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

内容

概要

このガイドでは、WCSおよび次のWLANコントローラでサポートされるRADIUS IPSec機能を設定する方法について説明します。

- 4400 シリーズ
- WISM
- 3750 G

コントローラのRADIUS IPSec機能は、コントローラのGUIの[Security] > [AAA] > [RADIUS Authentication Servers] セクションにあります。この機能を使用すると、コントローラとRADIUSサーバ(IAS)間のすべてのRADIUS通信をIPSecで暗号化できます。

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に関する知識
- RADIUS認証とIPSecに関する知識
- Windows 2003 Serverオペレーティングシステムでのサービスの設定方法に関する知識

使用するコンポーネント

コントローラのRADIUS IPSec機能を導入するには、次のネットワークコンポーネントとソフトウェアコンポーネントをインストールして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では、ソフトウェアバージョン5.2.178.0が稼働するWLC 4400を使用しています
- Lightweightアクセスポイント(LAP)。この例では、1231シリーズのLAPを使用しています。
- DHCPを使用したスイッチ
- Microsoft Certificate Authority（CA；認証局）およびMicrosoft Internet Authentication Service（IAS；インターネット認証サービス）とともにインストールされるドメインコントローラとして設定されたMicrosoft 2003サーバ。
- Microsoftドメインセキュリティ
- ADUバージョン3.6がWPA2/PEAPで設定された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ました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実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の設定

この設定ガイドでは、Microsoft WinServer、認証局、Active Directory、またはWLAN 802.1xクライアントのインストールや設定については説明していません。これらのコンポーネントは、コントローラIPSec RADIUS機能を導入する前にインストールして設定する必要があります。このガイドの残りの部分では、次のコンポーネントでIPSec RADIUSを設定する方法について説明します。

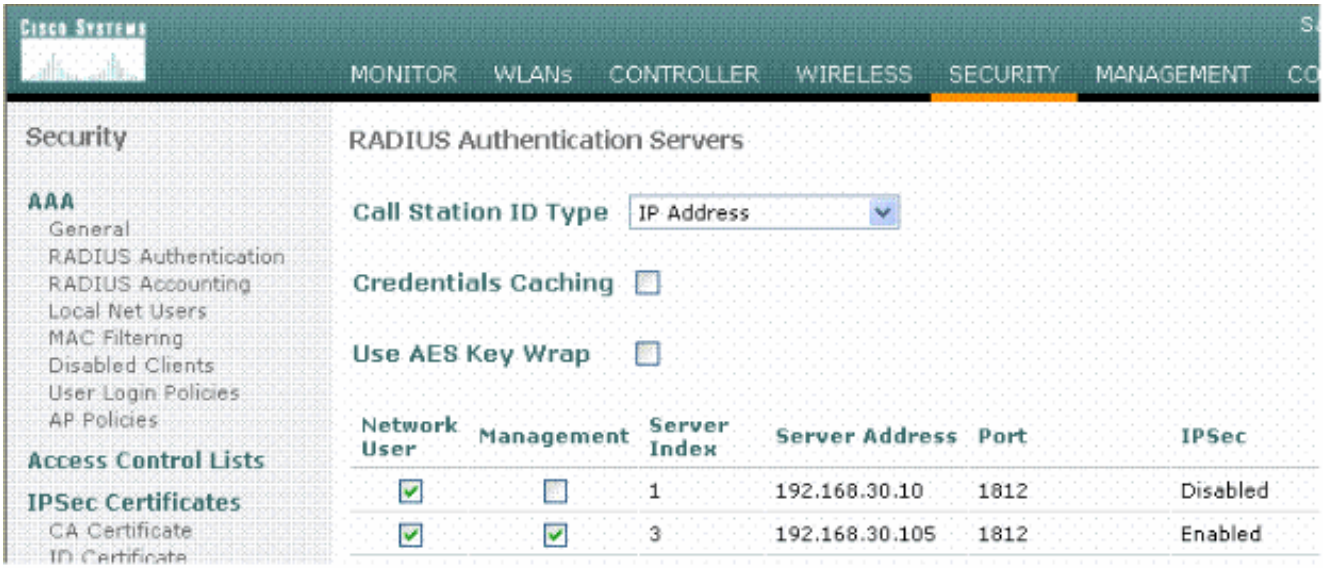
1. Cisco WLAN コントローラ
2. Windows 2003 IAS
3. Microsoft Windowsドメインのセキュリティ設定

WLC の設定

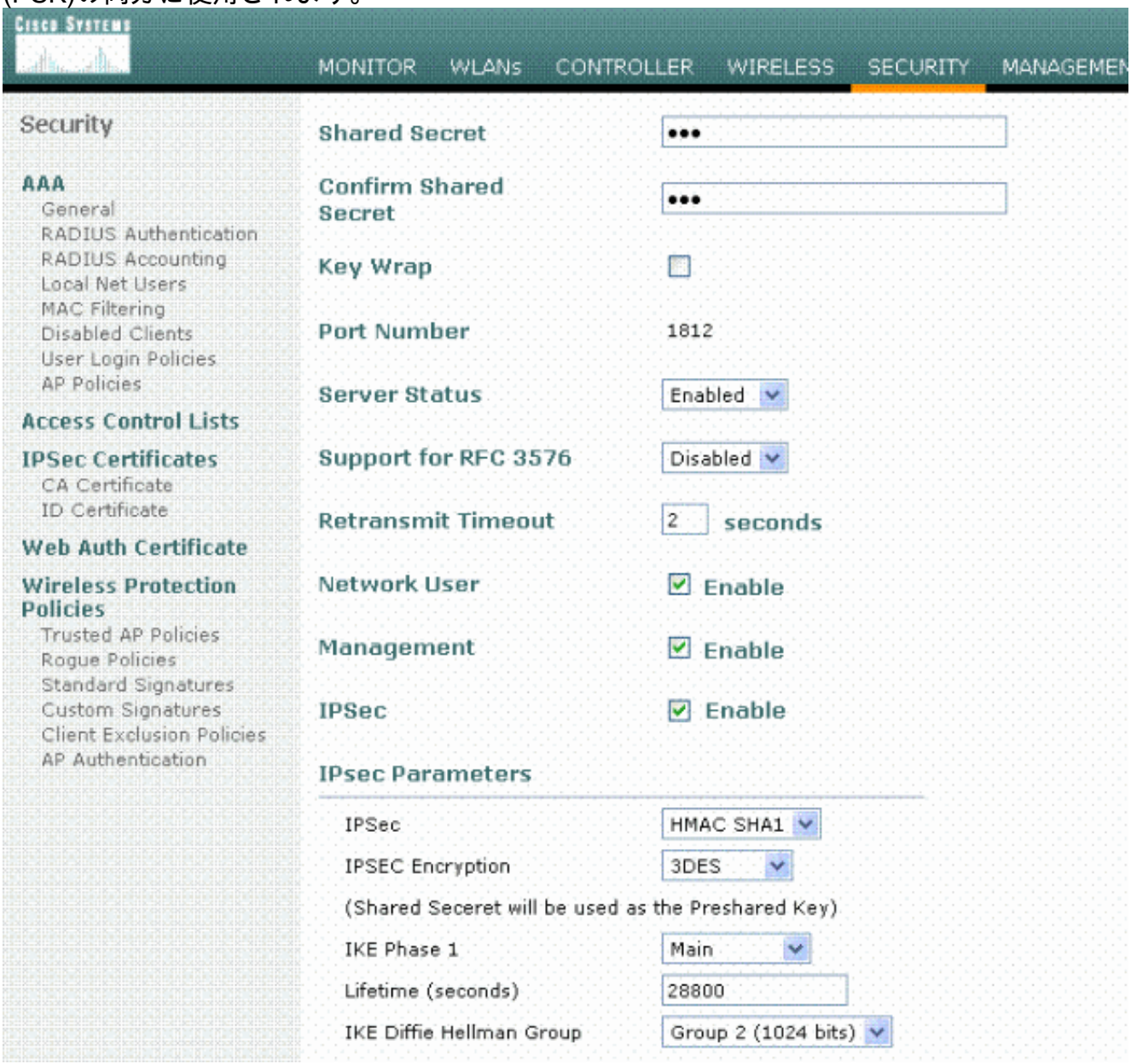
このセクションでは、GUIを使用してWLCでIPSecを設定する方法について説明します。

コントローラのGUIから、次の手順を実行します。

1. コントローラGUIで[Security] > [AAA] > [RADIUS Authentication] タブに移動し、新しいRADIUSサーバを追加します。



