# 为WLC和Microsoft Windows 2003 IAS服务器配置RADIUS IPSec安全

## 目录

## 简介

本指南介绍如何配置WCS和以下WLAN控制器支持的RADIUS IPSec功能：

- 4400 系列
- WiSM
- 3750克

控制器RADIUS IPSec功能位于控制器GUI的**安全> AAA > RADIUS身份验证服务器**部分下。此功能为您提供了一种使用IPSec加密控制器和RADIUS服务器(IAS)之间的所有RADIUS通信的方法。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- LWAPP知识
- RADIUS身份验证和IPSec知识
- 了解如何在Windows 2003 Server操作系统上配置服务

### 使用的组件

要部署控制器RADIUS IPSec功能，必须安装和配置以下网络和软件组件：

- WLC 4400、WiSM或3750G控制器。本示例使用运行软件版本5.2.178.0的WLC 4400
- 轻量接入点(LAP)。本示例使用1231系列LAP。
- 使用DHCP的交换机
- Microsoft 2003服务器配置为域控制器，安装有Microsoft Certificate Authority和Microsoft Internet Authentication Service(IAS)。
- Microsoft域安全
- Cisco 802.11 a/b/g无线客户端适配器，带ADU 3.6版，配置了WPA2/PEAP

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## 规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

# IPSec RADIUS配置

本配置指南不介绍Microsoft WinServer、证书颁发机构、Active Directory或WLAN 802.1x客户端的安装或配置。在部署控制器IPSec RADIUS功能之前，必须安装和配置这些组件。本指南的其余部分介绍如何在这些组件上配置IPSec RADIUS:

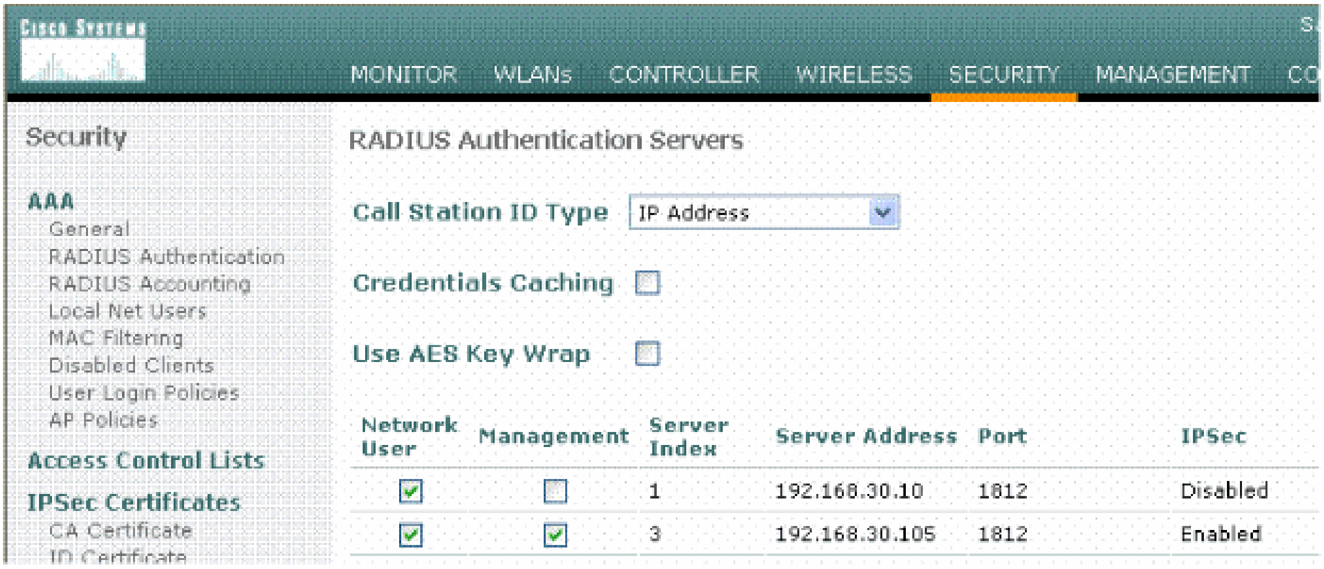
1. Cisco WLAN 控制器
2. Windows 2003 IAS
3. Microsoft Windows域安全设置

## 配置 WLC

本节介绍如何通过GUI在WLC上配置IPSec。

从控制器GUI中，完成以下步骤。

1. 导航到控制器GUI中的**Security > AAA > RADIUS Authentication**选项卡，然后添加新的RADIUS服务器。



RADIUS Authentication Servers

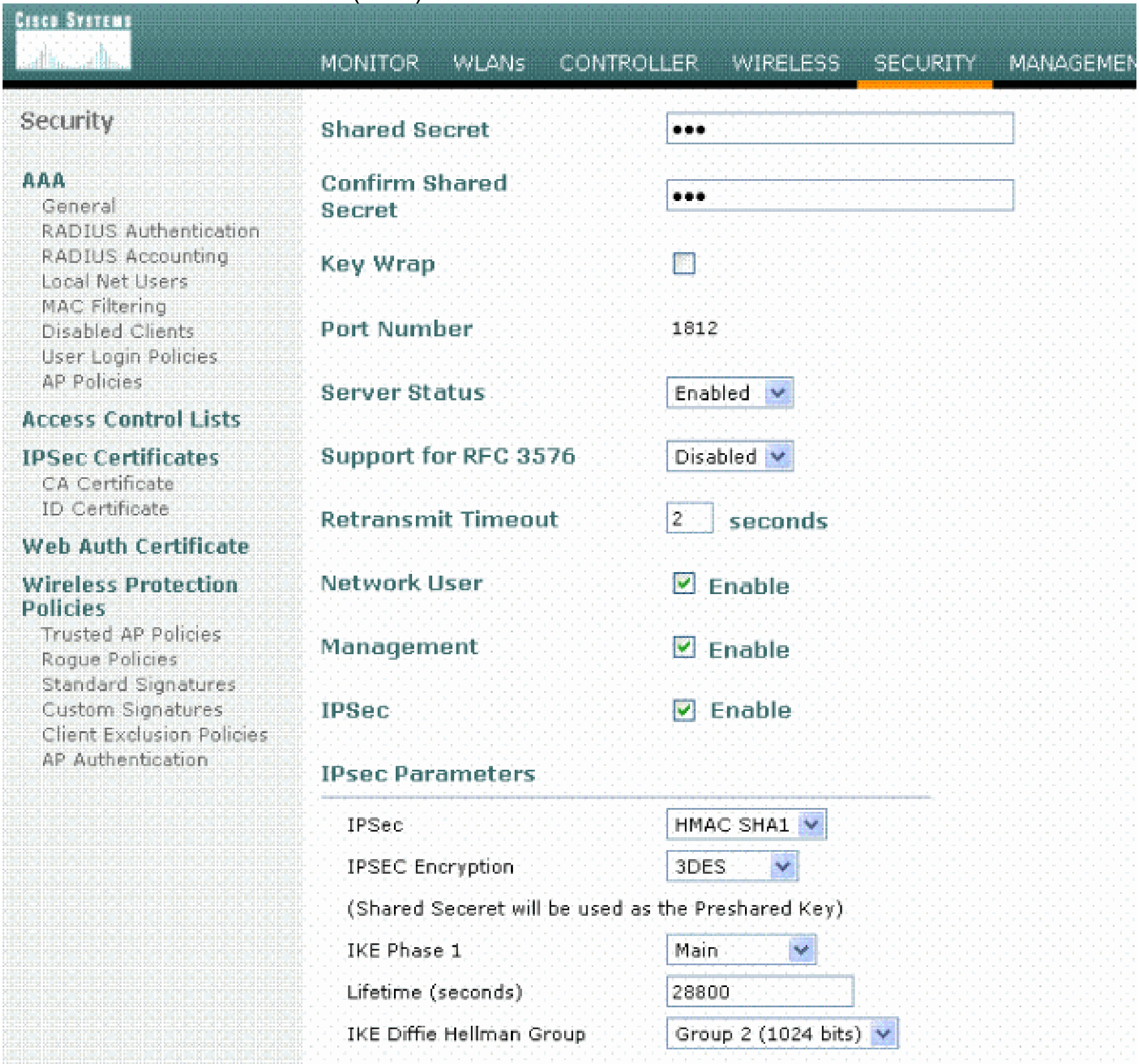
Call Station ID Type: IP Address

Credentials Caching □

Use AES Key Wrap □

| Network User | Management | Server Index | Server Address | Port | IPSec |
|---|---|---|---|---|---|
| ☑ | □ | 1 | 192.168.30.10 | 1812 | Disabled |
| ☑ | ☑ | 3 | 192.168.30.105 | 1812 | Enabled |

2. 配置新RADIUS服务器的IP地址、端口1812和共享密钥。选中**IPSec Enable**复选框，配置这些IPSec参数，然后单击**Apply**。**注意：**共享密钥既用于对RADIUS服务器进行身份验证，也用作IPSec身份验证的预共享密钥(PSK)。



Shared Secret ●●●

Confirm Shared Secret ●●●

Key Wrap □

Port Number 1812

Server Status Enabled

Support for RFC 3576 Disabled

Retransmit Timeout 2 seconds

Network User ☑ Enable

Management ☑ Enable

IPSec ☑ Enable

IPsec Parameters

IPSec HMAC SHA1

IPSEC Encryption 3DES

(Shared Seceret will be used as the Preshared Key)

