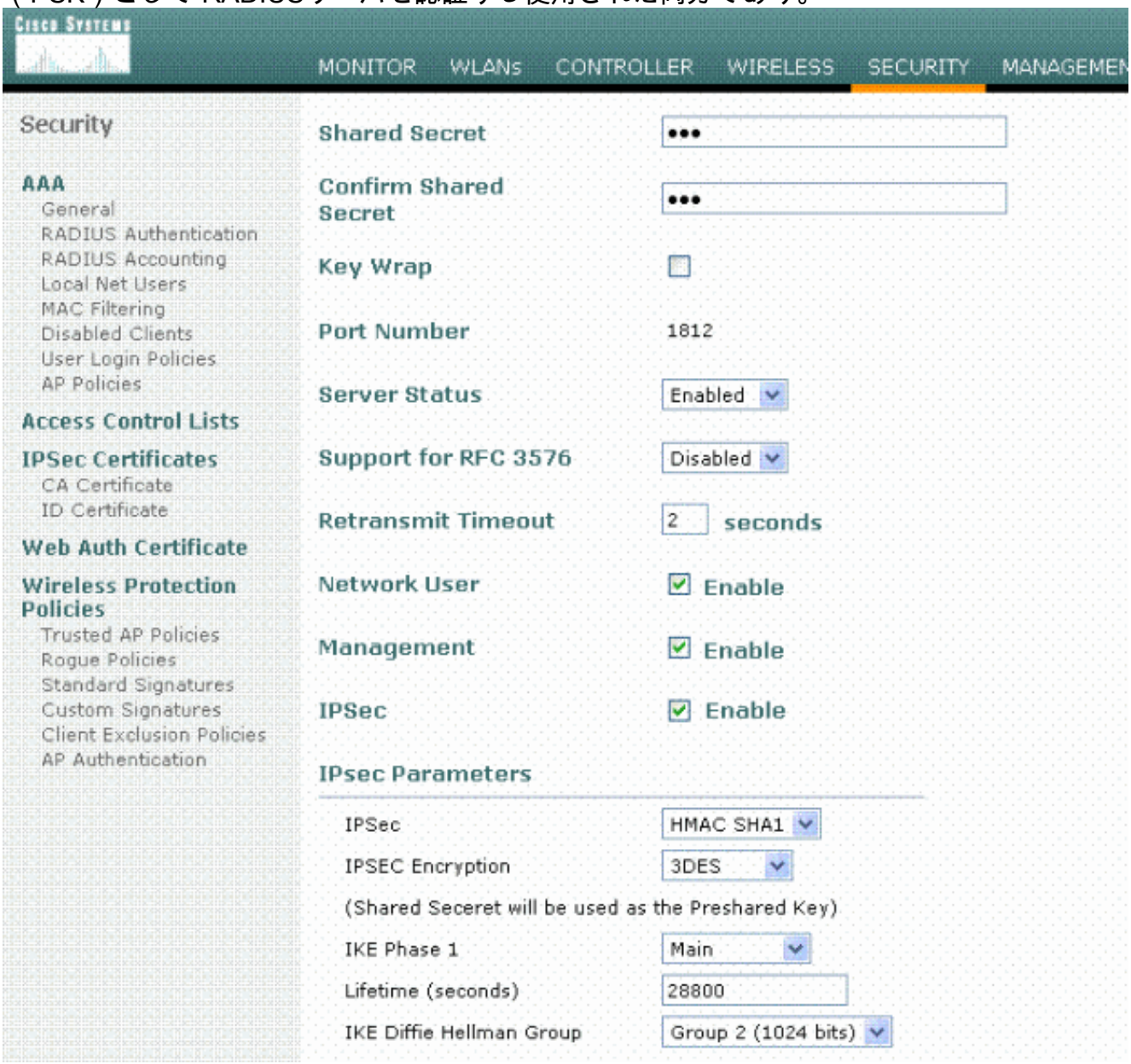
このセクションは GUI によって WLC の IPSec を設定する方法を説明します。

コントローラ GUI から、これらのステップを完了して下さい。

1. コントローラ GUI の**セキュリティ > AAA > Radius Authentication タブ**にナビゲート し、新しい RADIUSサーバを追加して下さい。



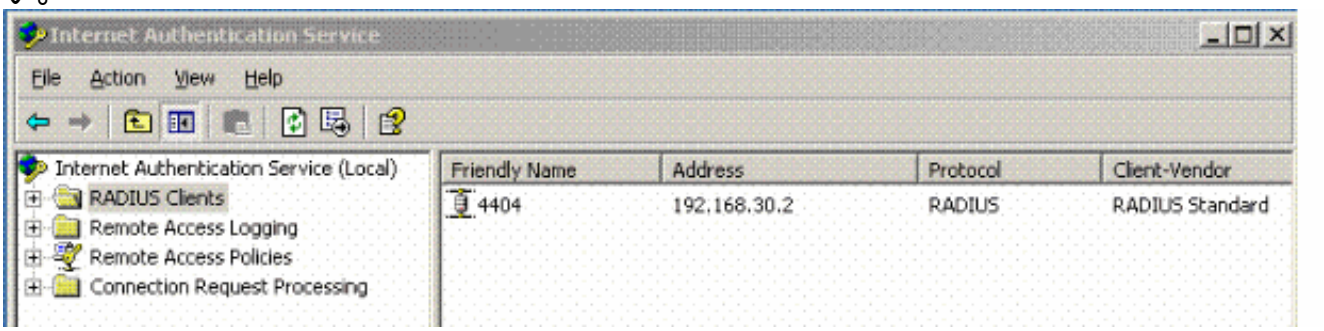
2. IP アドレス、ポート 1812、および新しい RADIUSサーバの共有秘密を設定して下さい。**IPSec Enable チェックボックスを**チェックし、これらの IPSecパラメータを設定し、それから『Apply』 をクリック して下さい。**注:** 共有秘密は IPSec 認証のための事前共有キー（PSK）として RADIUSサーバを認証する使用された両方であり。



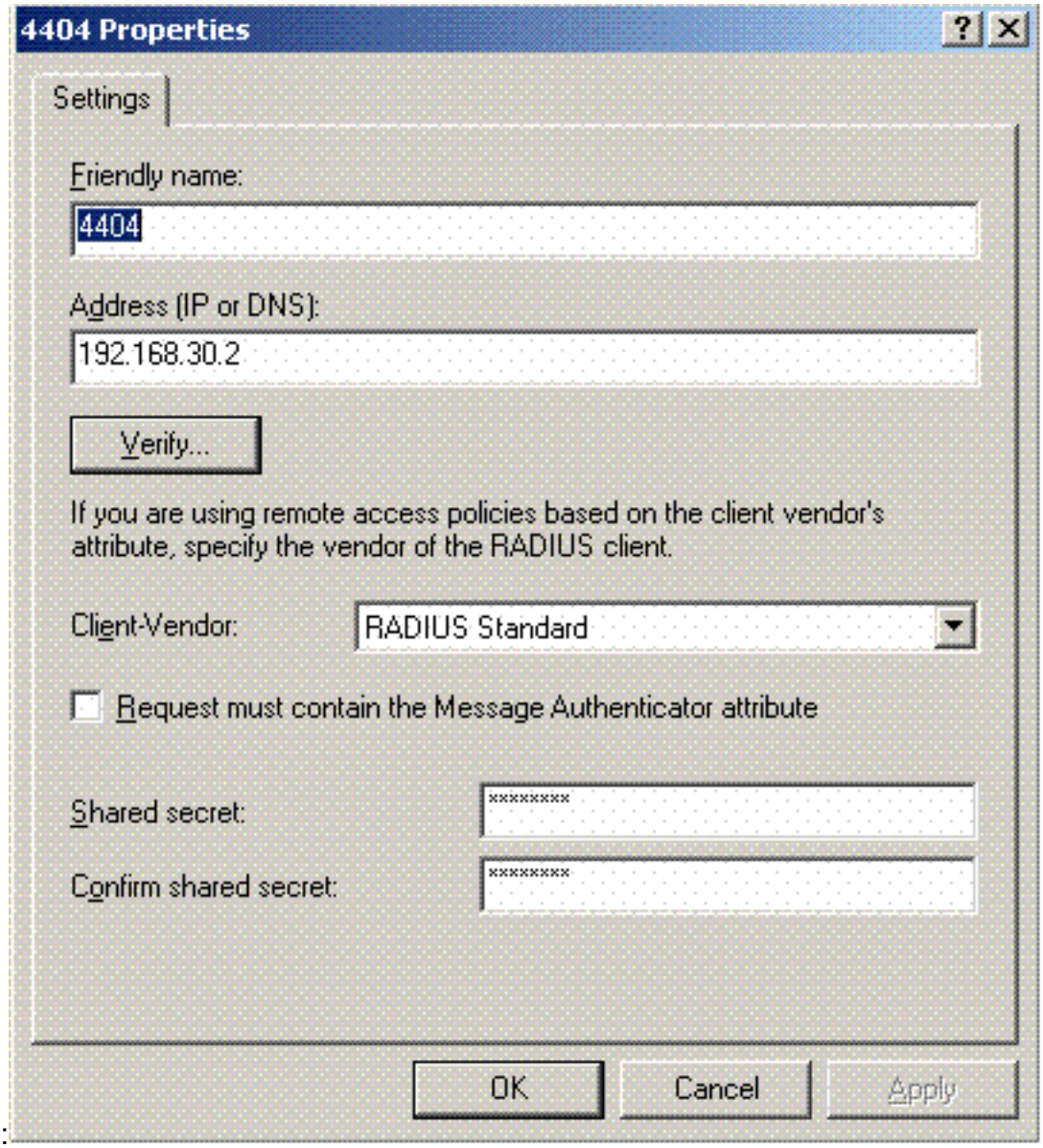
IAS を設定して下さい

IAS のこれらのステップを完了して下さい:

1. Win2003 の IAS マネージャにナビゲート し、新しい RADIUSクライアントを追加して下さい。



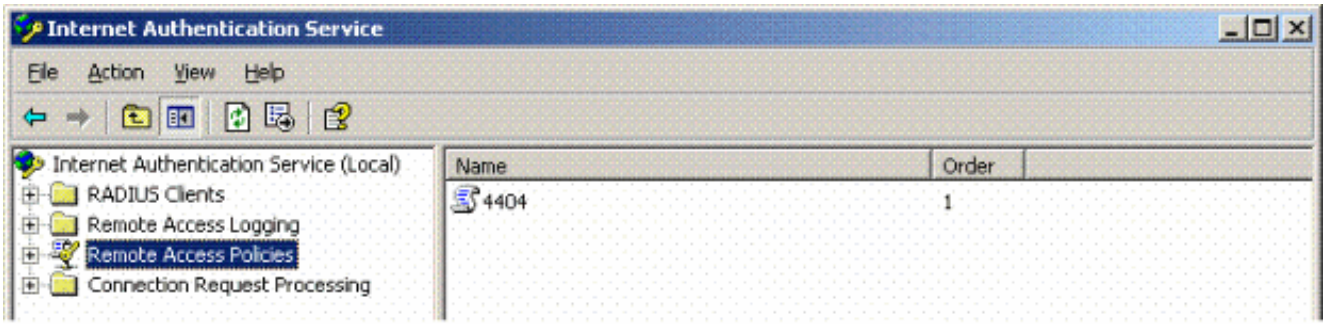
2. コントローラで設定される IP アドレスおよび共有秘密で RADIUSクライアント プロパティを設定して下さい



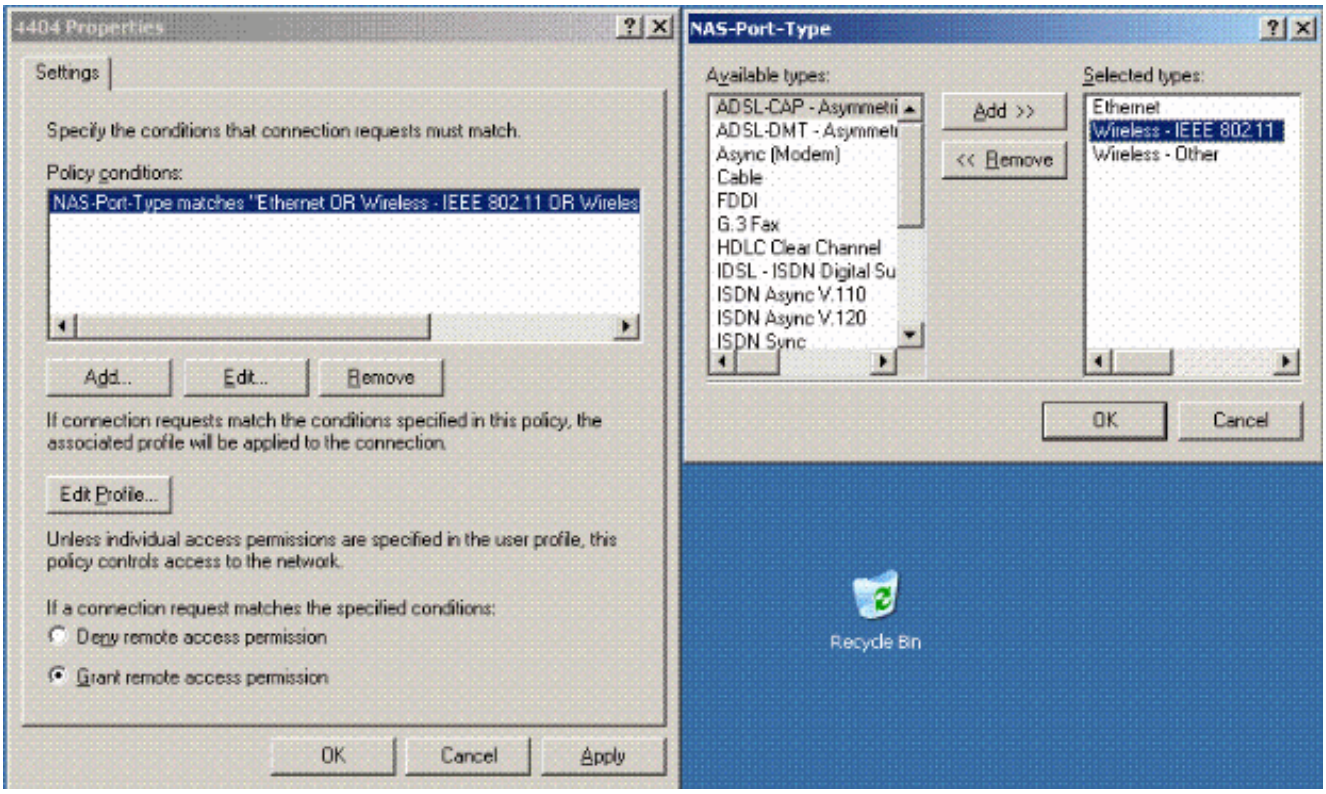
:

3. コントローラ用の新しいリモートアクセスポリシーを設定して下さい

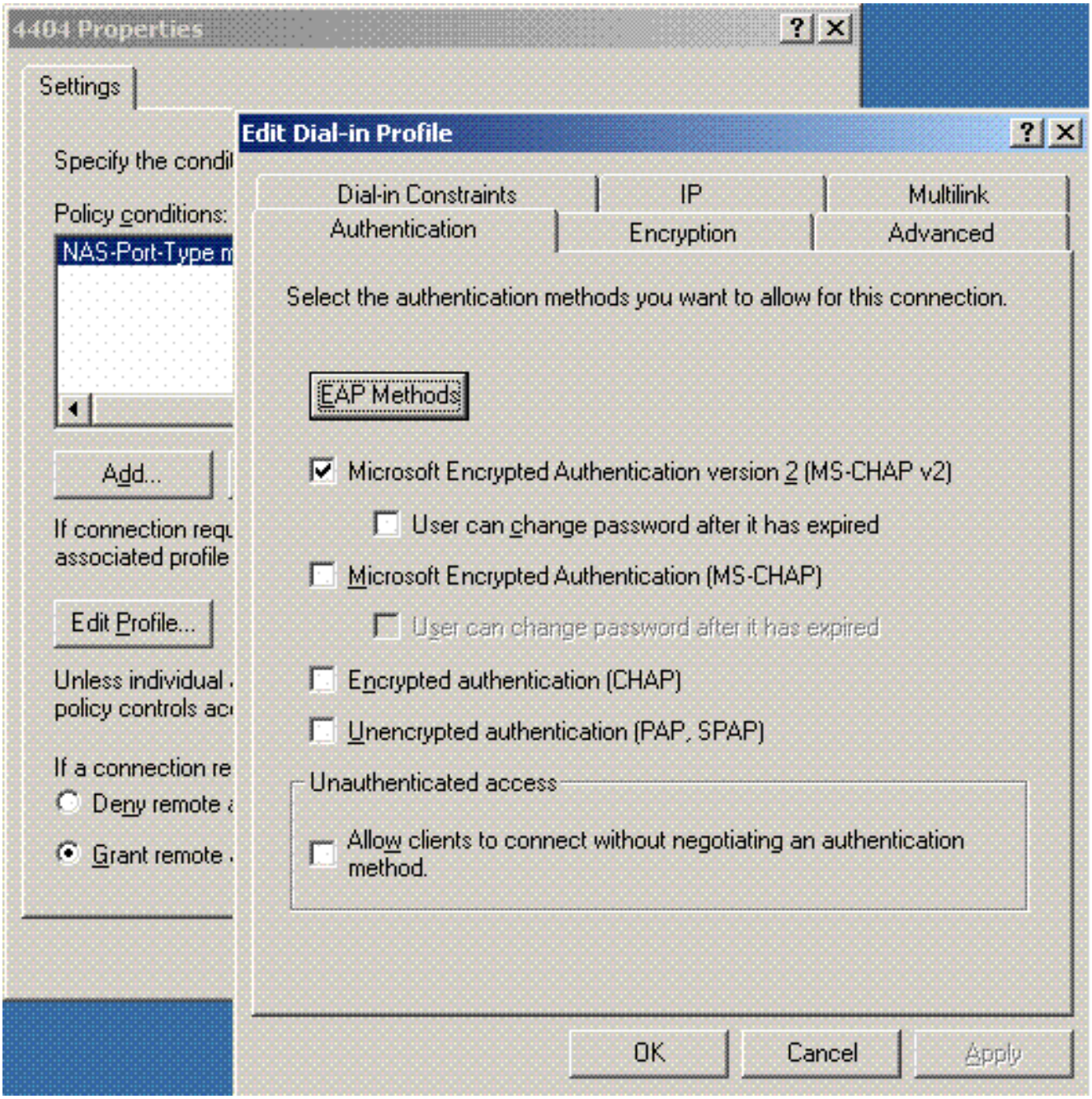
:



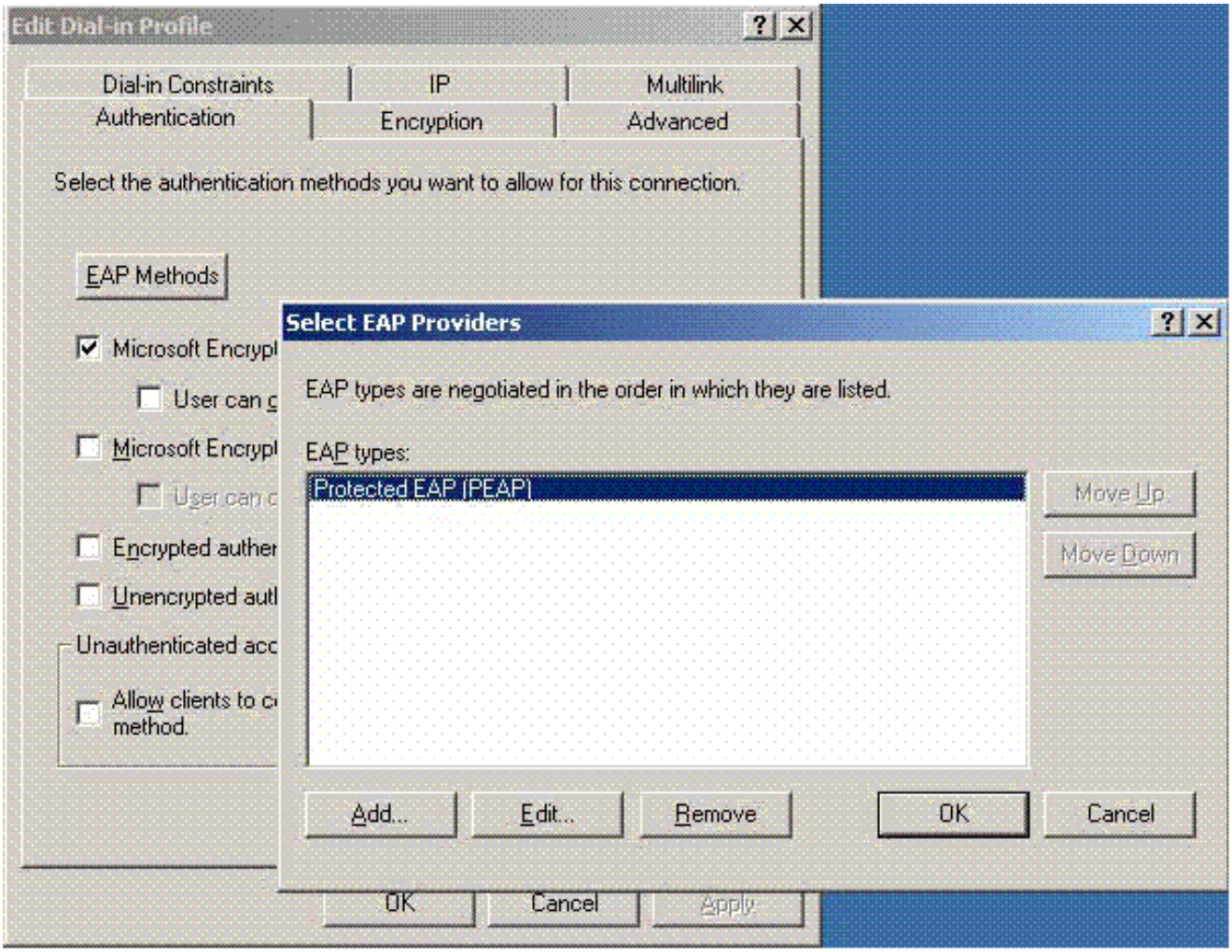
4. コントローラ リモートアクセスポリシーのプロパティを編集して下さい。 Nas-port 型追加することを確かめて下さい-ワイヤレス– IEEE 802.11:



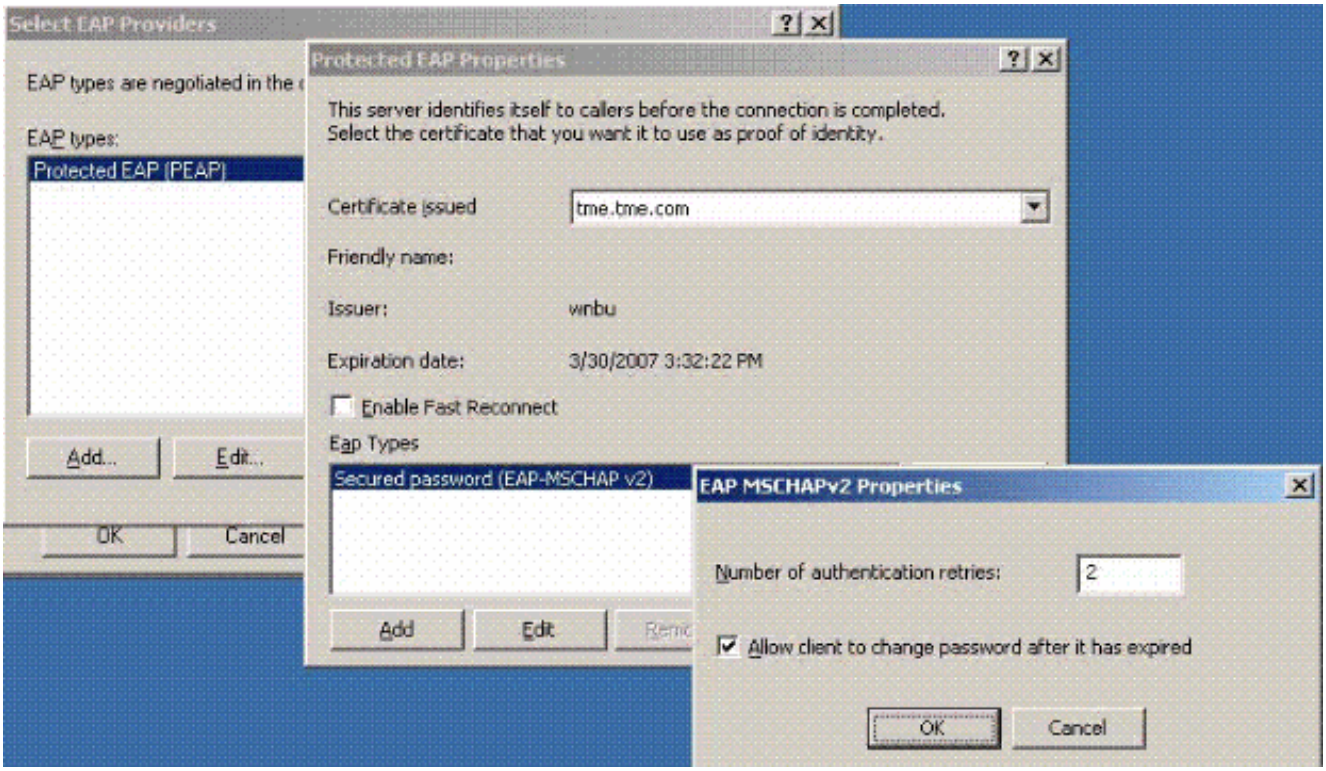
5. 『Edit Profile』 をクリック し、**Authentication タブを**クリックし、認証があるように MS-CHAP v2 を確認して下さい
:



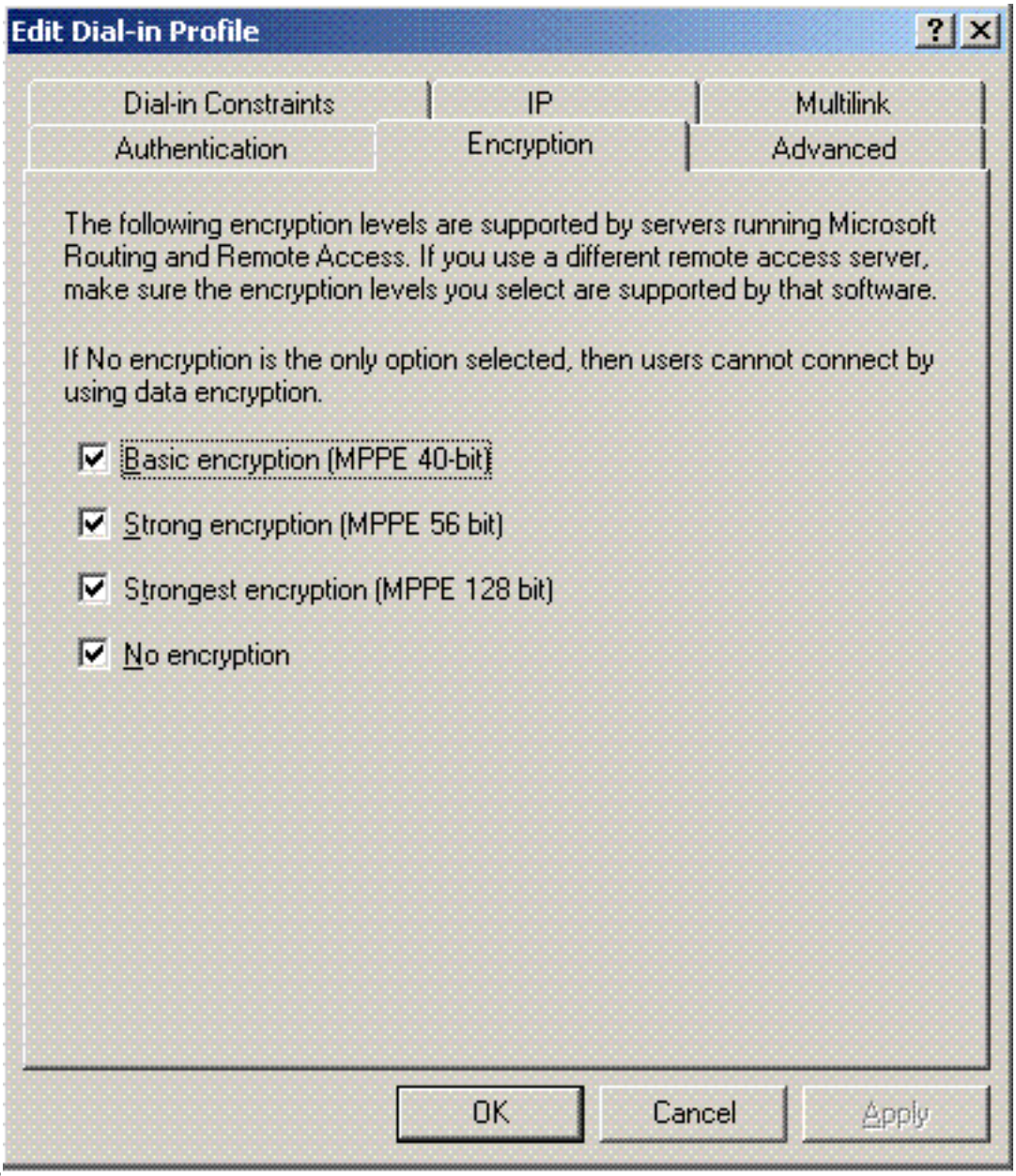
6. **メソッドを**『eap』 をクリック し、プロバイダを『eap』 を選択 し、EAP 型として PEAP を追加して下さい
:



7. select EAP プロバイダで『Edit』 をクリック し、サーバがアクティブ ディレクトリ ユーザ アカウントおよび CA （ 例えば tme.tme.com ）と関連付けた Pull Down メニューから選択して下さい。 EAP 型 MSCHAP v2 を追加して下さい
:

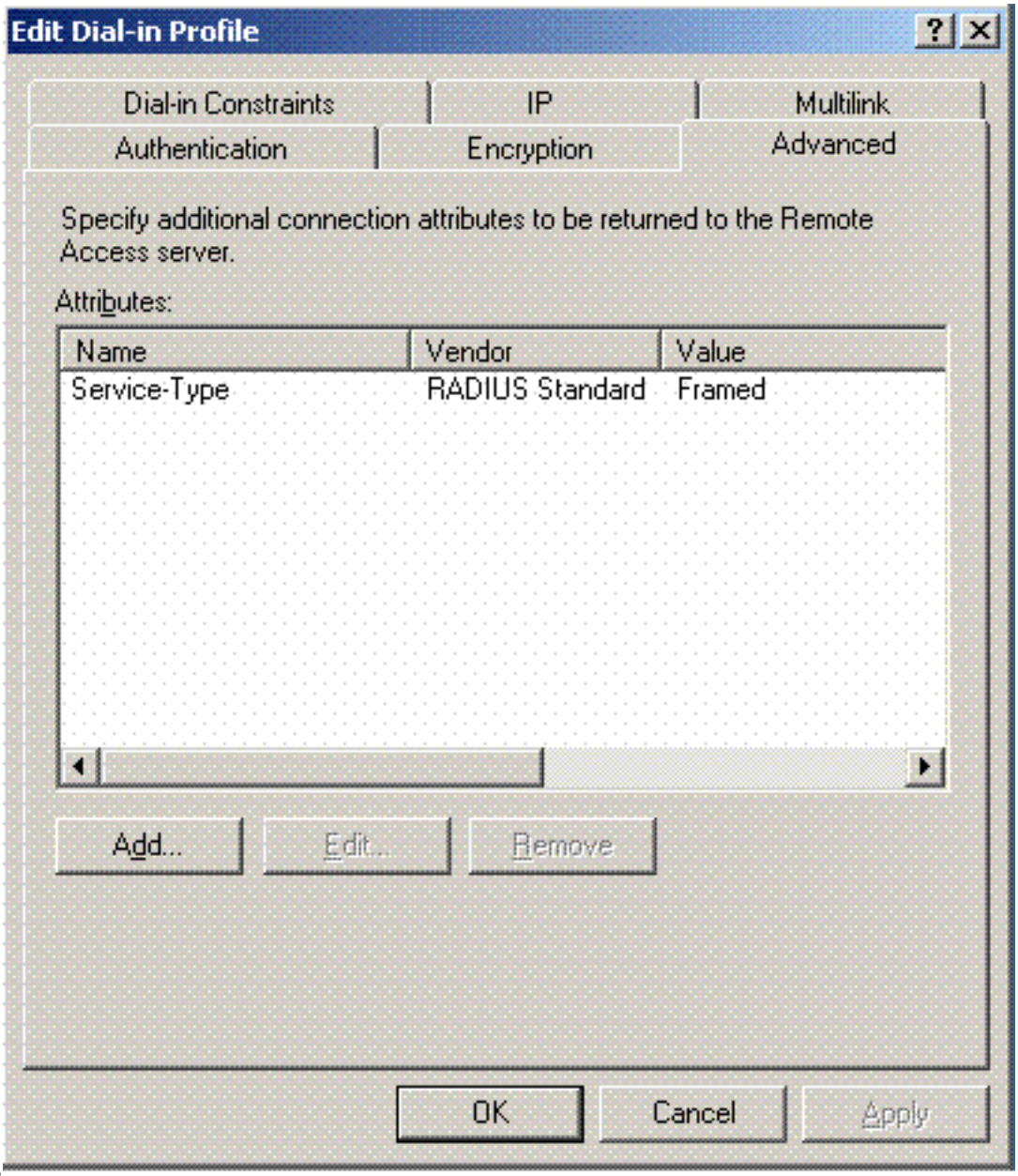


8. **Encryption タブを**クリックし、リモートアクセスがあるようにすべての暗号化タイプを確認



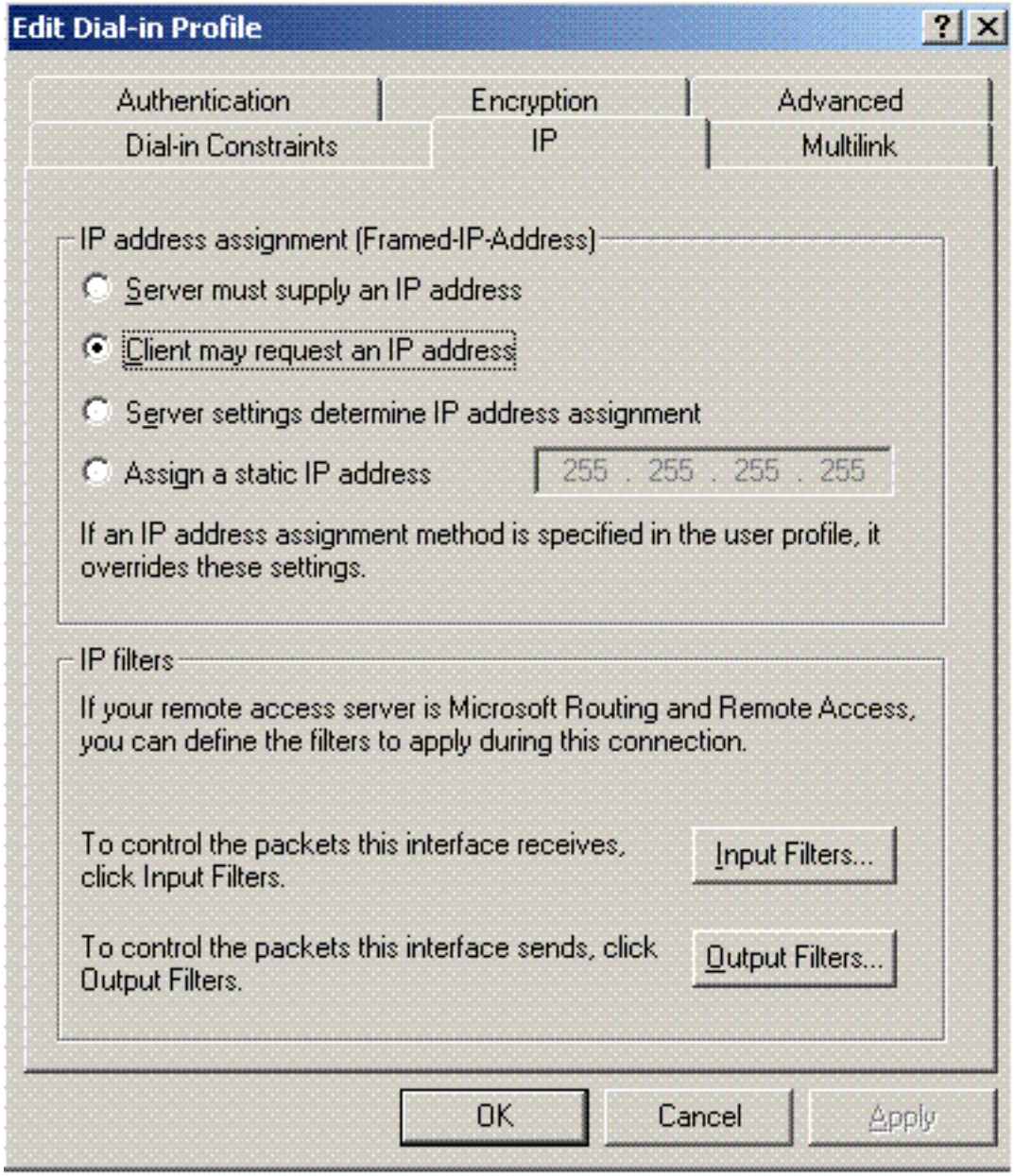
して下さい:

9. **Advanced タブを**クリックし、RADIUS標準を/サービス タイプとしてフレーム化されて追加



して下さい:

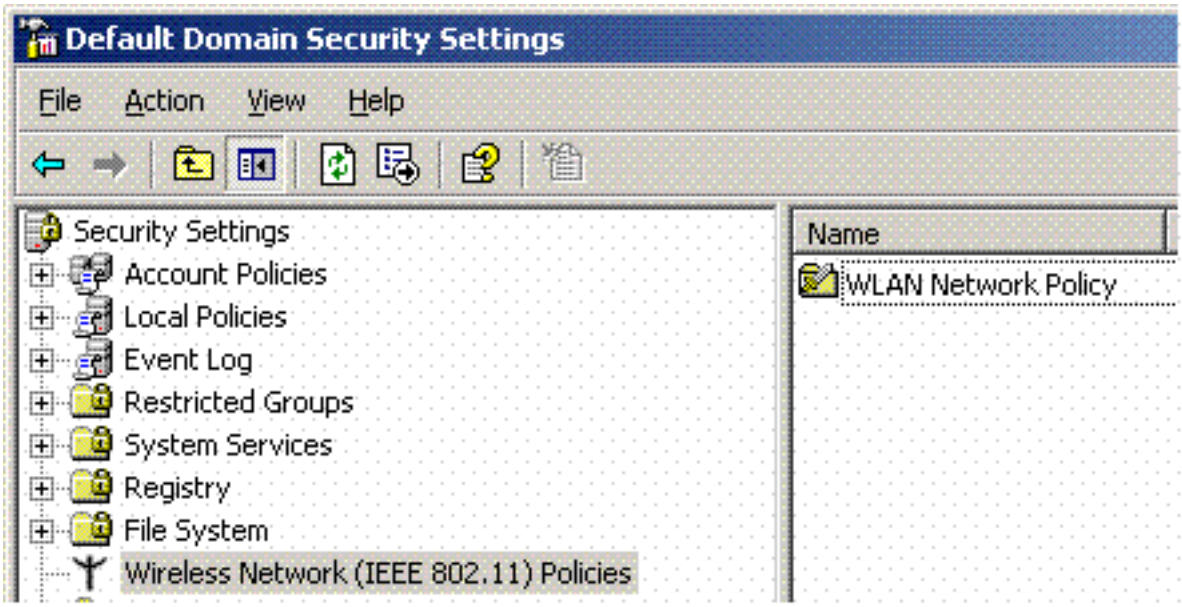
10. **IP** タブをクリックすれば、チェック **クライアントは IP アドレスを要求するかもしれません。** これはスイッチか WinServer で有効に なる DHCP があることを仮定します。