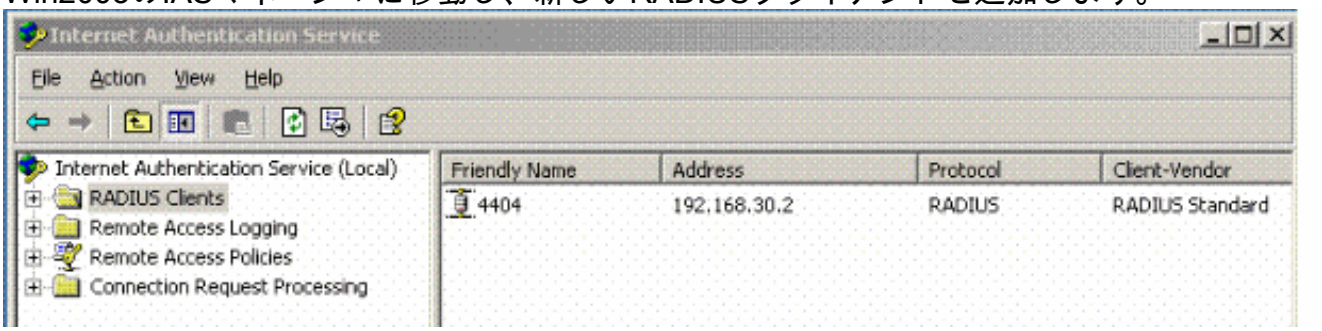
2. 新しいRADIUSサーバのIPアドレス、ポート1812、および共有秘密を設定します。[IPSec Enable] チェックボックスをオンにして、これらのIPSecパラメータを設定し、[Apply] をクリックします。**注：**共有秘密は、RADIUSサーバの認証と、IPSec認証用の事前共有キー(PSK)の両方に使用されます。



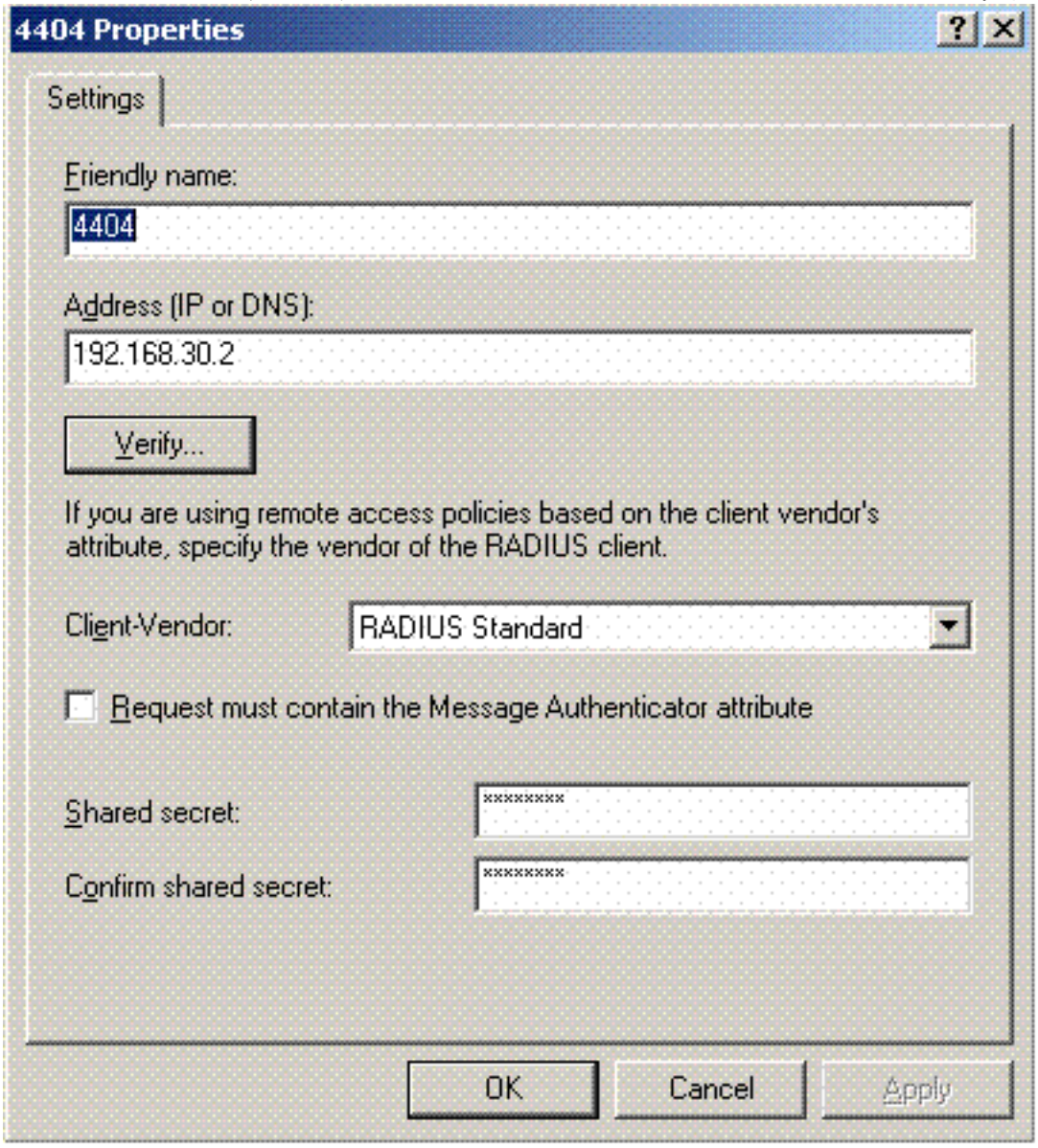
IASの設定

IASで次の手順を実行します。

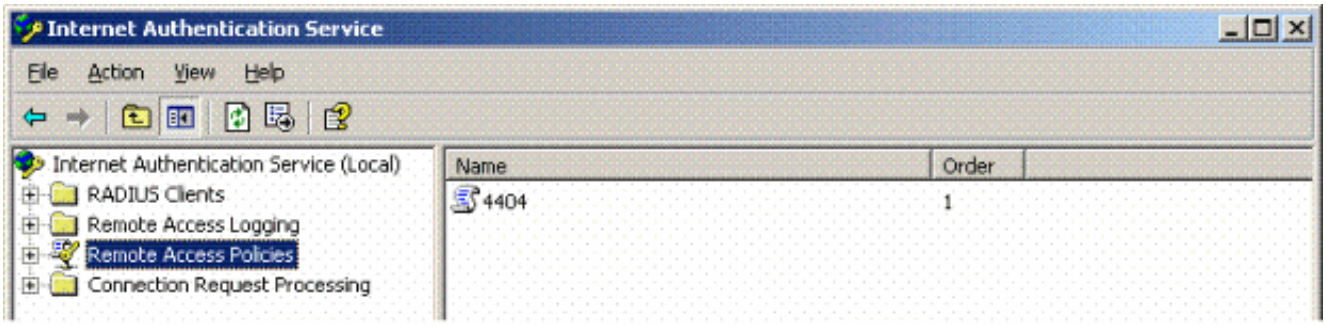
1. Win2003のIASマネージャに移動し、新しいRADIUSクライアントを追加します。



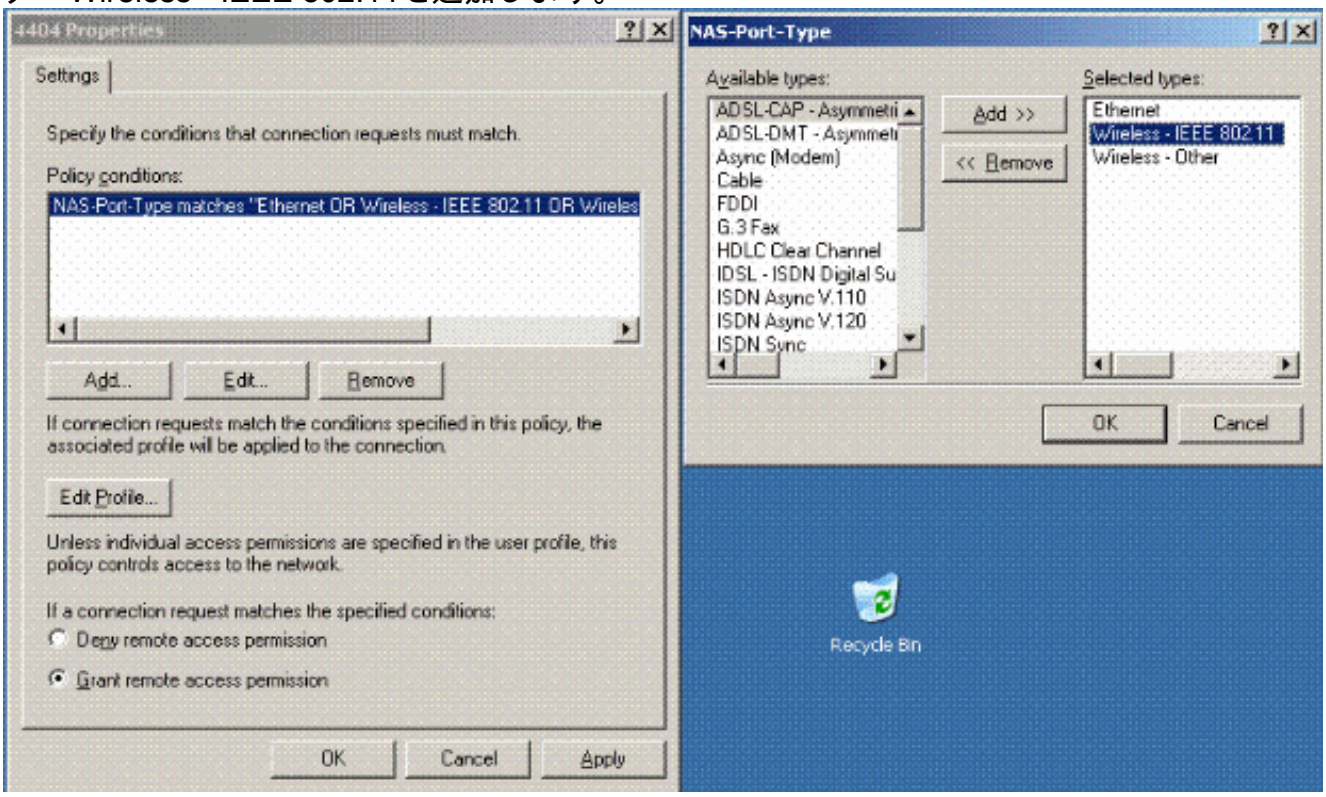
2. RADIUSクライアントのプロパティに、コントローラで設定されたIPアドレスと共有秘密を設定します。