IKE Phase 1 Main

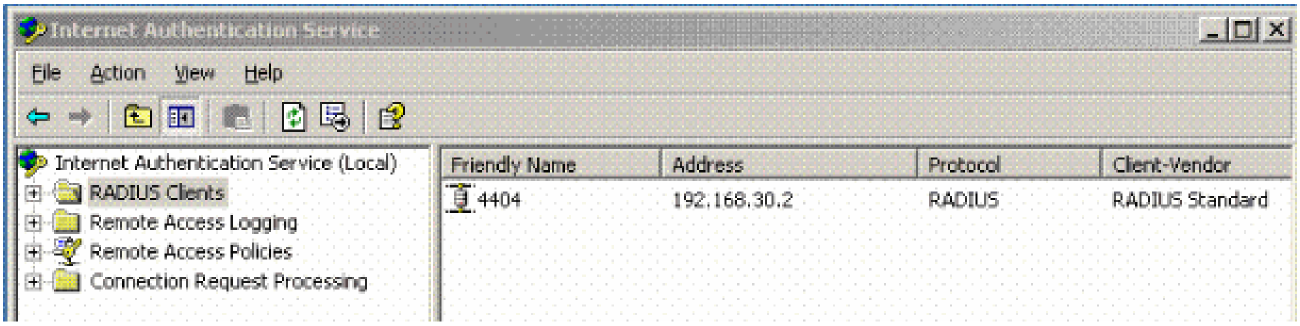
Lifetime (seconds) 28800

IKE Diffie Hellman Group Group 2 (1024 bits)

## 配置IAS

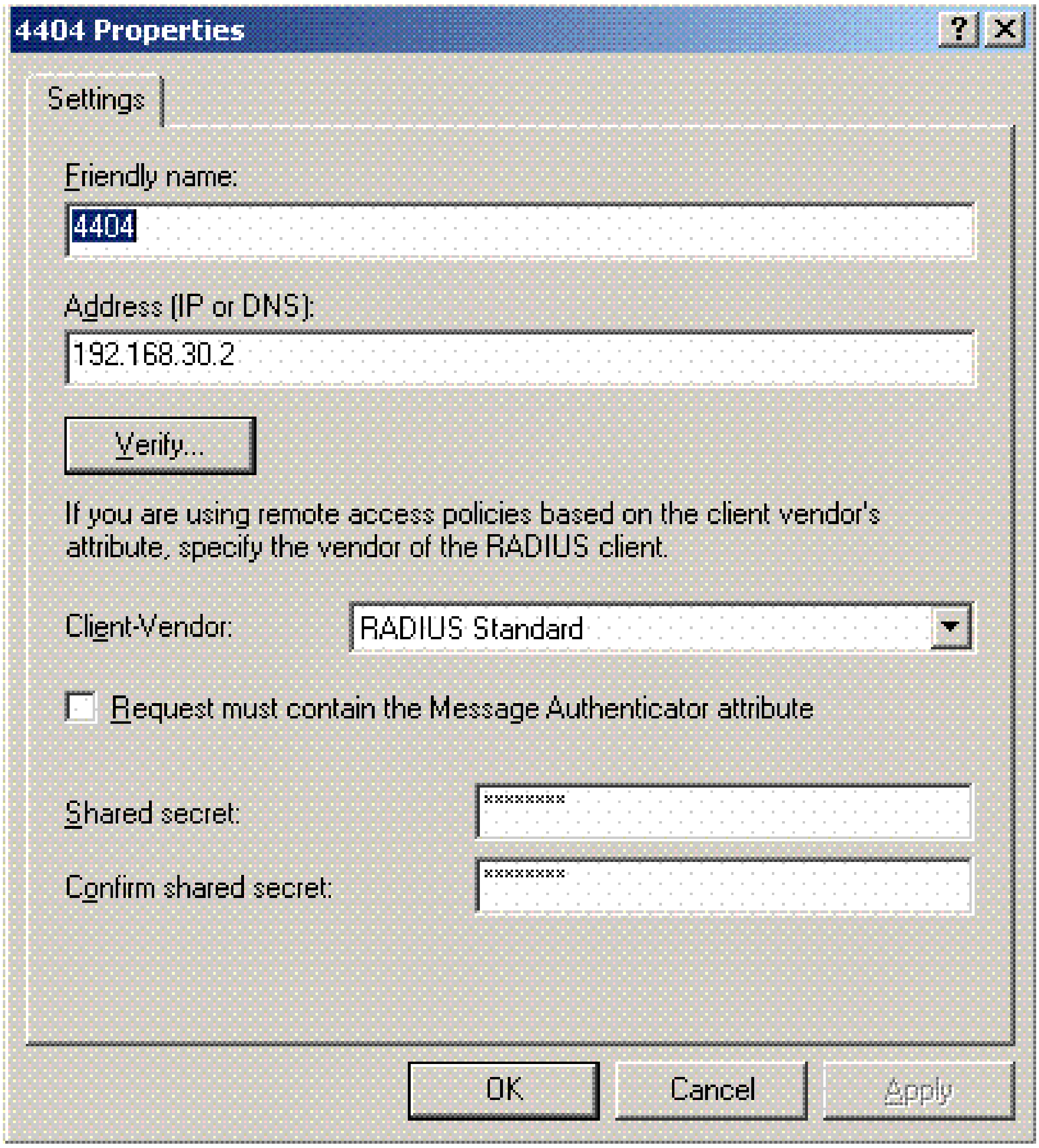
在IAS上完成以下步骤：

1. 导航到Win2003中的IAS管理器并添加新的RADIUS客户端。


Internet Authentication Service
File
Action
View
Help
Internet Authentication Service (Local)
RADIUS Clients
Remote Access Logging
Remote Access Policies
Connection Request Processing

| Friendly Name | Address | Protocol | Client-Vendor |
|---|---|---|---|
| 4404 | 192.168.30.2 | RADIUS | RADIUS Standard |

2. 使用控制器上配置的IP地址和共享密钥配置RADIUS客户端属性



4404 Properties

Settings

Friendly name: 4404

Address (IP or DNS): 192.168.30.2

If you are using remote access policies based on the client vendor's attribute, specify the vendor of the RADIUS client.

Client-Vendor: RADIUS Standard

□ Request must contain the Message Authenticator attribute

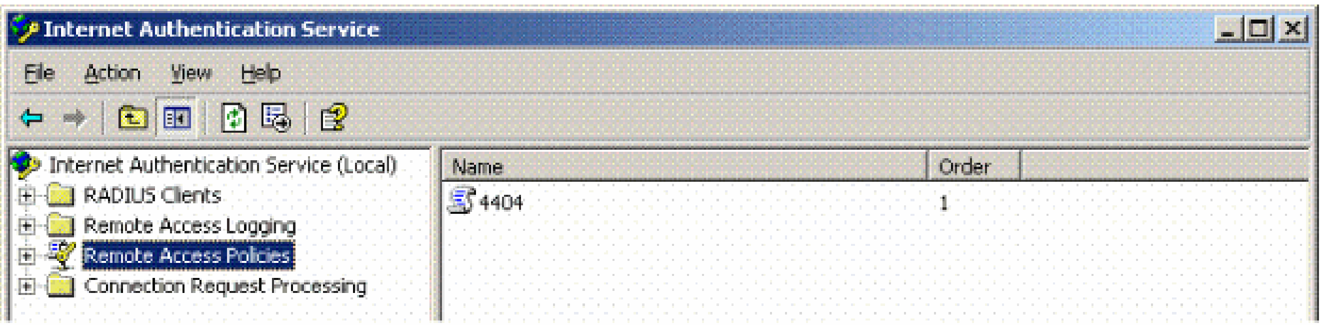
Shared secret: *********

Confirm shared secret: *********

:

3. 为控制器配置新的远程访问策略

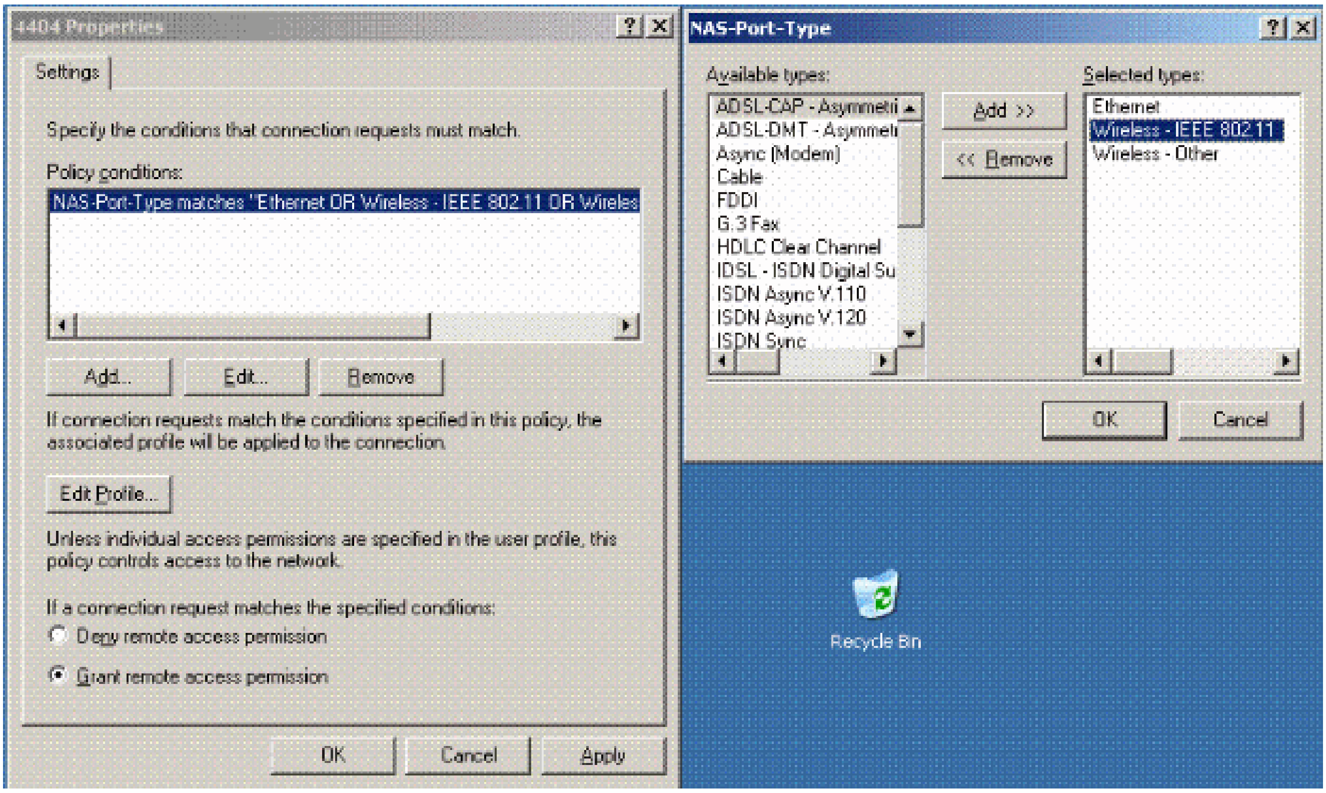
:



Internet Authentication Service

| Name | Order |
|---|---|
| 4404 | 1 |

4. 编辑控制器远程访问策略的属性。确保添加NAS端口类型 — 无线 — IEEE 802.11:



4404 Properties

Settings

Specify the conditions that connection requests must match.