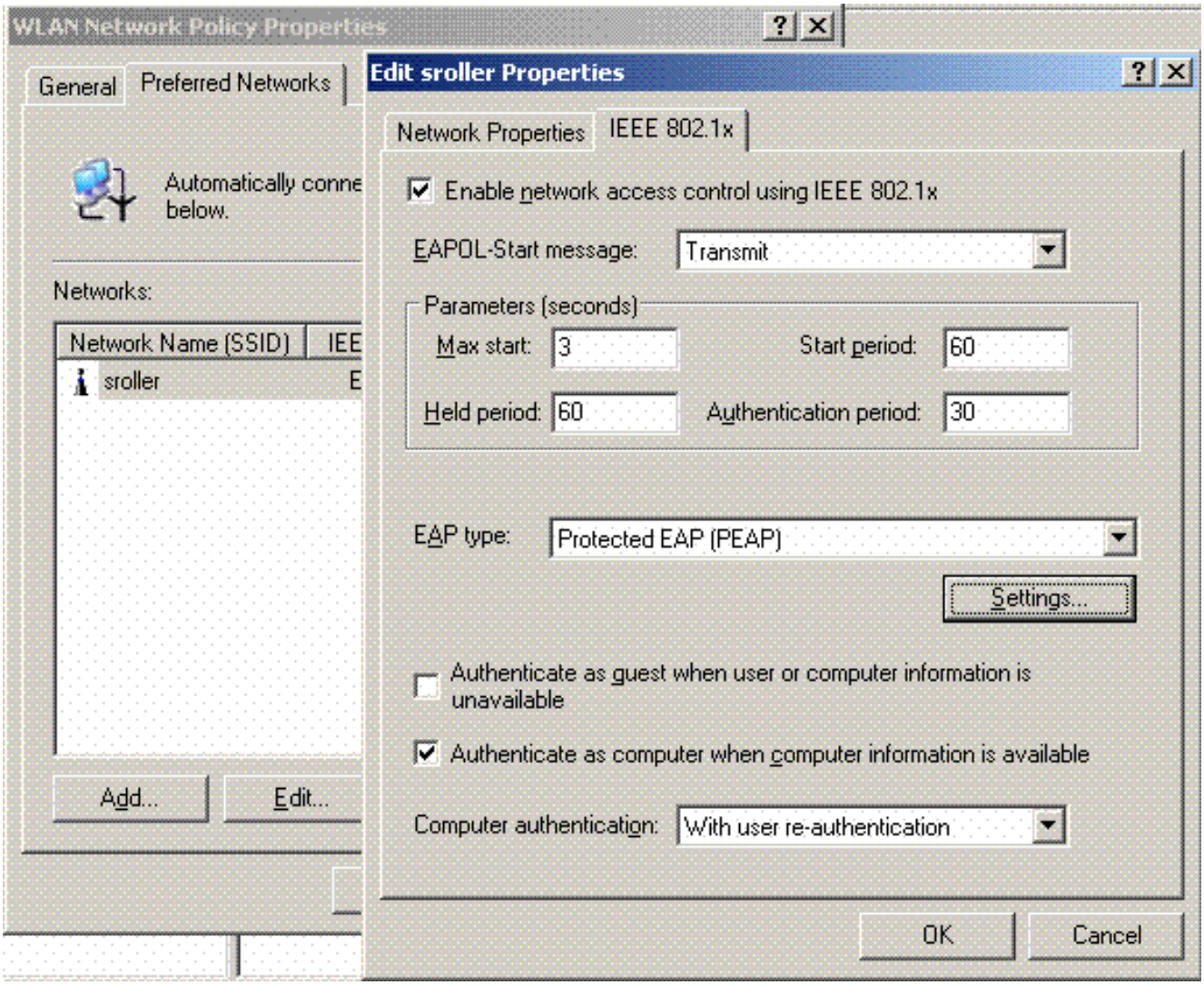
Microsoft Windows 2003 のドメイン セキュリティ設定

Windows 2003 ドメイン セキュリティ設定を行うためにこれらのステップを完了して下さい:

1. デフォルト ドメイン セキュリティ設定マネージャを起動させ、無線ネットワーク (IEEE 802.11) ポリシーのための新しいセキュリティポリシーを作成して下さい。

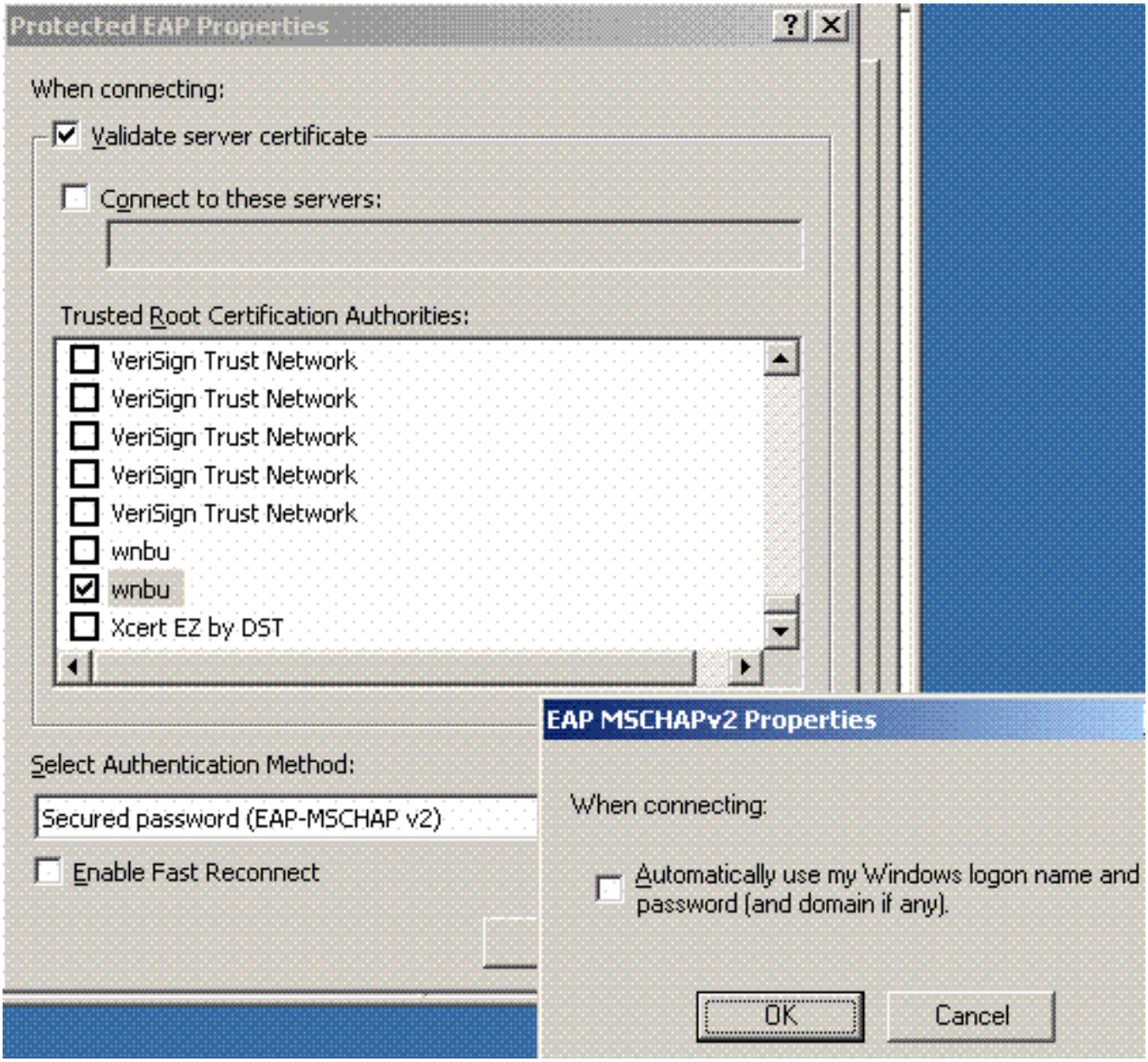


2. 開いた WLANネットワーク ポリシーのプロパティは、**優先 する ネットワークを**クリックし。 新しい優先 する WLAN を追加し、のような WLAN SSID の名前を、入力して下さい。 その新しい優先 する ネットワークをダブル クリックし、**IEEE 802.1x** タブをクリックして下さい。 EAP 型として『PEAP』 を選択 して下さい
:

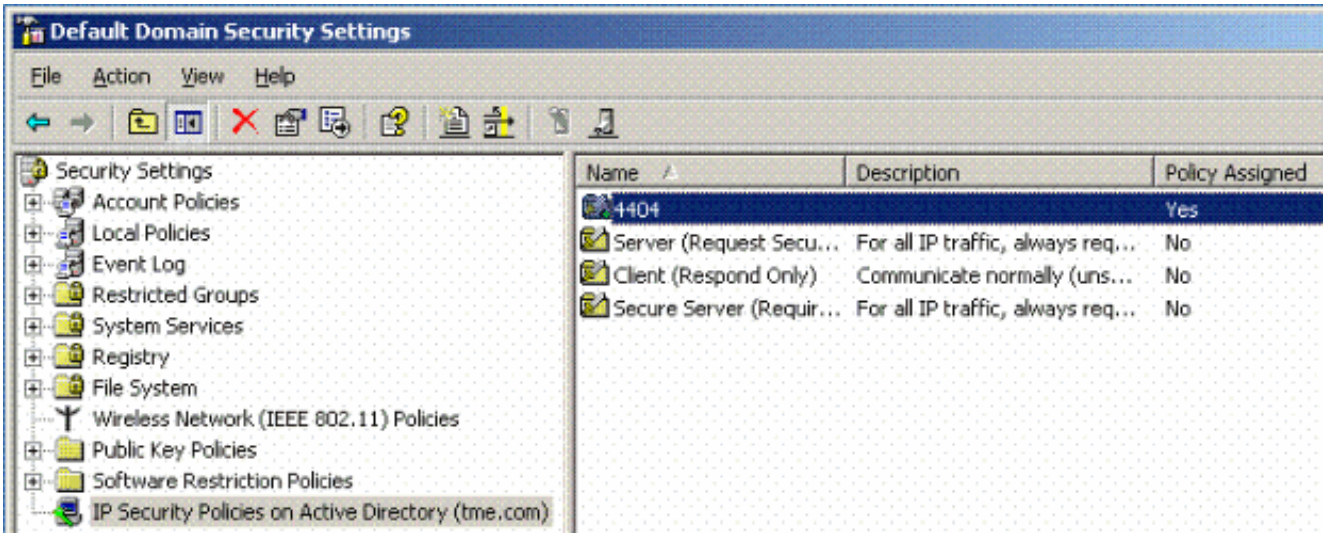


3. **設定を**『PEAP』 をクリック して下さい、チェックは認証局（CA）インストールされる**サーバ証明を検証し**、信頼されたルート証明書を選択します。 テストの目的で、自動的にのための MS CHAP v2 ボックスの使用します Windows ログオンおよびパスワードをチェック