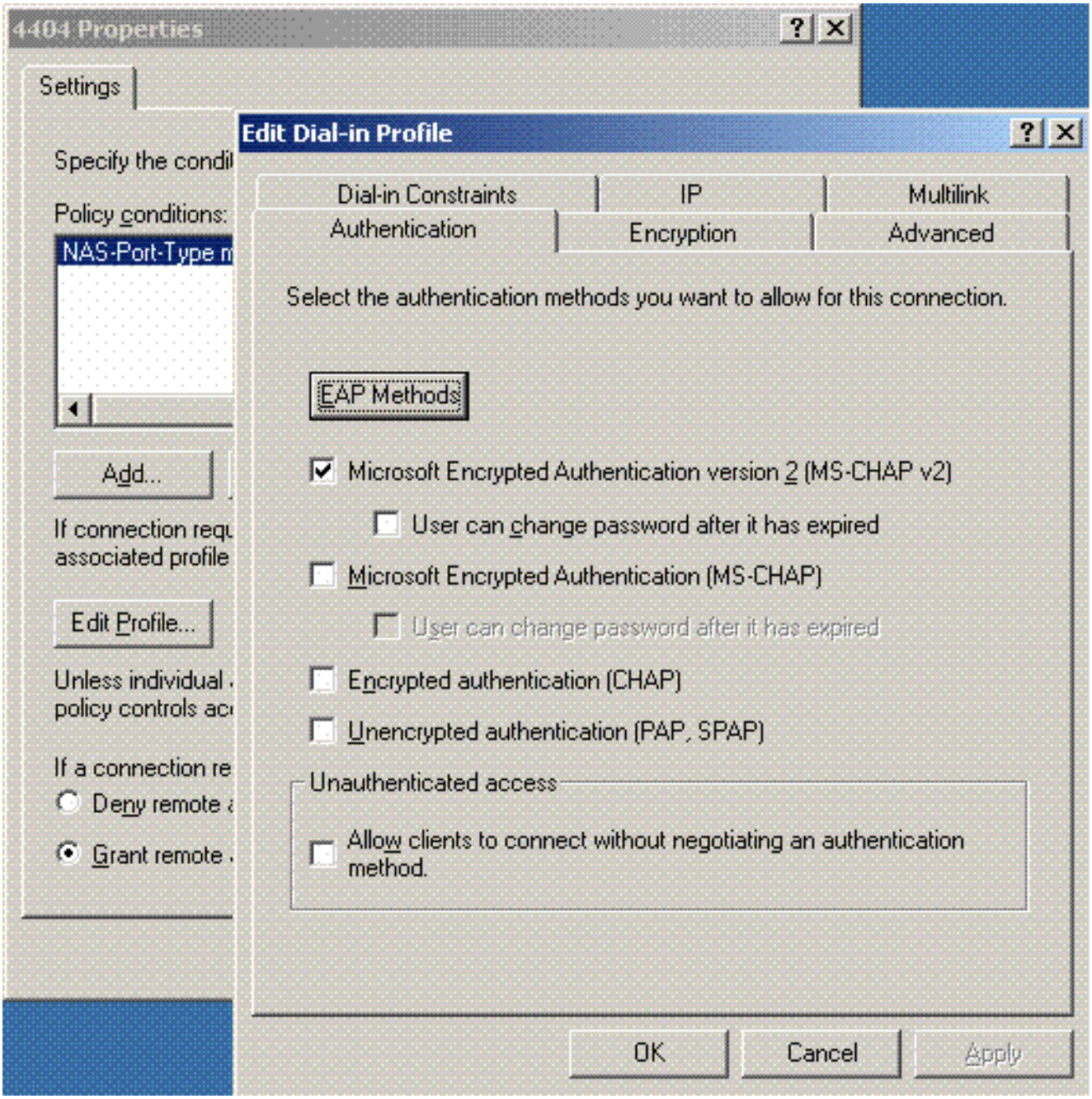
3. コントローラの新しいリモートアクセスポリシーを設定します。



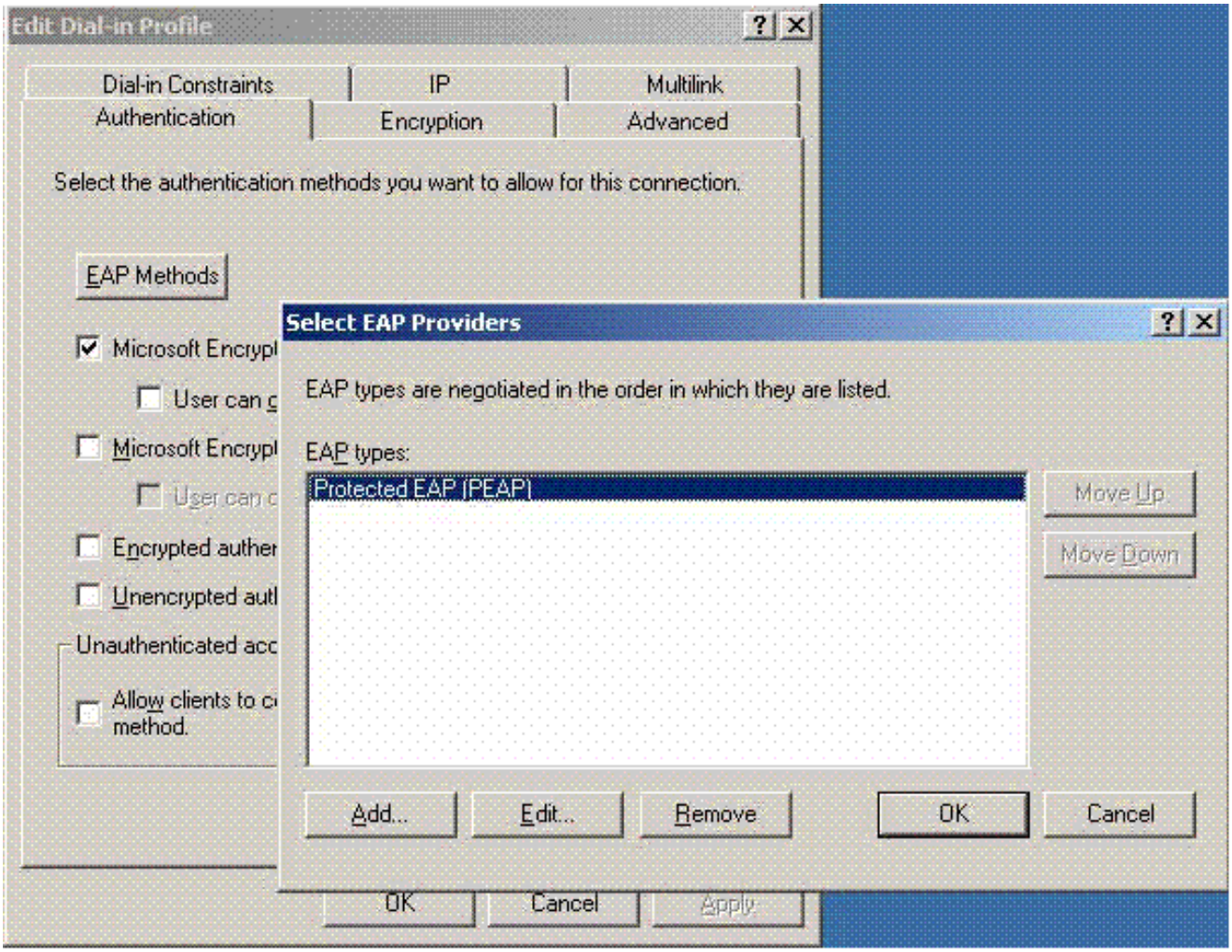
4. コントローラのリモートアクセスポリシーのプロパティを編集します。必ずNASポートタイプ – Wireless - IEEE 802.11を追加します。