Policy conditions:

NAS-Port-Type matches "Ethernet OR Wireless - IEEE 802.11 OR Wireles

If connection requests match the conditions specified in this policy, the associated profile will be applied to the connection.

Unless individual access permissions are specified in the user profile, this policy controls access to the network.

If a connection request matches the specified conditions:

○ Deny remote access permission

● Grant remote access permission

NAS-Port-Type

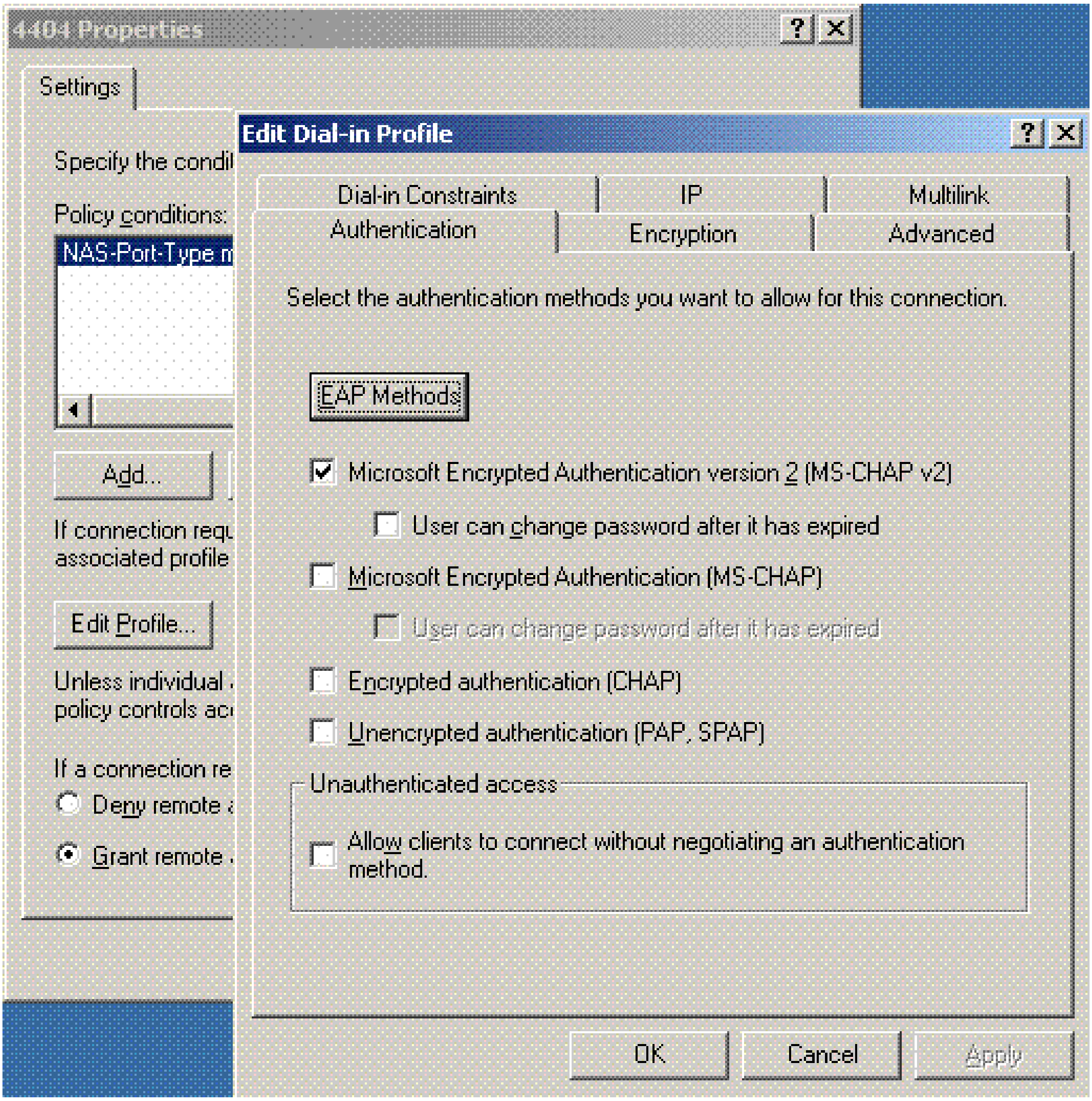
Available types:

ADSL-CAP - Asymmetri
ADSL-DMT - Asymmetri
Async (Modem)
Cable
FDDI
G.3 Fax
HDLC Clear Channel
IDSL - ISDN Digital Su
ISDN Async V.110
ISDN Async V.120
ISDN Sync

Selected types:

Ethernet
Wireless - IEEE 802.11
Wireless - Other

5. 单击**Edit Profile**，单击**Authentication**选项卡，并选中MS-CHAP v2进行身份验证：



Select the authentication methods you want to allow for this connection.

☑ Microsoft Encrypted Authentication version 2 (MS-CHAP v2)

☐ User can change password after it has expired

☐ Microsoft Encrypted Authentication (MS-CHAP)

☐ User can change password after it has expired

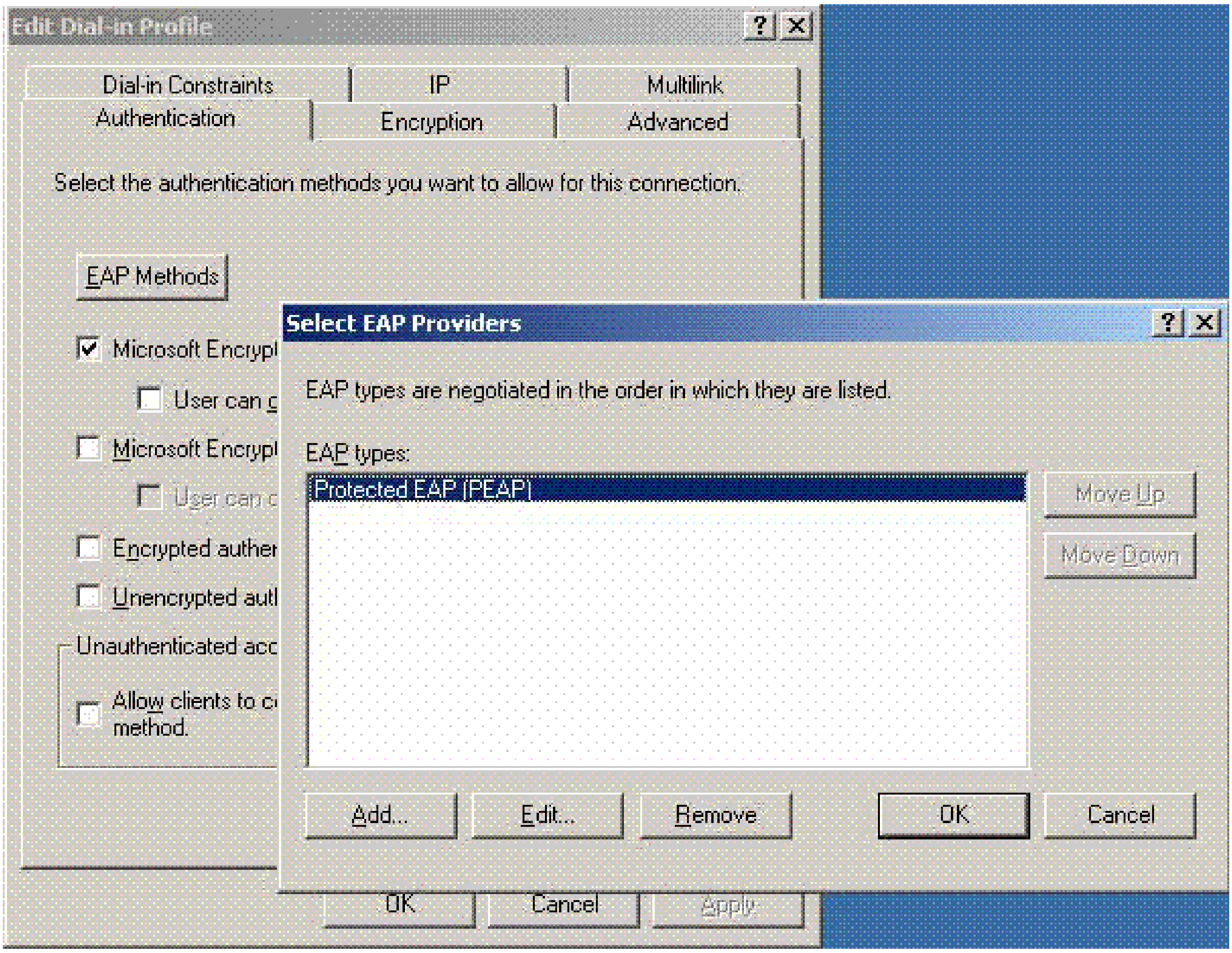
☐ Encrypted authentication (CHAP)

☐ Unencrypted authentication (PAP, SPAP)

Unauthenticated access

☐ Allow clients to connect without negotiating an authentication method.

6. 单击**EAP Methods**，选择EAP Providers，并将PEAP添加为EAP类型：



Edit Dial-in Profile

Select the authentication methods you want to allow for this connection.