を外して下さい。

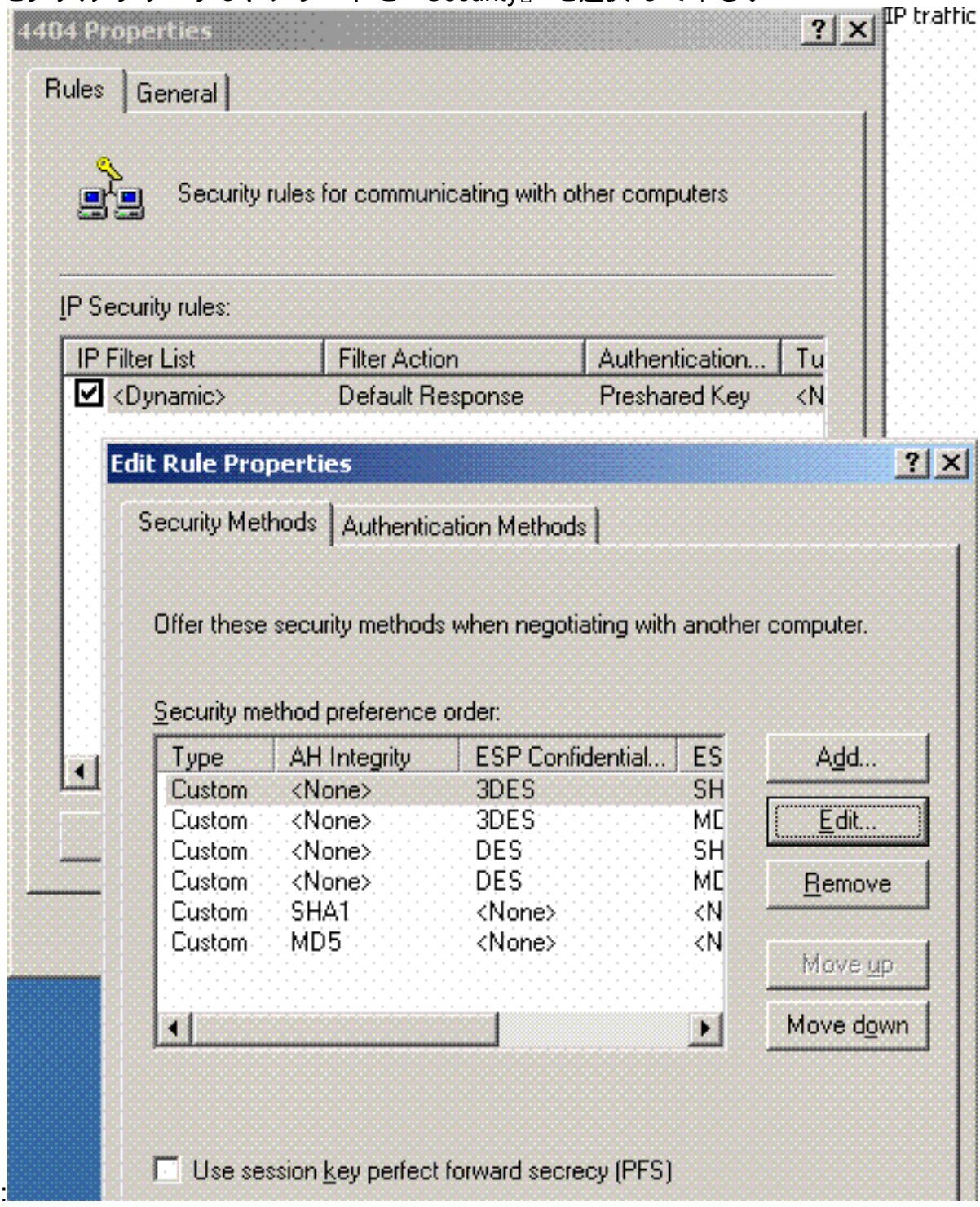


4. Windows 2003 デフォルト ドメイン セキュリティ設定 マネージャウィンドウで、**4404** のようなアクティブ ディレクトリ ポリシーの別の新しい IPセキュリティ ポリシーを、作成して下さい。



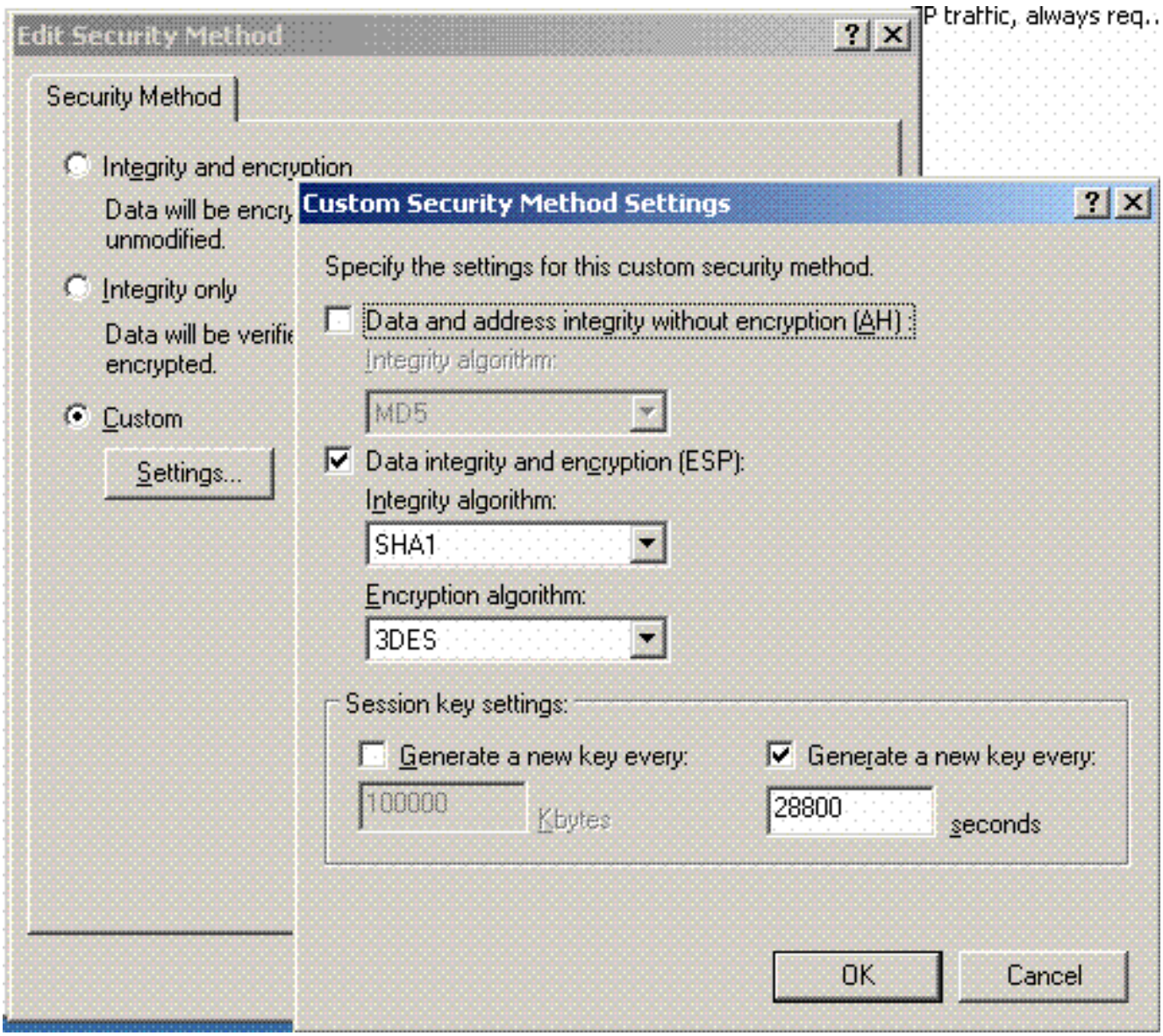
5. 新しい 4404 のポリシー特性を編集し、**Rules タブを**クリックして下さい。 追加して下さい新しいフィルタ規則- IP はリストを肉付けします (ダイナミック) ; フィルタ アクション

（デフォルト応答）; 認証（PSK）; トンネル（どれも）。 新しく作成されたフィルタ規則をダブル クリックし、メソッドを『Security』 を選択 して下さい