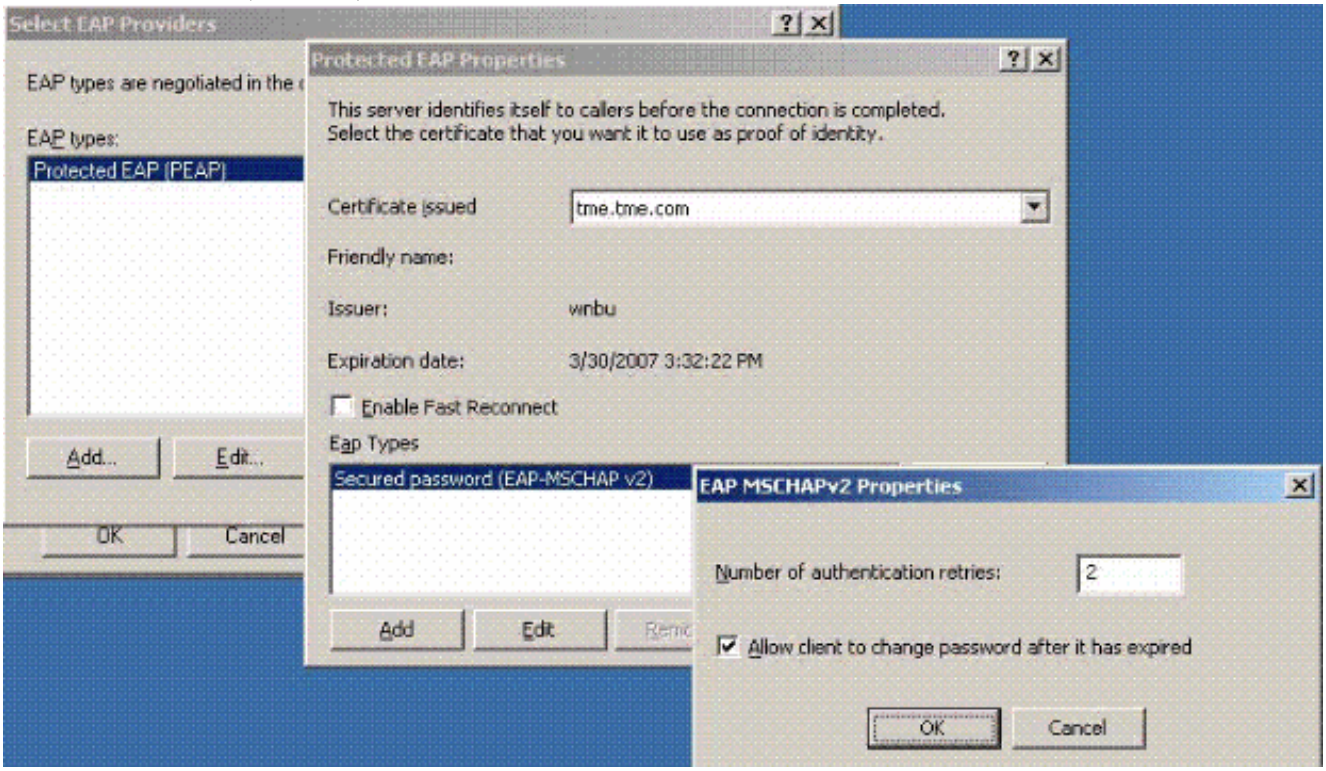
5. [Edit Profile] をクリックし、[Authentication] タブをクリックして、[MS-CHAP v2 for Authentication]にチェックマークを付けます。



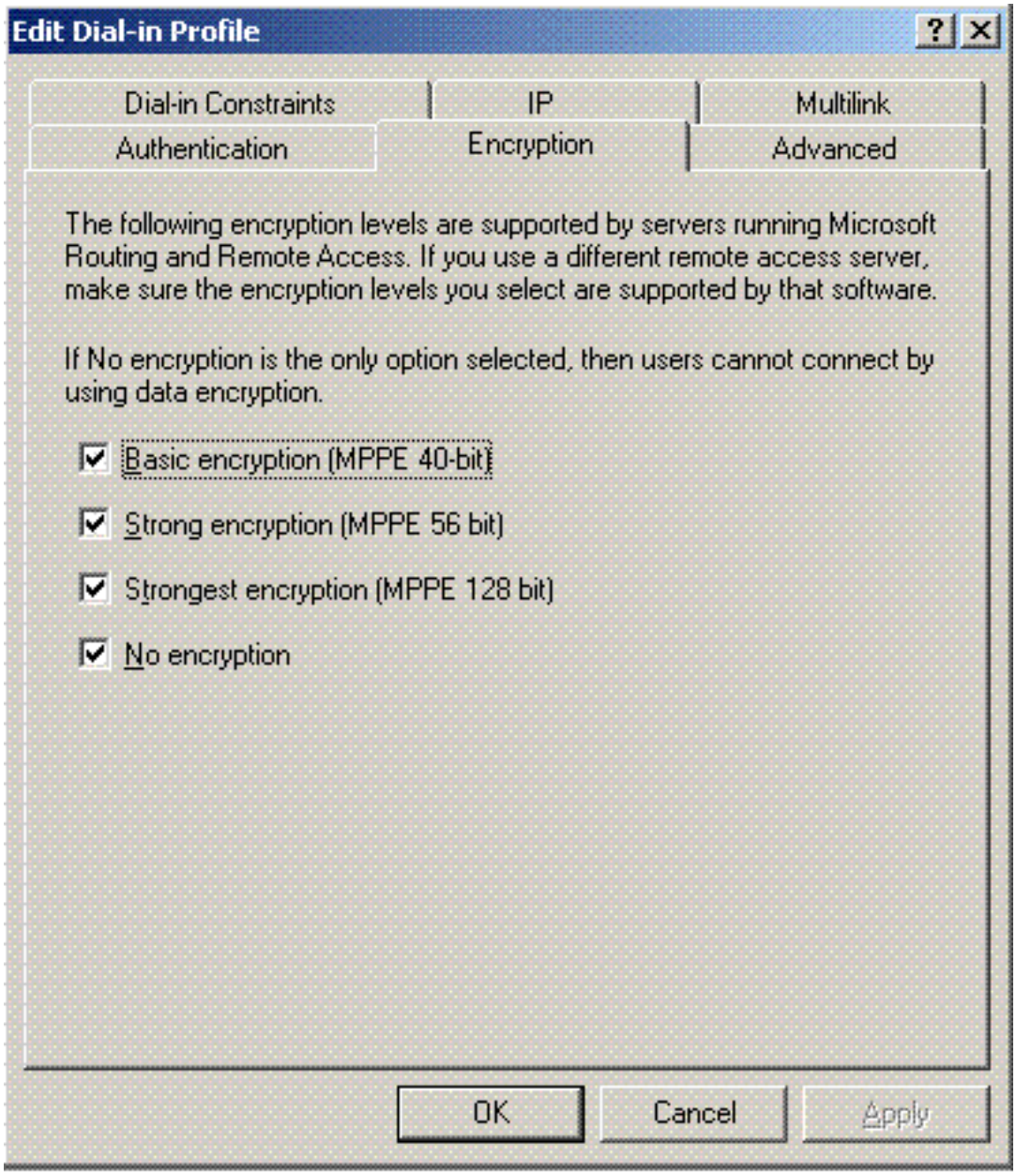
6. [EAP Methods] をクリックし、[EAP Providers]を選択して、EAPタイプとしてPEAPを追加します。



7. [Select EAP Providers]で[Edit] をクリックし、プルダウンメニューからActive Directoryユーザアカウントと CAに関連付けられたサーバ(tme.tme.comなど)を選択します。EAPタイプMSCHAP v2を追加します。