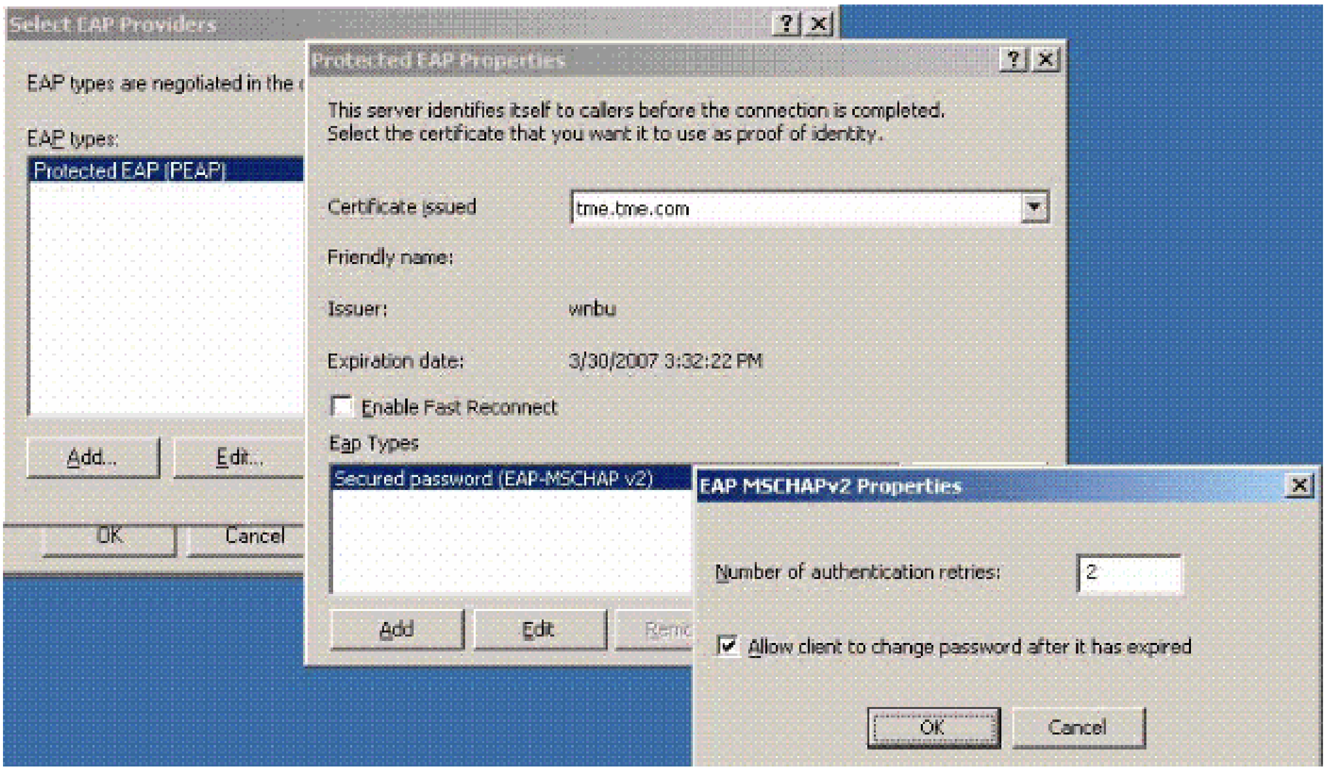
EAP types are negotiated in the order in which they are listed.

EAP types:

Protected EAP (PEAP)

☑ Microsoft Encrypt

7. 点击Select EAP Providers上的**Edit**，然后从下拉菜单中选择与您的Active Directory用户帐户和CA(例如tme.tme.com)关联的服务器。添加EAP类型MSCHAP v2:



Select EAP Providers

EAP types are negotiated in the

EAP types:

Protected EAP (PEAP)

Protected EAP Properties

This server identifies itself to callers before the connection is completed. Select the certificate that you want it to use as proof of identity.

Certificate issued: tme.tme.com

Friendly name:

Issuer: wnbu

Expiration date: 3/30/2007 3:32:22 PM

□ Enable Fast Reconnect

Eap Types

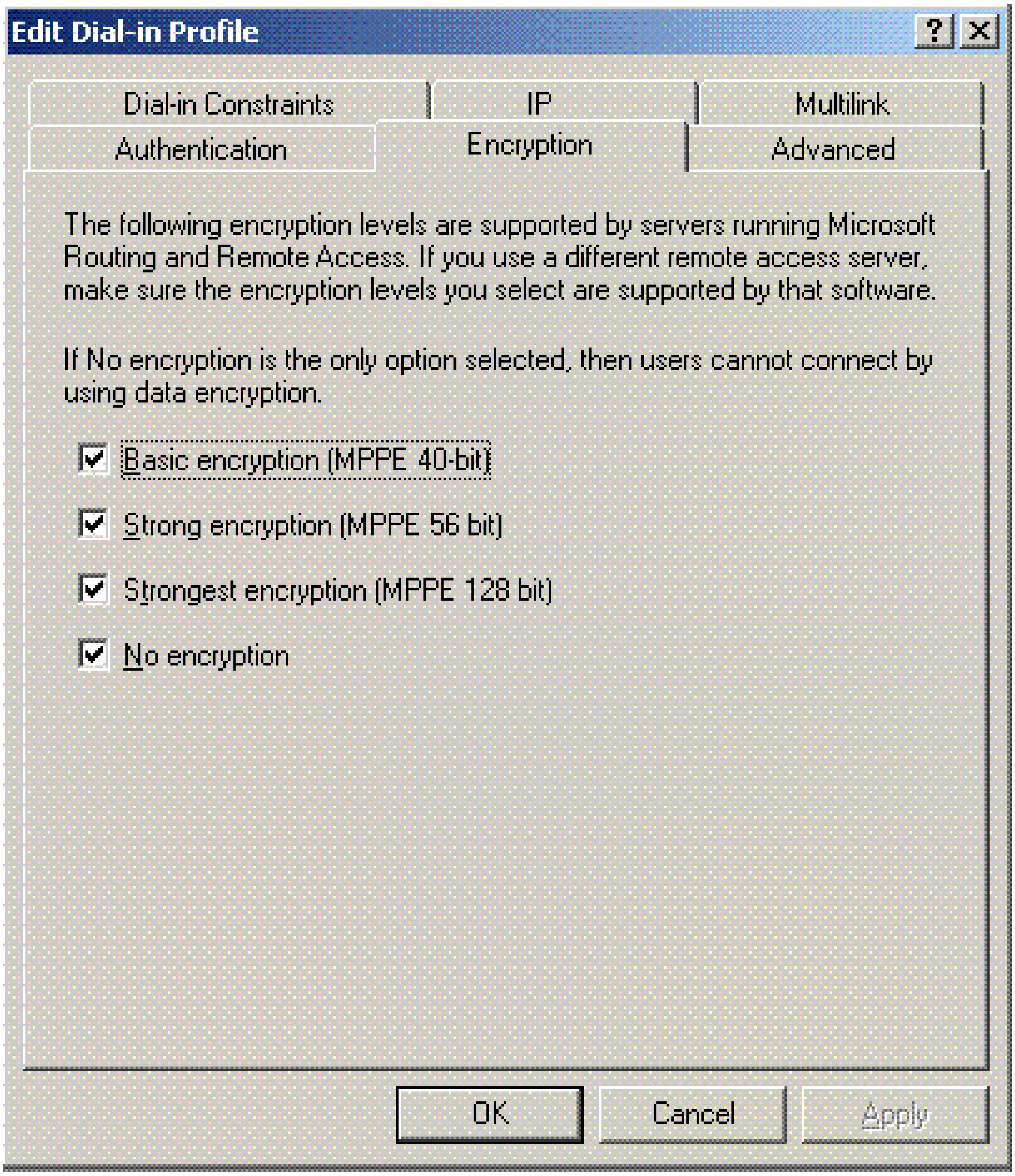
Secured password (EAP-MSCHAP v2)

EAP MSCHAPv2 Properties

Number of authentication retries: 2

☑ Allow client to change password after it has expired

8. 单击**Encryption**选项卡，并检查远程访问的所有加密类型



The following encryption levels are supported by servers running Microsoft Routing and Remote Access. If you use a different remote access server, make sure the encryption levels you select are supported by that software.

If No encryption is the only option selected, then users cannot connect by using data encryption.

☑ Basic encryption (MPPE 40-bit)