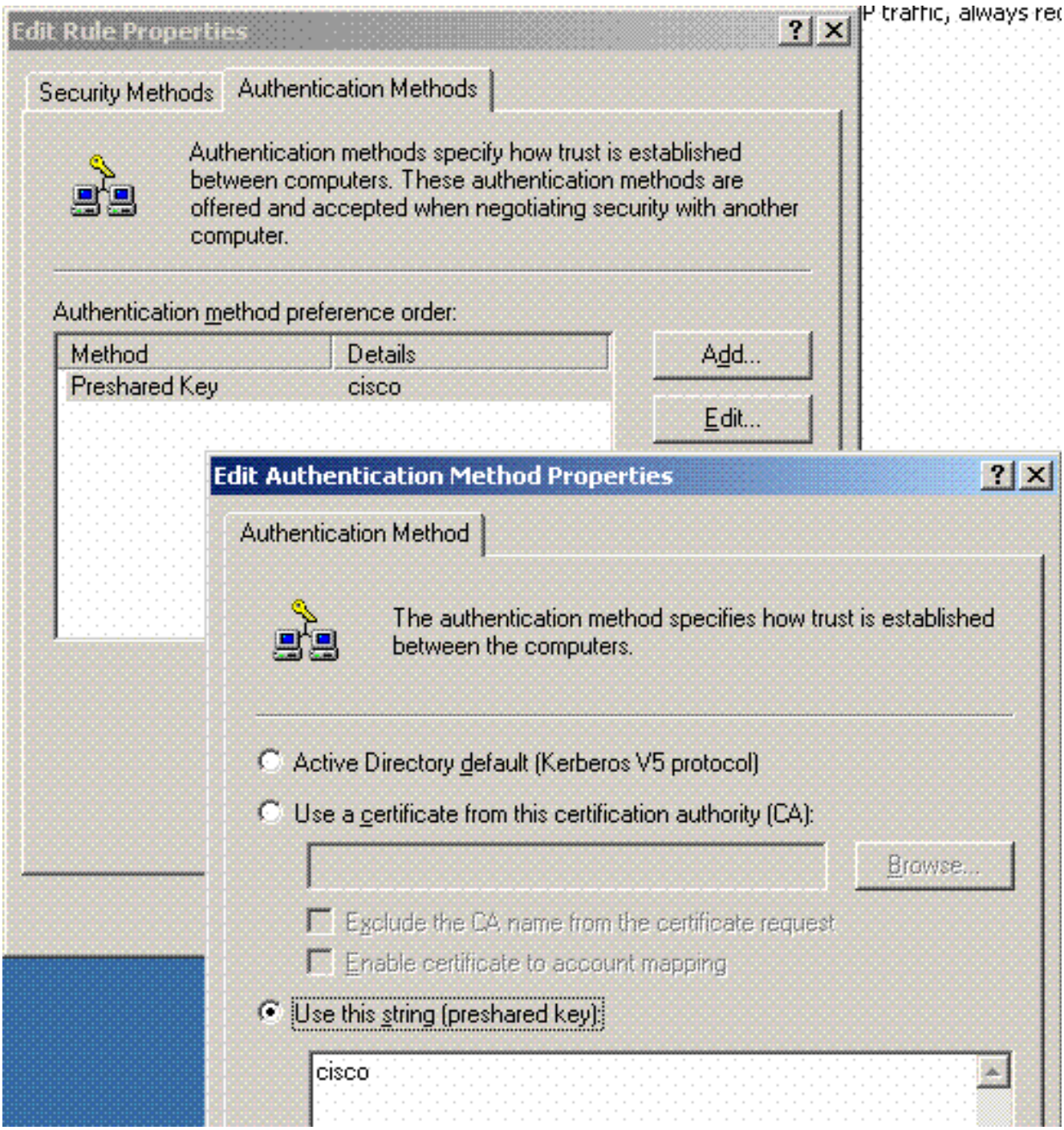


:

6. **セキュリティ 方式を**『Edit』 をクリック し、**カスタム 設定** オプション ボタンをクリック して下さい。 これらの設定を選択して下さい。**注:** これらの設定はコントローラ RADIUS IPsec セキュリティ設定を一致する必要があります。



7. 編集ルール Properties の下で**認証方式**タブをクリックして下さい。 コントローラ RADIUSコンフィギュレーションで以前に入力した同じ共有秘密を入力して下さい。



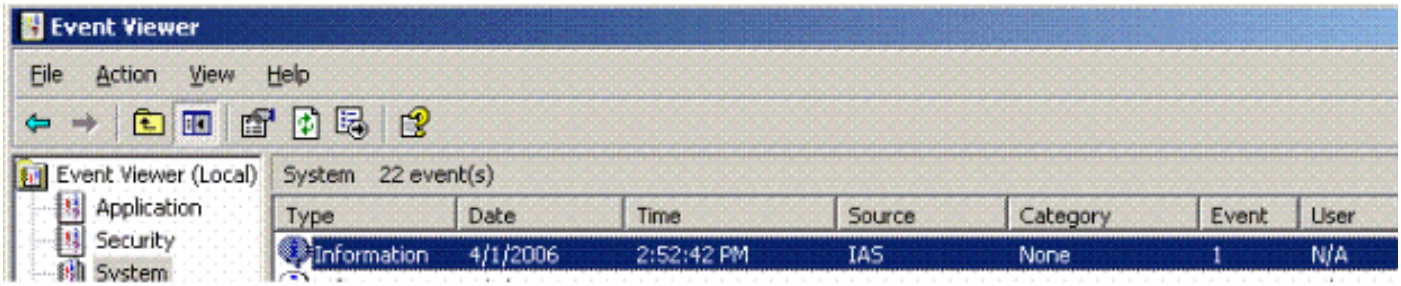
この時点で、コントローラ用のすべてのコンフィギュレーション、IAS およびドメイン セキュリティ設定は完了します。 すべてのコンフィギュレーションをコントローラおよび WinServer 両方で保存し、すべてのマシンをリブートして下さい。 テストのために使用する WLANクライアントで、ルート証明書をインストールし、WPA2/PEAP のために設定して下さい。 ルート証明書がクライアントでインストールされていた後、クライアントマシンをリブートして下さい。 結局マシンは WLAN にリブートし、クライアントを接続し、これらのログ イベントをキャプチャ します。

注: クライアント接続がコントローラと WinServer RADIUS 間の IPSec接続を設定するために必要となります。

Windows 2003 システムログ イベント

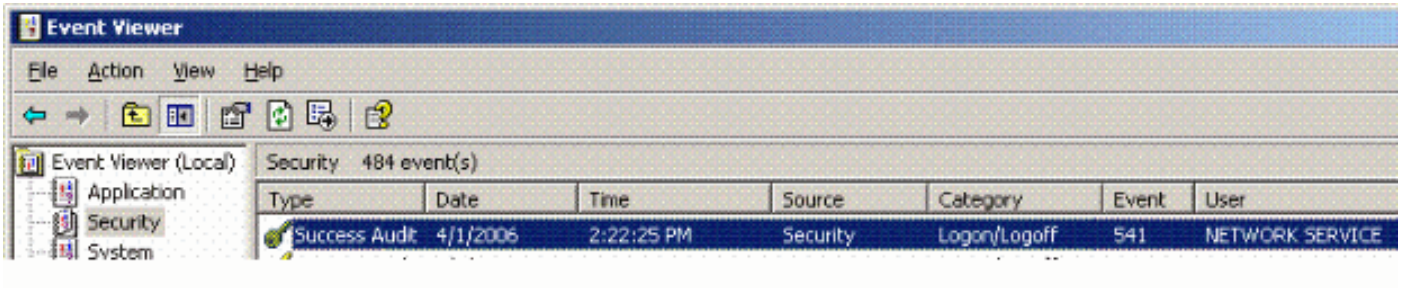
WPA2/PEAP のために設定される有効に なる IPSec WinServer で RADIUS の正常な WLANクライアント接続はこのシステムイベントを生成します:

192.168.30.105 = WinServer
192.168.30.2 = WLAN Controller



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)

正常なコントローラ <> RADIUS IPSec接続は WinServer ログでこのセキュリティイベントを生成します:



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
```

ワイヤレス LAN コントローラ RADIUS IPSec 成功デバッグ例

この設定を確認するためにコントローラの debug コマンド **デバッグ pm ikemsg イネーブル**を使用できます。 次に例を示します。

```
(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
```

Ethreal キャプチャ

サンプル Ethreal キャプチャはここにあります。

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

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

関連情報

- Cisco ワイヤレス LAN コントローラ コンフィギュレーション ガイド、リリース 5.2
- テクニカルサポートとドキュメント - Cisco Systems