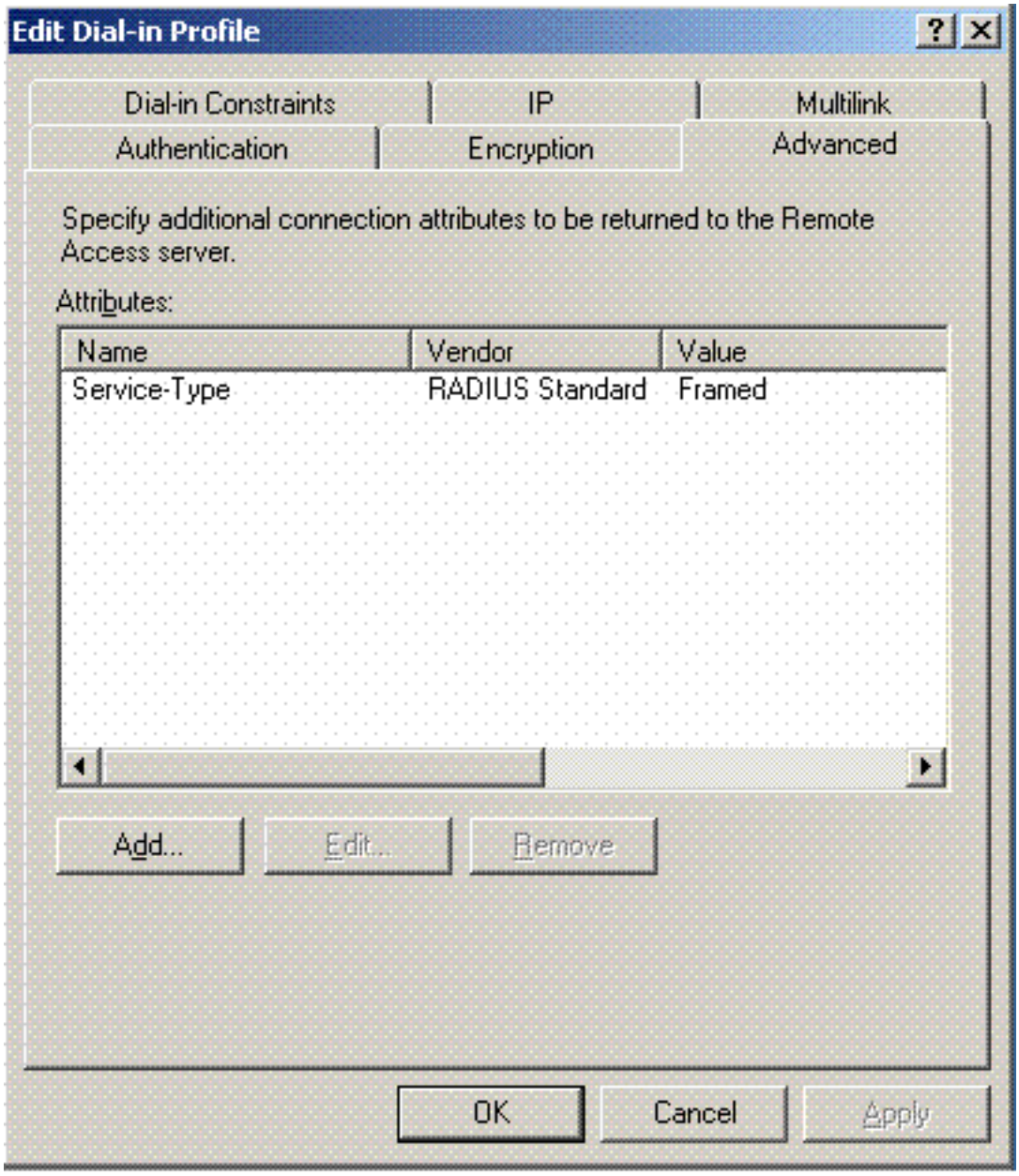


8. [Encryption] タブをクリックし、リモートアクセス用のすべての暗号化タイプを確認します



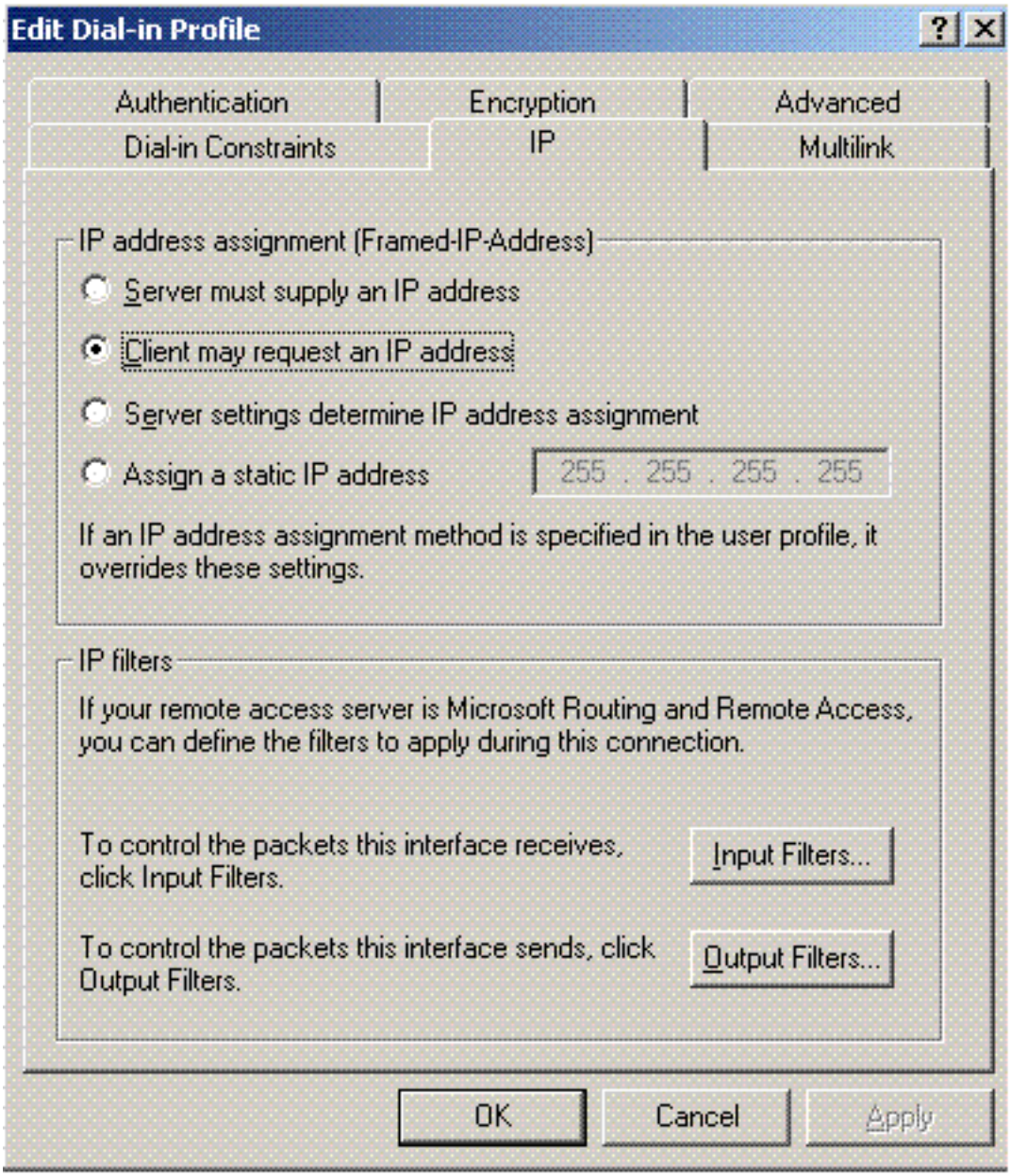
。

9. [Advanced] タブをクリックし、[Service-Type]として[RADIUS Standard/Framed]を追加しま



す。

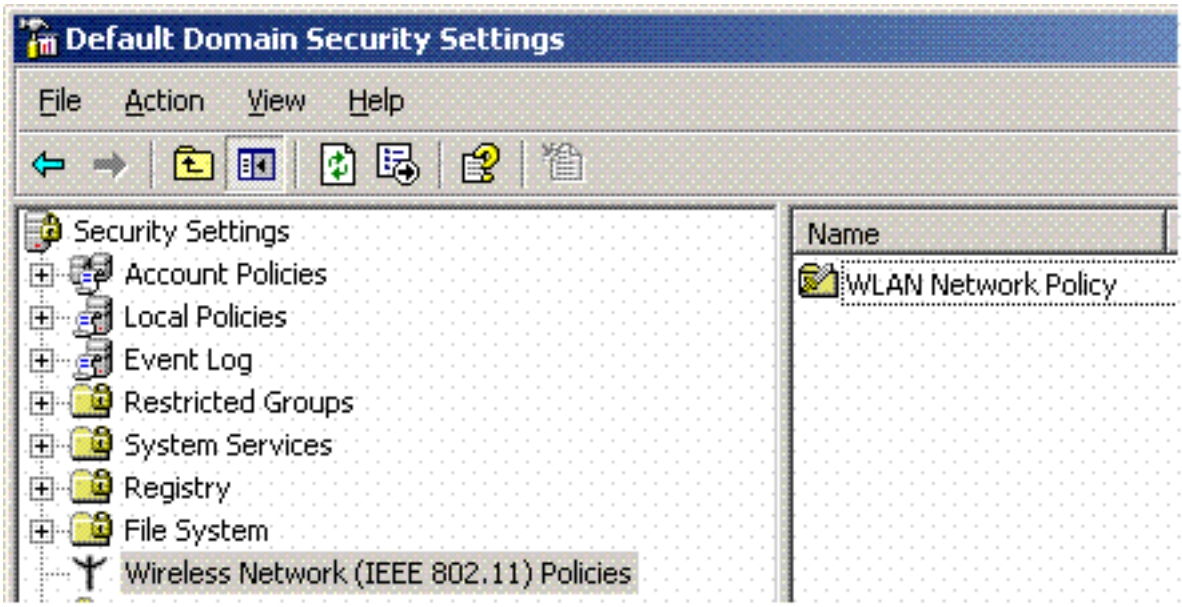
10. [IP] タブをクリックし、[Client may request an IP address] にチェックマークを付けます。
    ここでは、スイッチまたはWinServerでDHCPが有効になっていることを前提としています