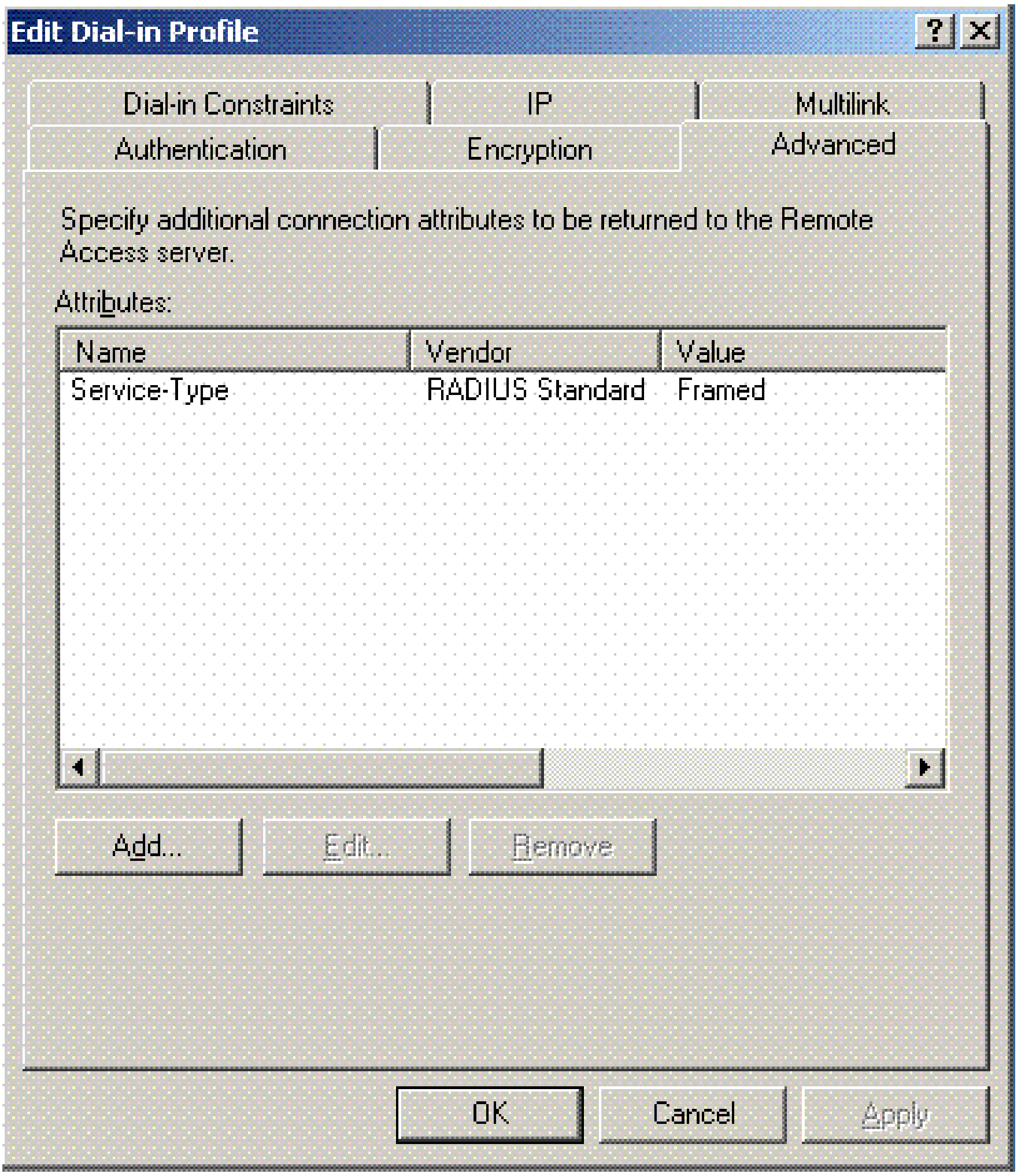
☑ Strong encryption (MPPE 56 bit)

☑ Strongest encryption (MPPE 128 bit)

☑ No encryption

:

9. 单击**Advanced**选项卡，并将RADIUS Standard/Framed添加为Service-



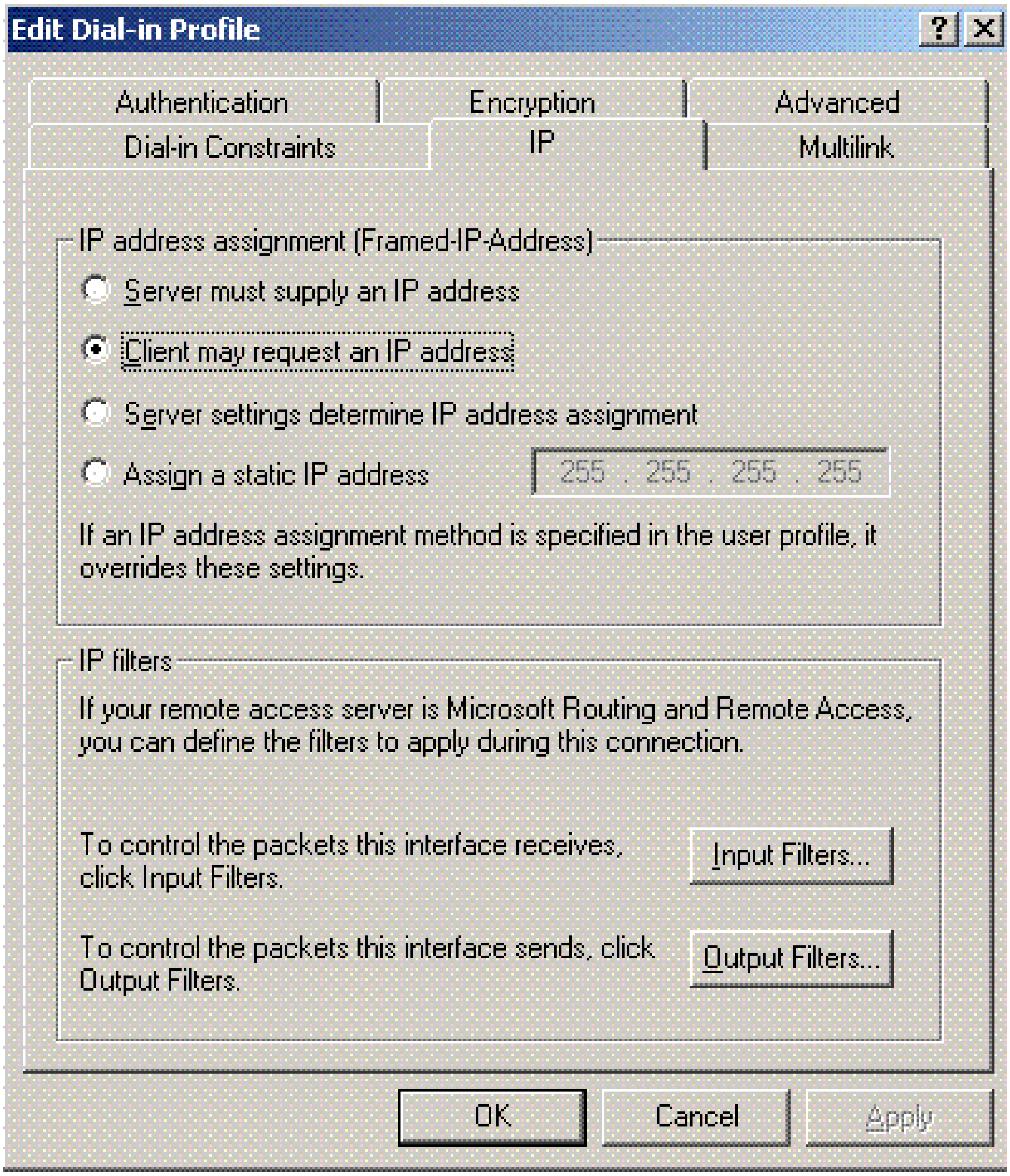
Specify additional connection attributes to be returned to the Remote Access server.

Attributes:

| Name | Vendor | Value |
|---|---|---|
| Service-Type | RADIUS Standard | Framed |

Type:

10. 单击**IP**选项卡，并选中**Client may request an IP address**。假设您在交换机或WinServer上启



IP address assignment (Framed-IP-Address)

○ Server must supply an IP address

● Client may request an IP address

○ Server settings determine IP address assignment

○ Assign a static IP address 255 . 255 . 255 . 255

If an IP address assignment method is specified in the user profile, it overrides these settings.

IP filters

If your remote access server is Microsoft Routing and Remote Access, you can define the filters to apply during this connection.

To control the packets this interface receives, click Input Filters.

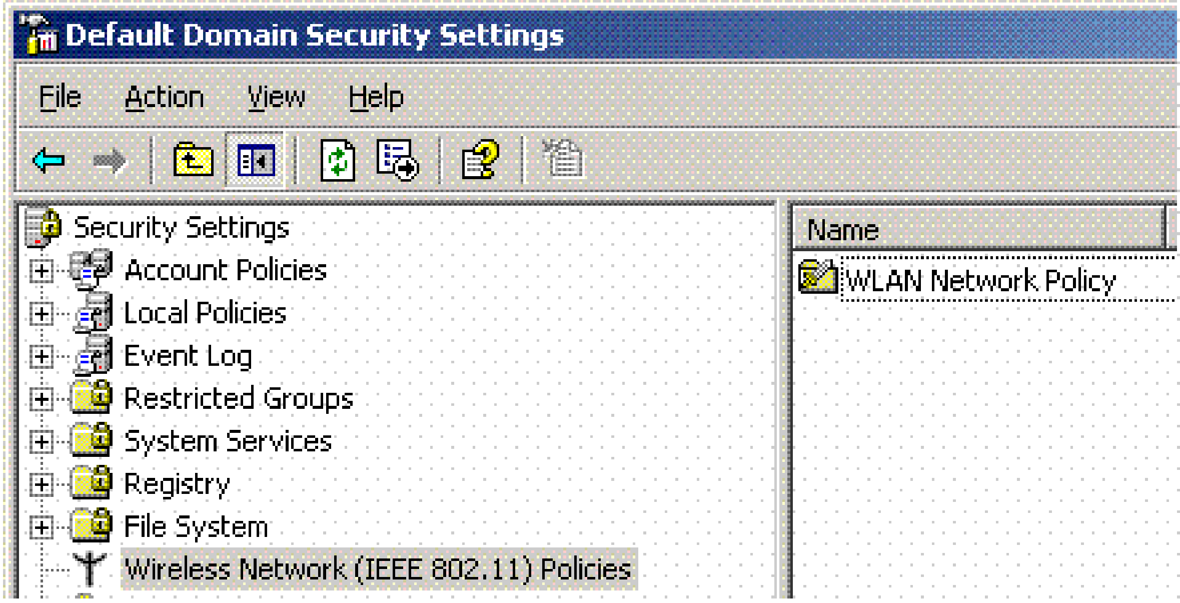
To control the packets this interface sends, click Output Filters.

用了DHCP。

## Microsoft Windows 2003域安全设置

要配置Windows 2003域安全设置，请完成以下步骤：

1. 启动默认域安全设置管理器，并为无线网络(IEEE 802.11)策略创建新的安全策略。

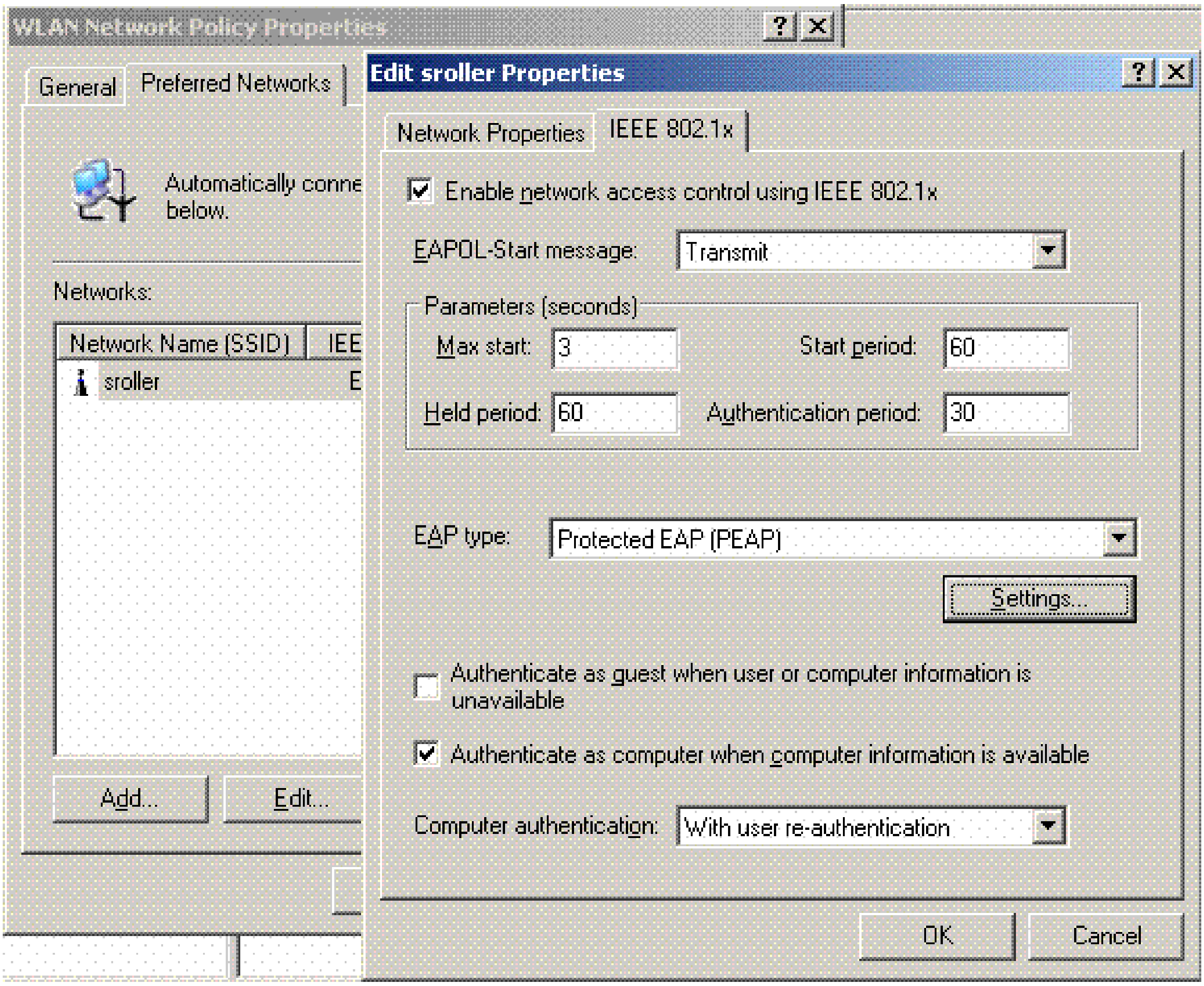


Security Settings
- Account Policies
- Local Policies
- Event Log
- Restricted Groups
- System Services
- Registry
- File System
- Wireless Network (IEEE 802.11) Policies

Name
- WLAN Network Policy

2. 打开WLAN网络策略属性，然后单击**首选网络**。添加新的首选WLAN并键入您的WLAN SSID的名称，例如`Wireless`。双击新的首选网络，然后点**击IEEE 802.1x选项**卡。选择PEAP作为EAP类型

：



| Network Name (SSID) | IEE |
|---|---|
| sroller | E |

☑ Enable network access control using IEEE 802.1x

EAPOL-Start message: Transmit

Parameters (seconds)

Max start: 3　Start period: 60

Held period: 60　Authentication period: 30

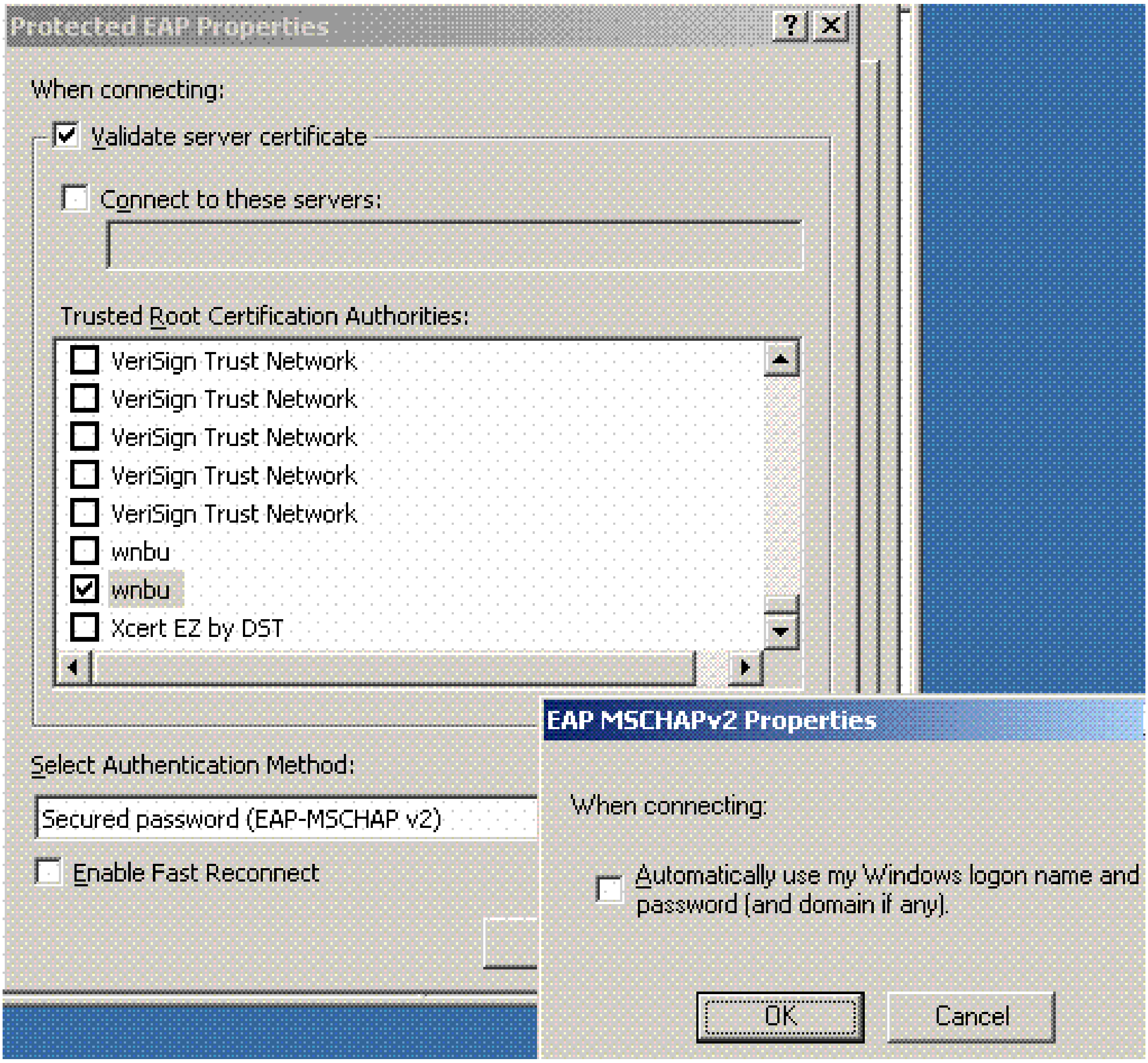
EAP type: Protected EAP (PEAP)

□ Authenticate as guest when user or computer information is unavailable

☑ Authenticate as computer when computer information is available

Computer authentication: With user re-authentication

3. 单击**PEAP Settings**，选中**Validate server certificate**，然后选择Trusted Root Cert installed on Certificate Authority。出于测试目的，请取消选中MS CHAP v2 for Automatically use my Windows login and password。



Protected EAP Properties

When connecting:

☑ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

□ VeriSign Trust Network
□ VeriSign Trust Network
□ VeriSign Trust Network
□ VeriSign Trust Network
□ VeriSign Trust Network
□ wnbu
☑ wnbu
□ Xcert EZ by DST

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

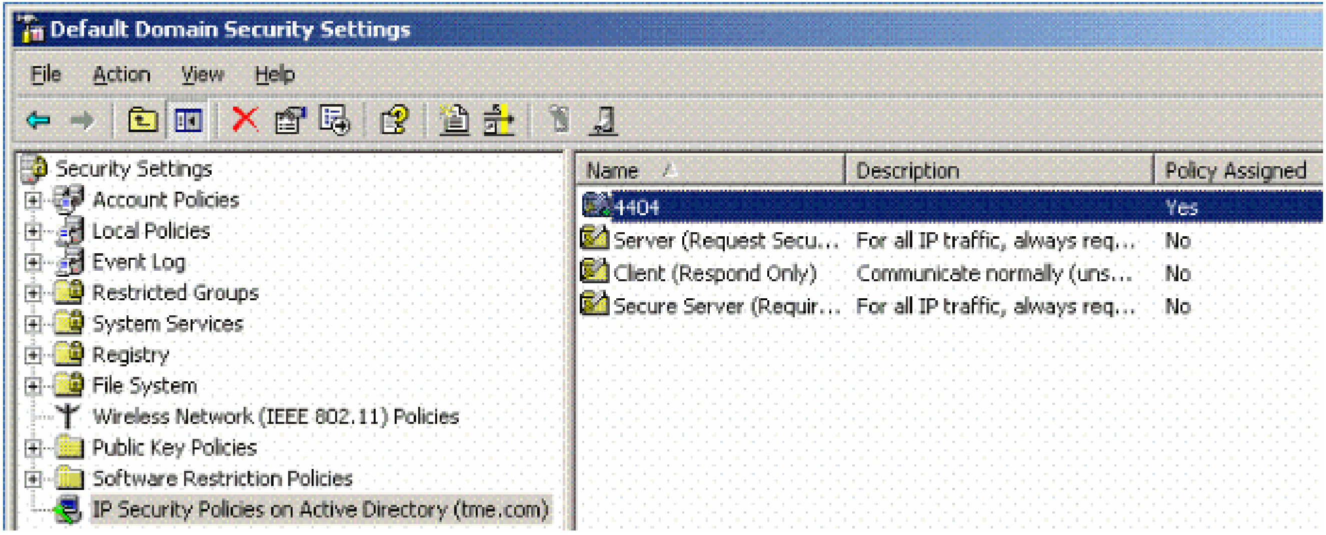
□ Enable Fast Reconnect

EAP MSCHAPv2 Properties

When connecting:

□ Automatically use my Windows logon name and password (and domain if any).