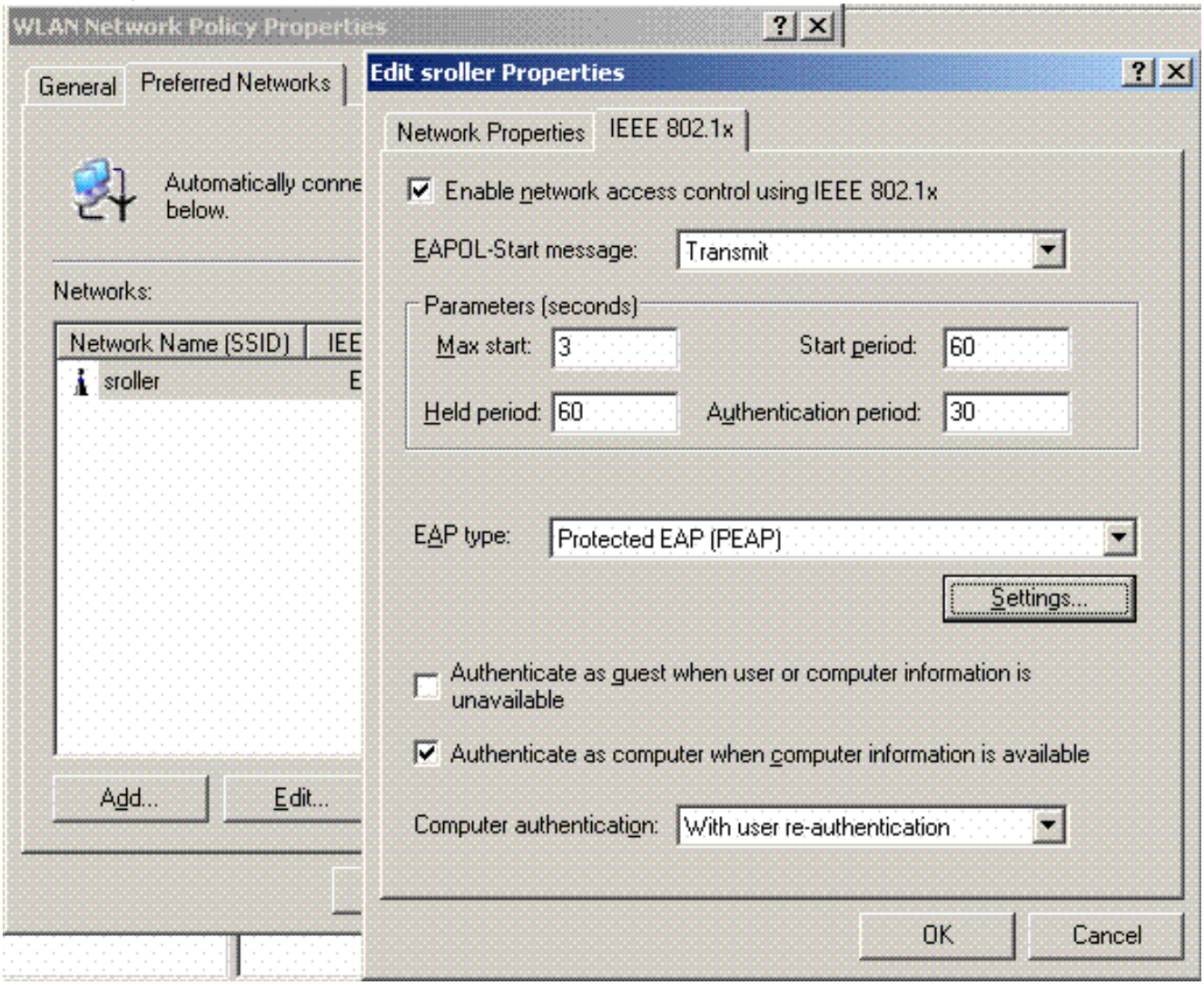
Microsoft Windows 2003ドメインのセキュリティ設定

Windows 2003ドメインのセキュリティ設定を行うには、次の手順を実行します。

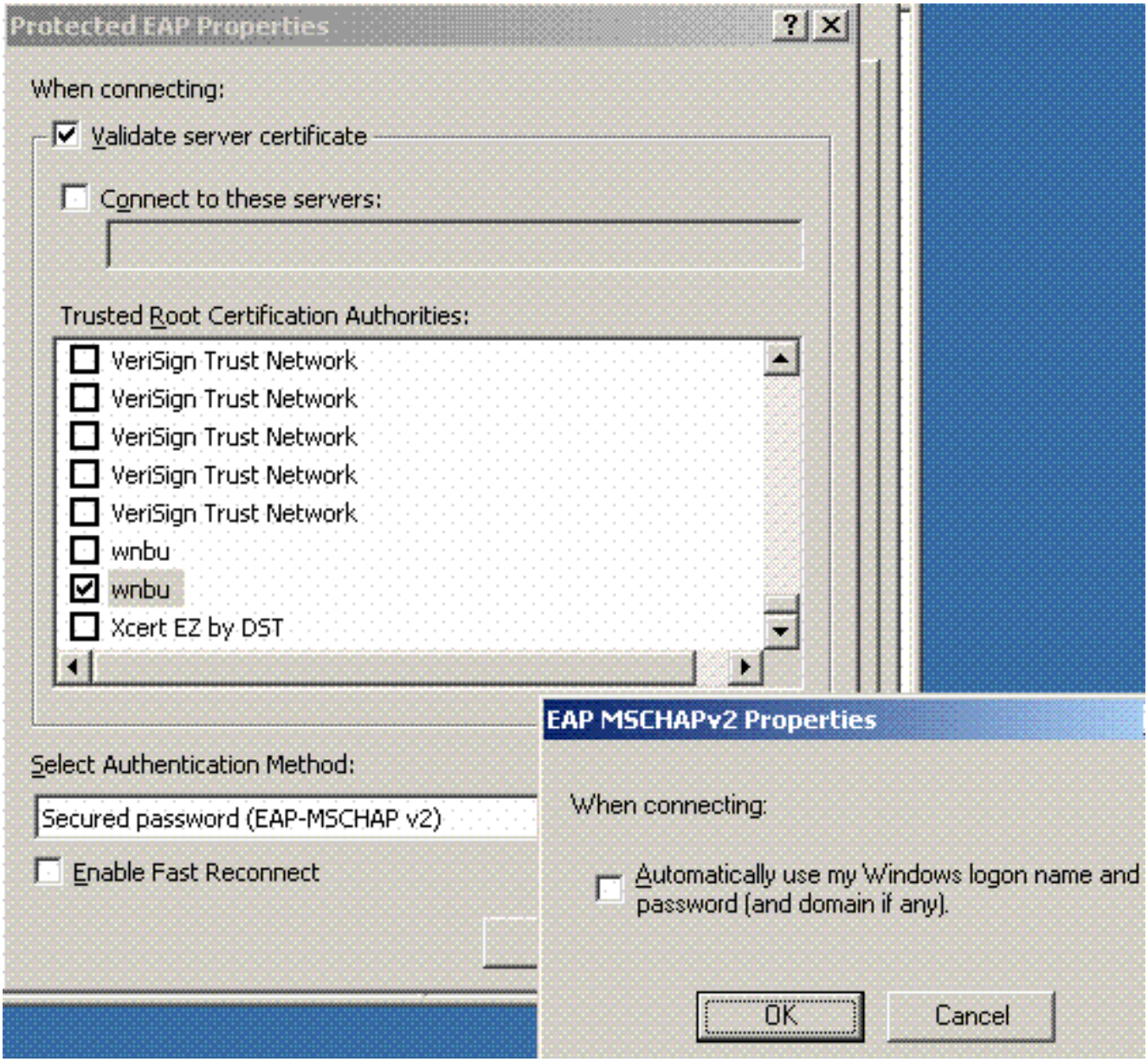
1. 既定のドメインセキュリティ設定マネージャーを起動し、ワイヤレスネットワーク(IEEE 802.11)ポリシーの新しいセキュリティポリシーを作成します。