4. 在Windows 2003 Default Domain Security Settings Manager窗口中，在Active Directory策略上创建另一个新的IP安全策略，例如**4404**。

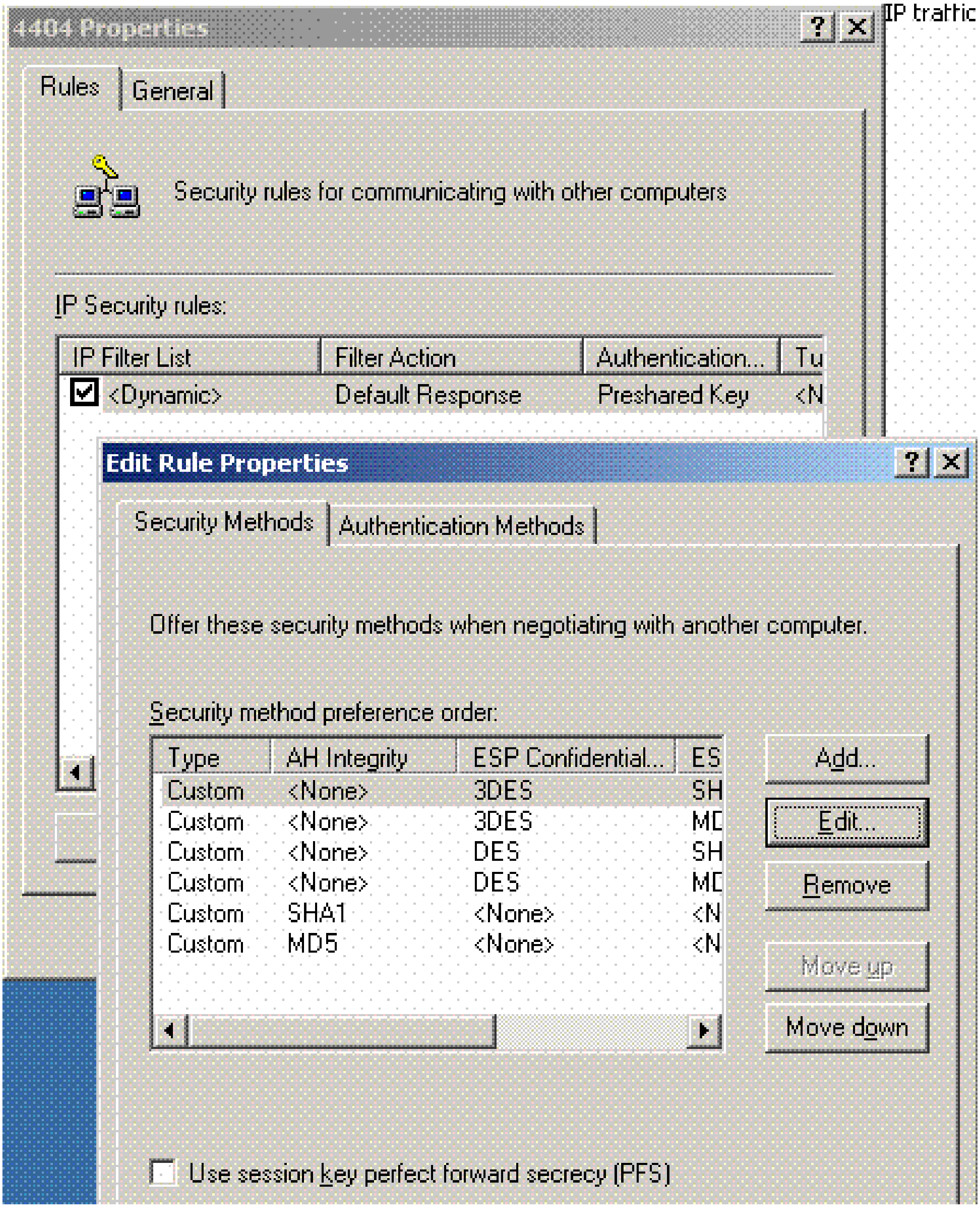


Default Domain Security Settings

- Security Settings
  - Account Policies
  - Local Policies
  - Event Log
  - Restricted Groups
  - System Services
  - Registry
  - File System
  - Wireless Network (IEEE 802.11) Policies
  - Public Key Policies
  - Software Restriction Policies
  - IP Security Policies on Active Directory (tme.com)

| Name | Description | Policy Assigned |
|---|---|---|
| 4404 | | Yes |
| Server (Request Secu... | For all IP traffic, always req... | No |
| Client (Respond Only) | Communicate normally (uns... | No |
| Secure Server (Requir... | For all IP traffic, always req... | No |

5. 编辑新的4404策略属性，然后点击**Rules**选项卡。添加新的过滤规则 — IP Filet List(Dynamic);Filter Action(Default Response);Authentication(PSK);Tunnel(None)。双击新创建的过滤规则，然后选择Security Methods:



4404 Properties

Rules | General

Security rules for communicating with other computers

IP Security rules:

| IP Filter List | Filter Action | Authentication... | Tu |
|---|---|---|---|
| ☑ <Dynamic> | Default Response | Preshared Key | <N |

IP traffic

Edit Rule Properties

Security Methods | Authentication Methods

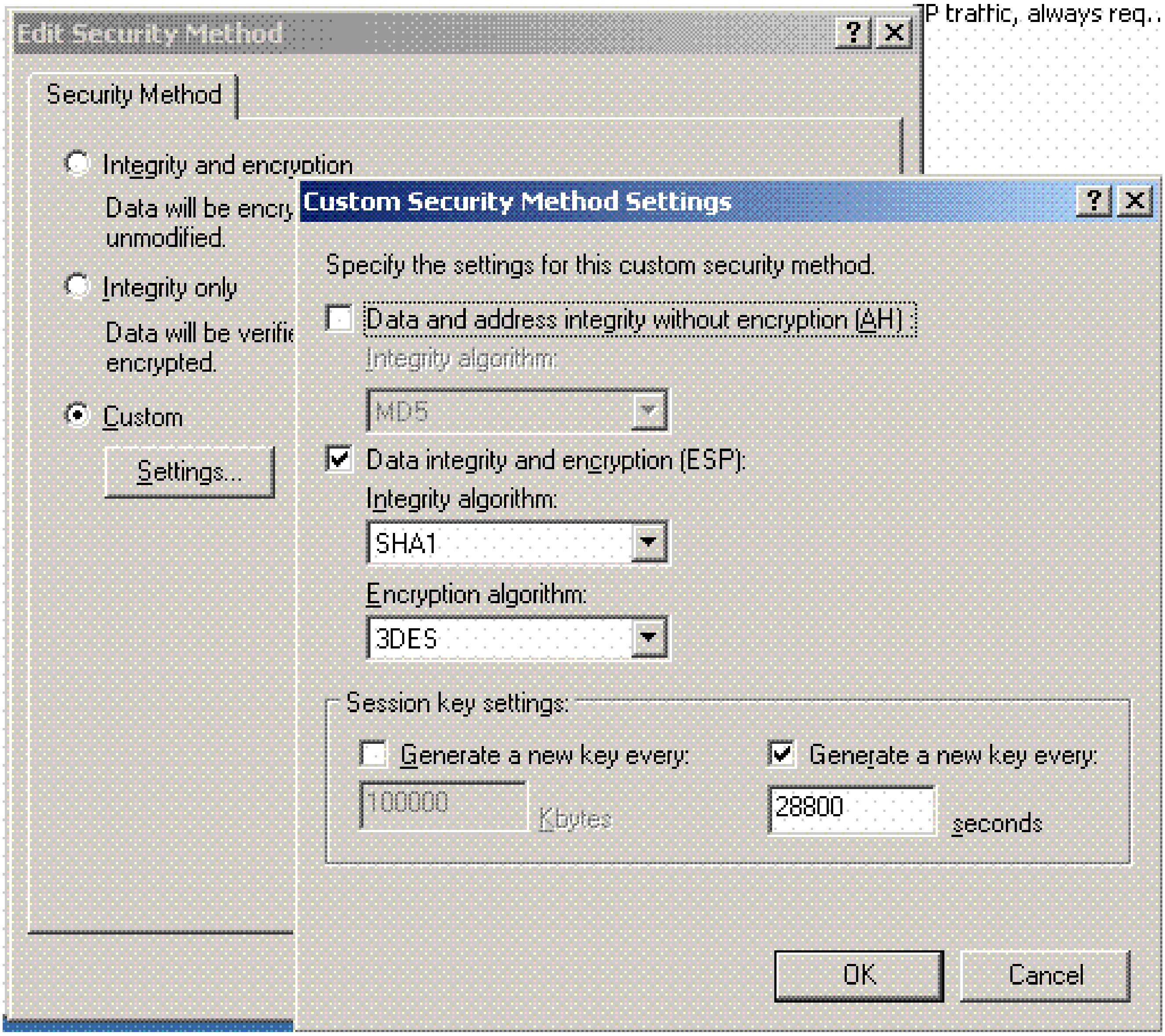
Offer these security methods when negotiating with another computer.