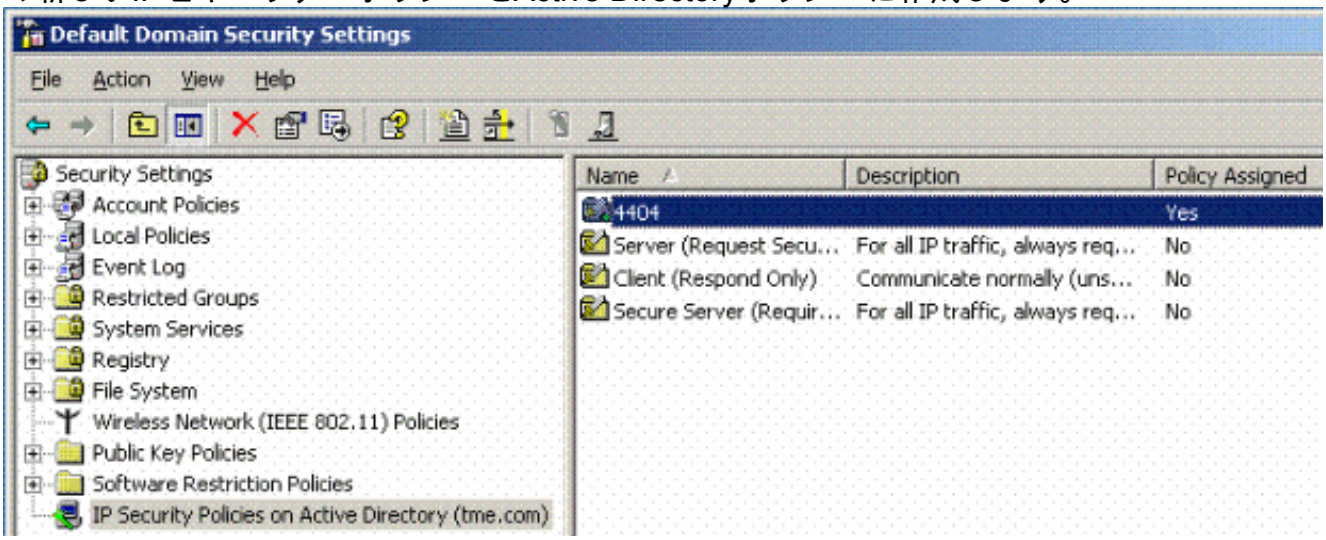
2. [WLAN Network Policy Properties]を開き、[Preferred Networks] をクリックします。新しい優先WLANを追加し、WLAN SSIDの名前(`Wireless`など)を入力します。新しい優先ネットワークをダブルクリックし、[**IEEE 802.1x**]タブをクリックします。EAPタイプとしてPEAPを選択します。



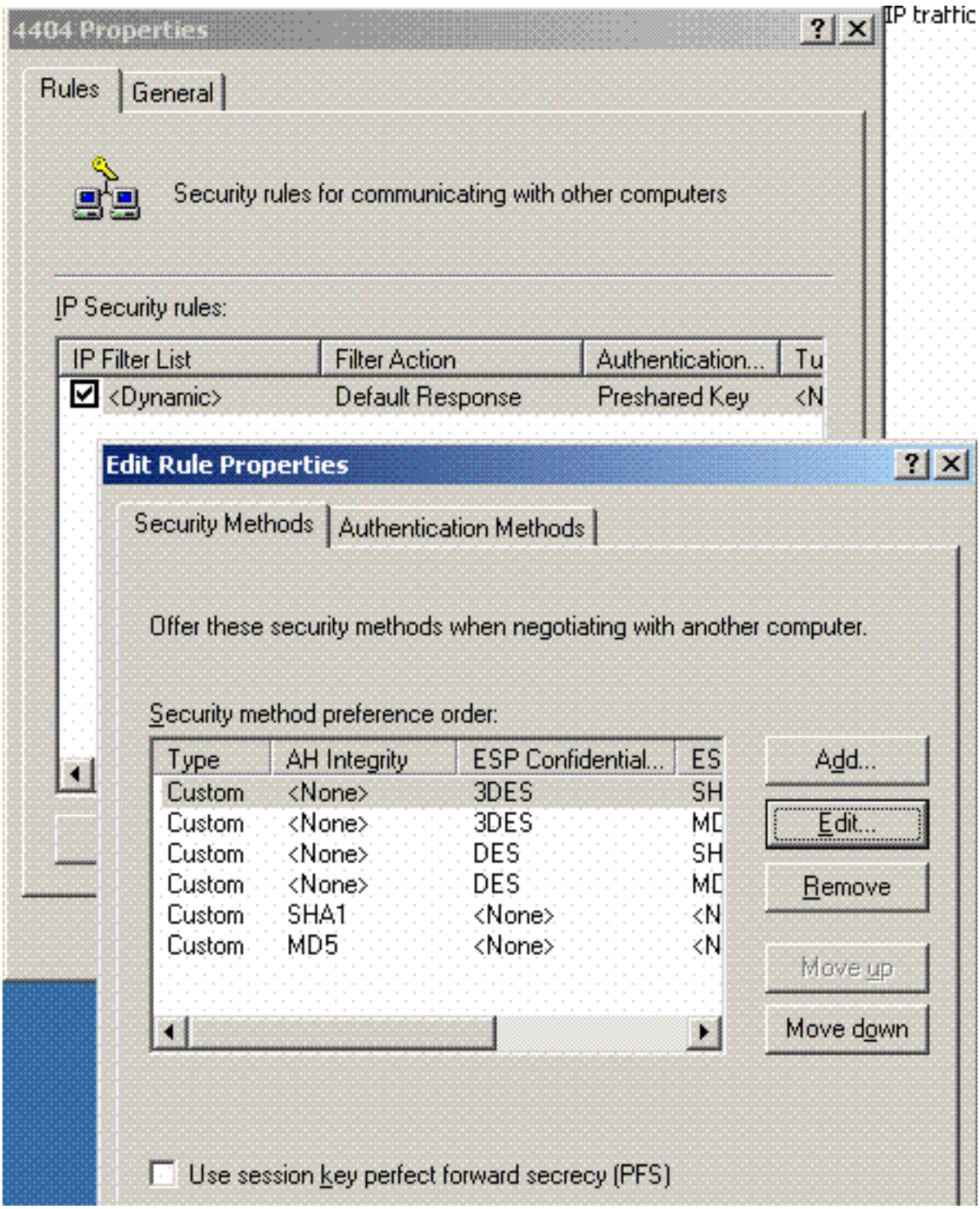
3. [PEAP Settings] をクリックし、[Validate server certificate] にチェックマークを入れて、[Trusted Root Cert installed on Certificate Authority]を選択します。テスト目的で、[Automatically use my Windows login and password]の[MS CHAP v2]ボックスをオフにします。



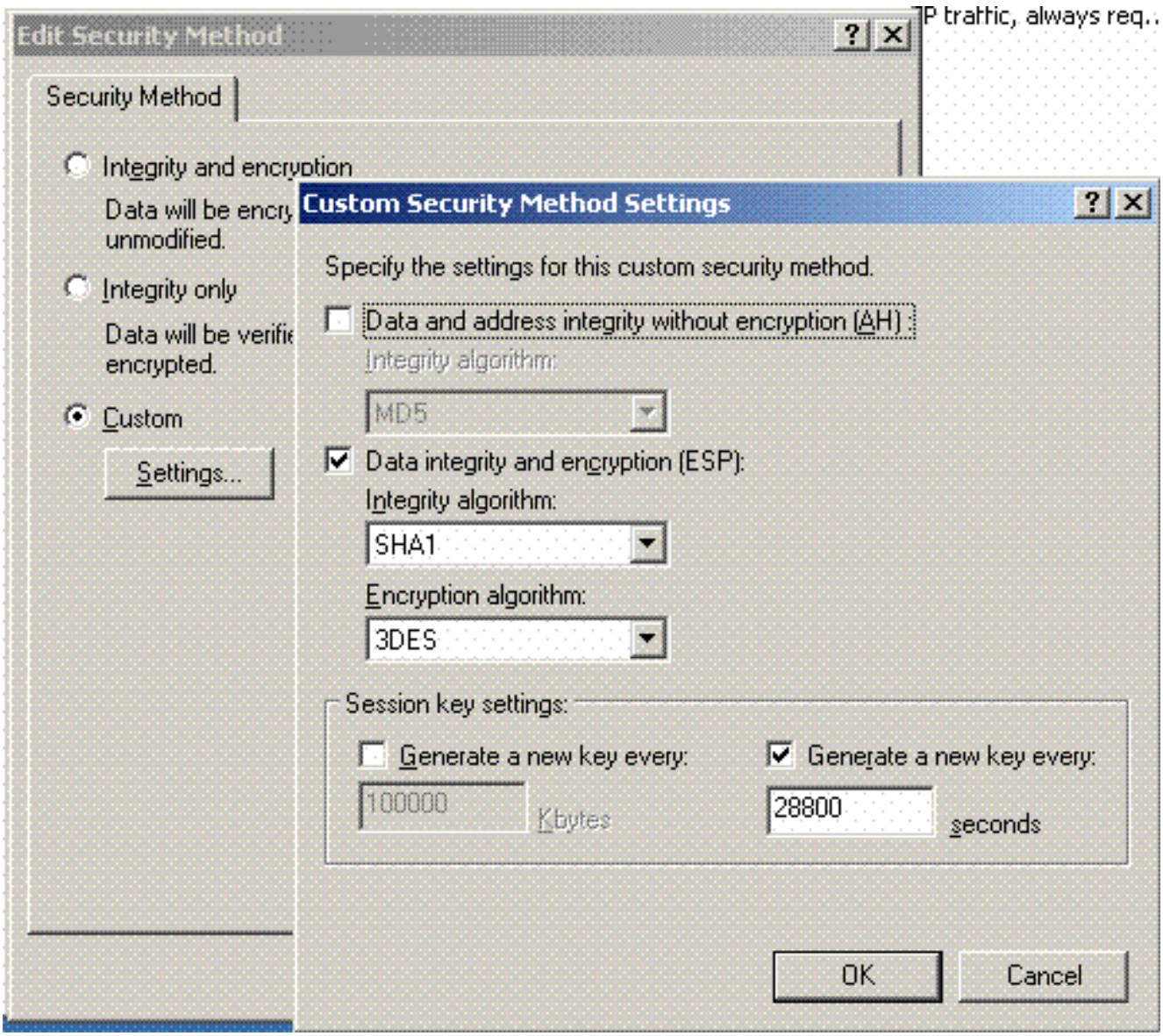
4. Windows 2003の[Default Domain Security Settings]マネージャウィンドウで、**4404**などの別の新しいIPセキュリティポリシーをActive Directoryポリシーに作成します。



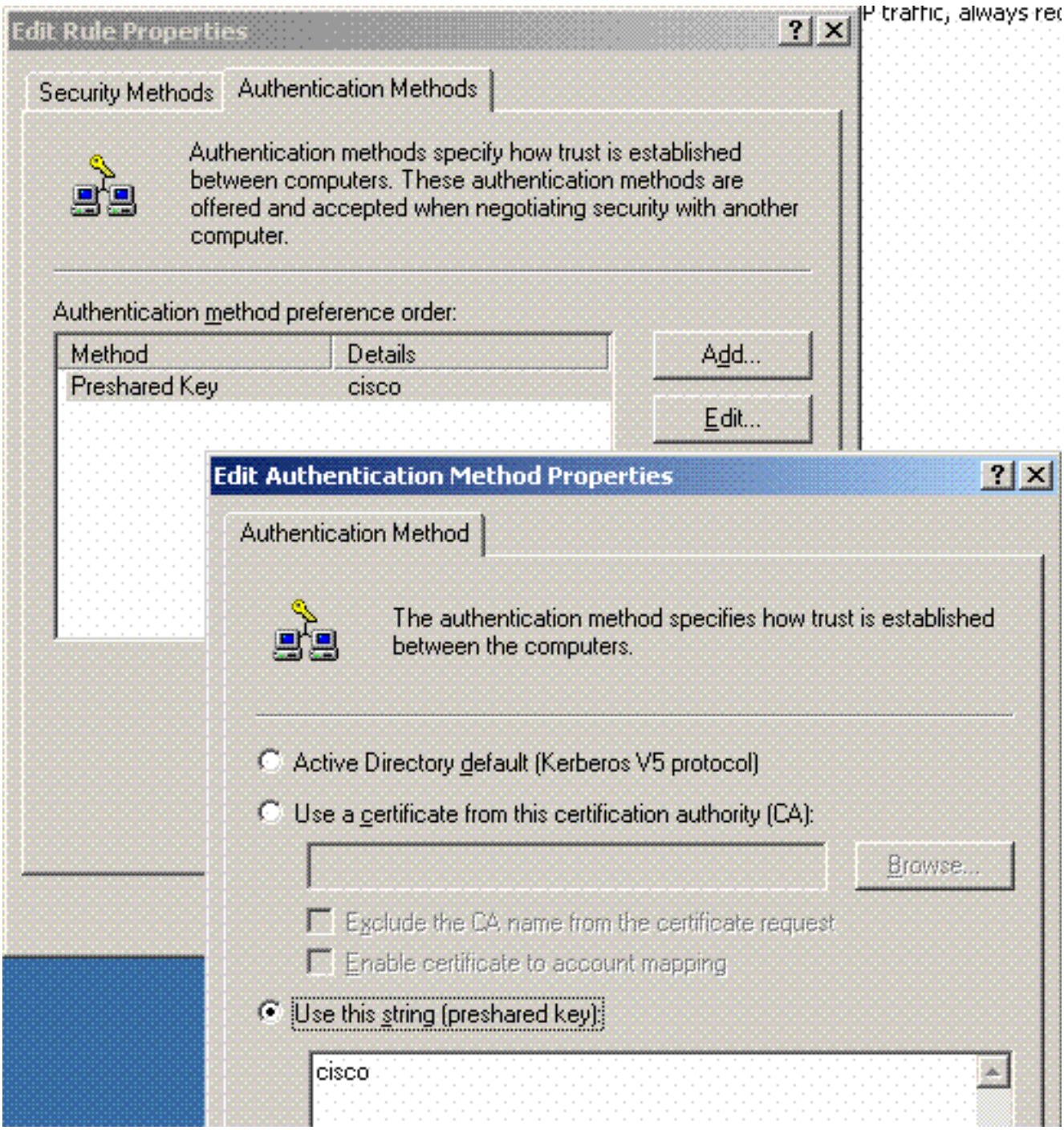
5. 新しい4404ポリシーのプロパティを編集し、[Rules] タブをクリックします。新しいフィルタルールを追加します(IPフィレットリスト（ダイナミック）、フィルタアクション（デフォルト応答）、認証(PSK)、トンネル（なし）)。新しく作成したフィルタルールをダブルクリックし、[Security Methods]を選択します。



6. [Edit Security Method] をクリックし、[Custom Settings] オプションボタンをクリックします。次の設定を選択します。**注：これらの設**定は、コントローラのRADIUS IPSecセキュリティ設定と一致している必要があります。



7. [Edit Rule Properties]の下の[Authentication Method] タブをクリックします。コントローラのRADIUS設定で以前に入力したのと同じ共有秘密を入力します。



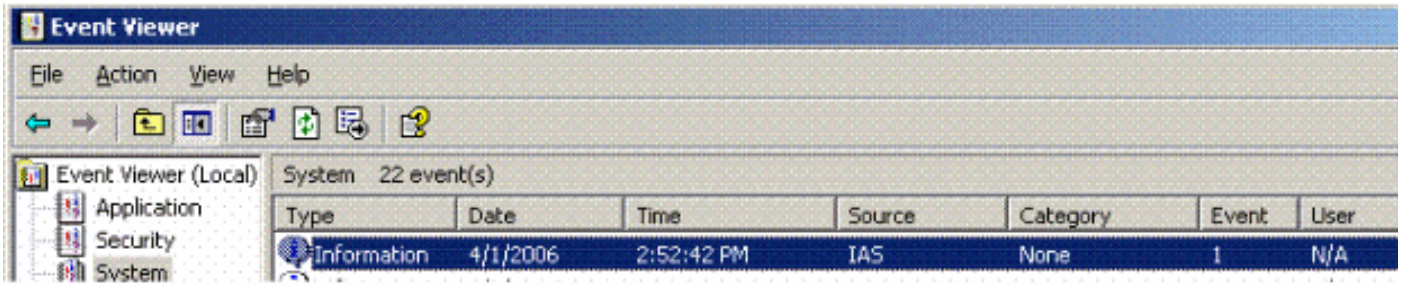
この時点で、コントローラ、IAS、およびドメインセキュリティ設定のすべての設定が完了します。コントローラとWinServerの両方ですべての設定を保存し、すべてのマシンをリブートします。テストに使用するWLANクライアントで、ルート証明書をインストールし、WPA2/PEAPを設定します。ルート証明書がクライアントにインストールされたら、クライアントマシンをリブートします。すべてのマシンが再起動したら、クライアントをWLANに接続し、これらのログイベントをキャプチャします。

注：コントローラとWinServer RADIUS間のIPSec接続をセットアップするには、クライアント接続が必要です。

Windows 2003システムログイベント

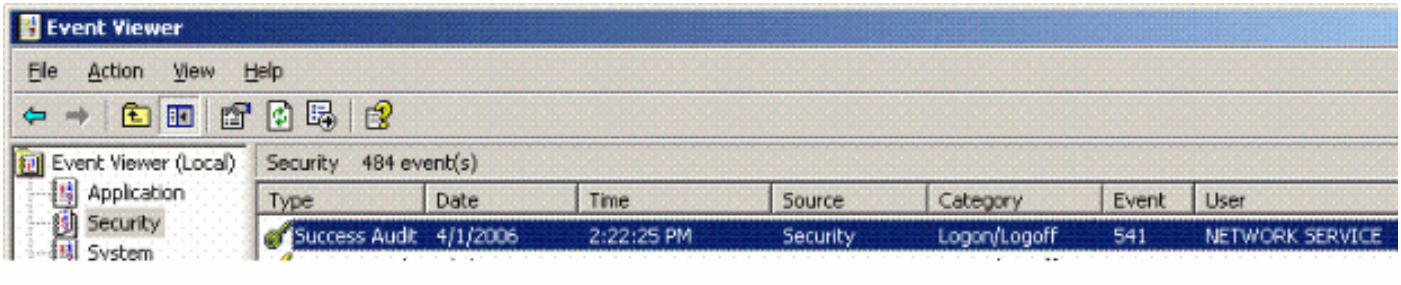
IPSec RADIUSが有効になっているWPA2/PEAP用に設定されたWLANクライアント接続が成功すると、WinServerで次のシステムイベントが生成されます。

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)
```

コントローラ<> RADIUS IPSec接続が成功すると、WinServerログに次のセキュリティイベントが生成されます。




```
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コントローラのRADIUS IPSec成功のデバッグ例

この設定を確認するには、コントローラでdebugコマンド**debug pm ikemsg enable**を使用します。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
```

民族的捕獲

以下に民族的捕獲の例を示す。

```
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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。