Security method preference order:

| Type | AH Integrity | ESP Confidential... | ES |
|---|---|---|---|
| Custom | <None> | 3DES | SH |
| Custom | <None> | 3DES | MD |
| Custom | <None> | DES | SH |
| Custom | <None> | DES | MD |
| Custom | SHA1 | <None> | <N |
| Custom | MD5 | <None> | <N |

□ Use session key perfect forward secrecy (PFS)

6. 单击**Edit Security Method**，然后单击**Custom** Settings单选按钮。选择这些设置。**注意：**这些设置必须与控制器RADIUS IPSec安全设置匹配。



Edit Security Method

Security Method

○ Integrity and encryption

Data will be encry
unmodified.

○ Integrity only

Data will be verifie
encrypted.

● Custom

Settings...

P traffic, always req...

Custom Security Method Settings

Specify the settings for this custom security method.

□ Data and address integrity without encryption (AH) :

Integrity algorithm:

MD5

☑ Data integrity and encryption (ESP):

Integrity algorithm:

SHA1

Encryption algorithm:

3DES

Session key settings:

□ Generate a new key every:

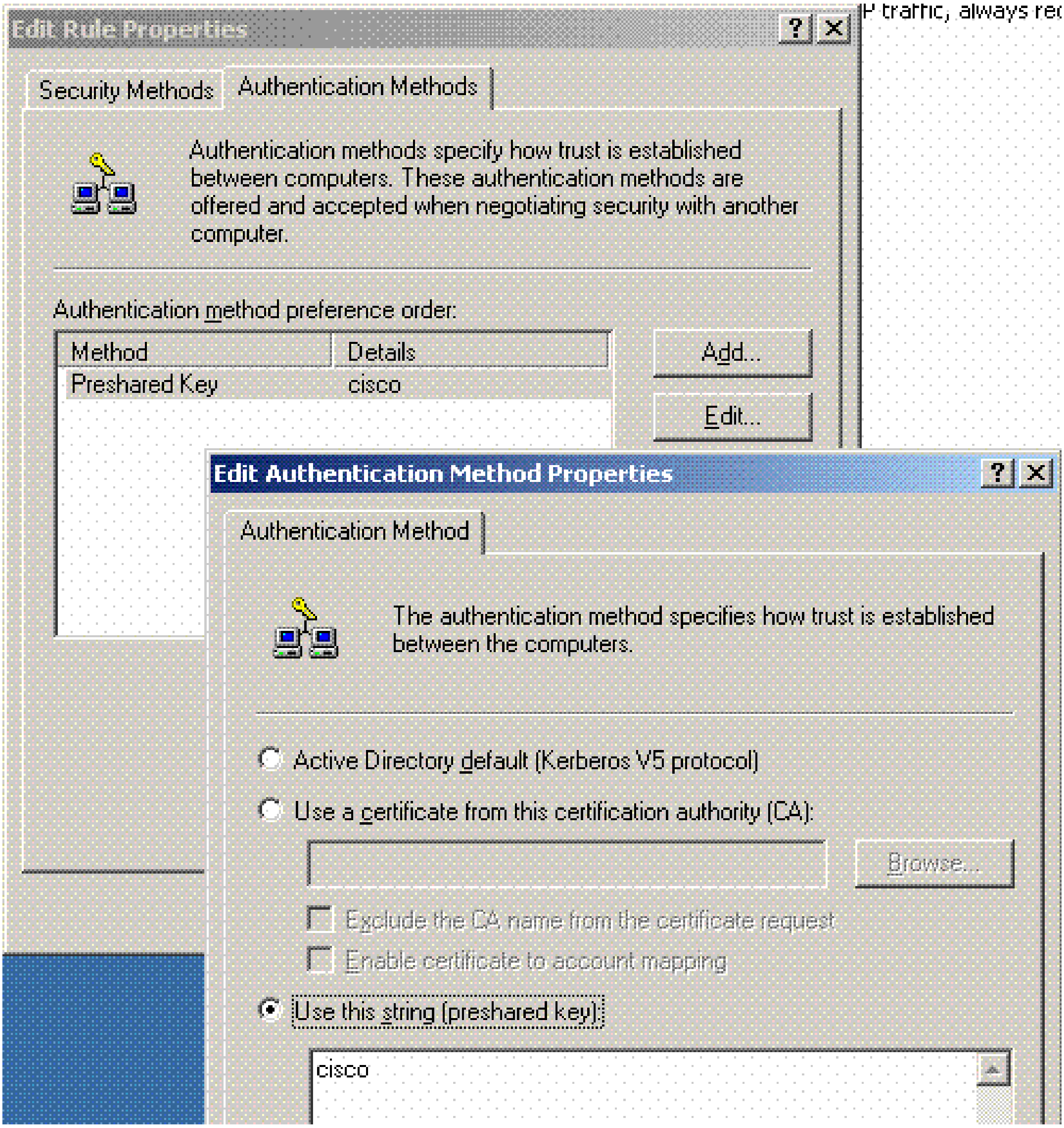
100000 Kbytes

☑ Generate a new key every:

28800 seconds

OK Cancel

7. 点击Edit Rule Properties下的**Authentication Method**选项卡。输入之前在控制器RADIUS配置上输入的共享密钥。


Edit Rule Properties

Security Methods | Authentication Methods

Authentication methods specify how trust is established between computers. These authentication methods are offered and accepted when negotiating security with another computer.

Authentication method preference order:

| Method | Details |
|---|---|
| Preshared Key | cisco |

Edit Authentication Method Properties

Authentication Method

The authentication method specifies how trust is established between the computers.

○ Active Directory default (Kerberos V5 protocol)

○ Use a certificate from this certification authority (CA):

□ Exclude the CA name from the certificate request

□ Enable certificate to account mapping

● Use this string (preshared key):

cisco

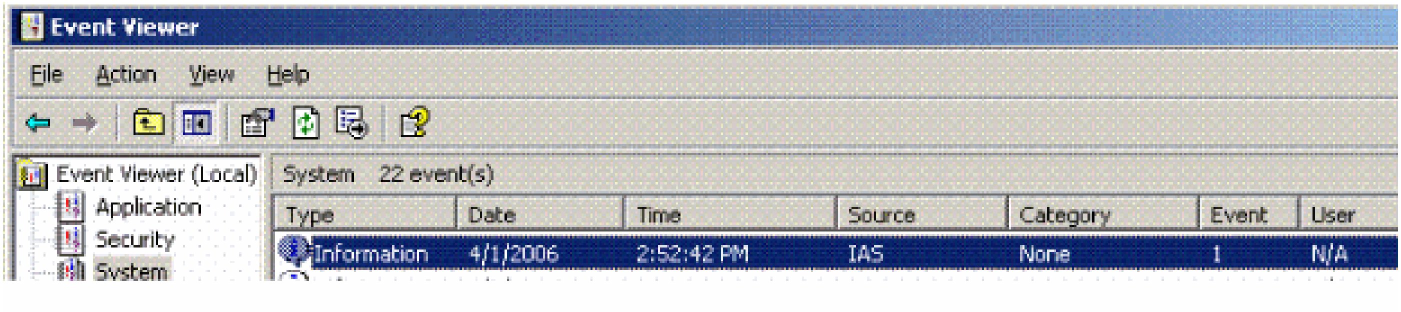
此时，控制器、IAS和域安全设置的所有配置都已完成。保存控制器和WinServer上的所有配置，并重新启动所有计算机。在用于测试的WLAN客户端上，安装根证书并配置WPA2/PEAP。在客户端上安装根证书后，重新启动客户端计算机。在所有计算机重新启动后，将客户端连接到WLAN并捕获这些日志事件。

**注意：**要在控制器和WinServer RADIUS之间设置IPSec连接，需要客户端连接。

## Windows 2003系统日志事件

为启用IPSec RADIUS的WPA2/PEAP配置的WLAN客户端连接成功，将在WinServer上生成以下系统事件：

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

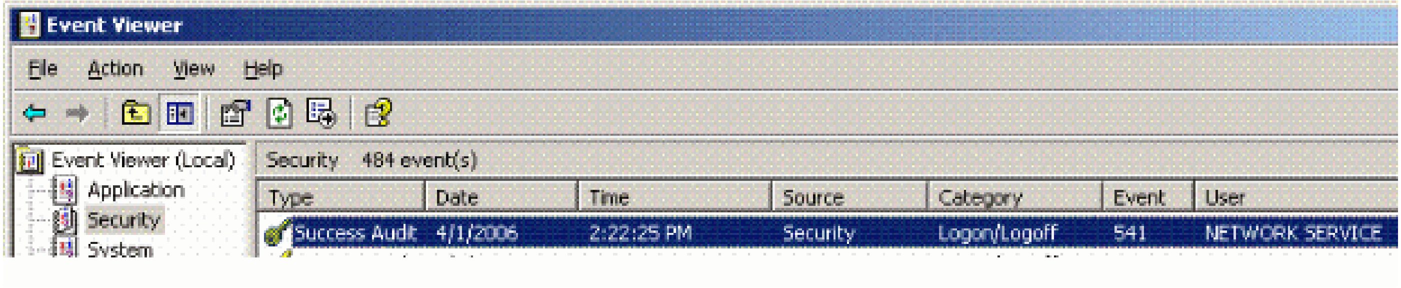


System 22 event(s)

| Type | Date | Time | Source | Category | Event | User |
|---|---|---|---|---|---|---|
| Information | 4/1/2006 | 2:52:42 PM | IAS | None | 1 | N/A |

```
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)
```

成功的控制器<> RADIUS IPSec连接在WinServer日志中生成此安全事件：



Security 484 event(s)

| Type | Date | Time | Source | Category | Event | User |
|---|---|---|---|---|---|---|
| Success Audit | 4/1/2006 | 2:22:25 PM | Security | Logon/Logoff | 541 | NETWORK SERVICE |

```
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
```

## 无线局域网控制器RADIUS IPSec成功调试示例

您可以在控制器上使用debug命令**debug pm ikemsg enable**以验证此配置。下面是一个示例。

```
(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
```

## 种族捕获

这是一个Ethreal Capture示例。

```
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
```

## 相关信息

- Cisco 无线局域网控制器配置指南 5.2 版
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。