

Configuración de la seguridad IPSec de RADIUS para WLCs y Microsoft Windows 2003 IAS Server

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configuración de IPSec RADIUS](#)

[Configurar la WLC](#)

[Configuración de IAS](#)

[Configuración de seguridad del dominio de Microsoft Windows 2003](#)

[Eventos del registro del sistema de Windows 2003](#)

[Ejemplo de Depuración Correcta de RADIUS IPSec del Controlador de LAN Inalámbrica](#)

[Captura de Ethernet](#)

[Información Relacionada](#)

Introducción

Esta guía documenta cómo configurar la función IPSec de RADIUS soportada por WCS y estos controladores WLAN:

- Serie 4400
- WiSM
- 3750 G

La función IPSec de RADIUS del controlador se encuentra en la GUI del controlador en la sección **Seguridad > AAA > Servidores de autenticación RADIUS**. La característica proporciona un método para cifrar todas las comunicaciones RADIUS entre los controladores y los servidores RADIUS (IAS) con IPSec.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento sobre LWAPP
- Conocimientos sobre autenticación RADIUS e IPSec

- Conocimientos sobre cómo configurar servicios en el sistema operativo Windows 2003 Server

Componentes Utilizados

Estos componentes de red y software se deben instalar y configurar para implementar la función IPsec de RADIUS del controlador:

- Controladores WLC 4400, WiSM o 3750G. Este ejemplo utiliza el WLC 4400 que ejecuta la versión de software 5.2.178.0
- Puntos de acceso ligeros (LAP). Este ejemplo utiliza el LAP de la serie 1231.
- Switch con DHCP
- Servidor de Microsoft 2003 configurado como controlador de dominio instalado con la Autoridad de certificados de Microsoft y con el Servicio de autenticación de Internet (IAS) de Microsoft.
- Microsoft Domain Security
- Adaptador de cliente inalámbrico 802.11 a/b/g de Cisco con ADU versión 3.6 configurado con WPA2/PEAP

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte [Convenciones de Consejos Técnicos Cisco para obtener más información sobre las convenciones del documento.](#)

Configuración de IPsec RADIUS

Esta guía de configuración no aborda la instalación o configuración de Microsoft WinServer, Certificate Authority, Active Directory o cliente WLAN 802.1x. Estos componentes deben instalarse y configurarse antes de implementar la función Controller IPsec RADIUS. El resto de esta guía documenta cómo configurar IPsec RADIUS en estos componentes:

1. Controladores WLAN de Cisco
2. Windows 2003 IAS
3. Configuración de seguridad de dominio de Microsoft Windows

Configurar la WLC

Esta sección explica cómo configurar IPsec en el WLC a través de la GUI.

Complete estos pasos desde la GUI del controlador.

1. Navegue hasta la pestaña **Security > AAA > RADIUS Authentication** en la GUI del controlador y agregue un nuevo servidor RADIUS.

CISCO SYSTEMS

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT

Security

AAA

- General
- RADIUS Authentication
- RADIUS Accounting
- Local Net Users
- MAC Filtering
- Disabled Clients
- User Login Policies
- AP Policies

Access Control Lists

IPSec Certificates

- CA Certificate
- ID Certificate

RADIUS Authentication Servers

Call Station ID Type

Credentials Caching

Use AES Key Wrap

Network User	Management	Server Index	Server Address	Port	IPSec
<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	192.168.30.10	1812	Disabled
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3	192.168.30.105	1812	Enabled

2. Configure la dirección IP, el puerto 1812 y un secreto compartido del nuevo servidor RADIUS. Marque la casilla de verificación **IPSec Enable**-, configure estos parámetros IPSec y, a continuación, haga clic en **Apply**.**Nota:** El secreto compartido se utiliza para autenticar el servidor RADIUS y como clave precompartida (PSK) para la autenticación IPSec.

CISCO SYSTEMS

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT

Security

AAA

- General
- RADIUS Authentication
- RADIUS Accounting
- Local Net Users
- MAC Filtering
- Disabled Clients
- User Login Policies
- AP Policies

Access Control Lists

IPSec Certificates

- CA Certificate
- ID Certificate

Web Auth Certificate

Wireless Protection Policies

- Trusted AP Policies
- Rogue Policies
- Standard Signatures
- Custom Signatures
- Client Exclusion Policies
- AP Authentication

Shared Secret

Confirm Shared Secret

Key Wrap

Port Number

Server Status

Support for RFC 3576

Retransmit Timeout seconds

Network User Enable

Management Enable

IPSec Enable

IPsec Parameters

IPSec

IPSEC Encryption

(Shared Secret will be used as the Preshared Key)

IKE Phase 1

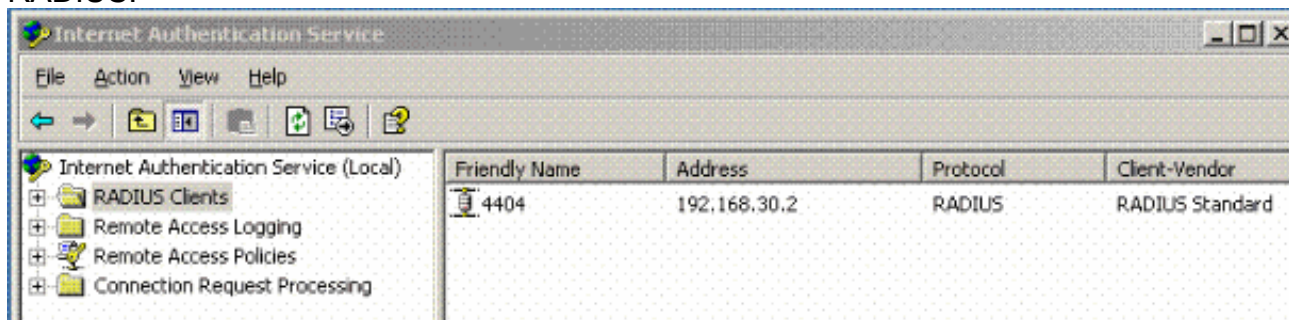
Lifetime (seconds)

IKE Diffie Hellman Group

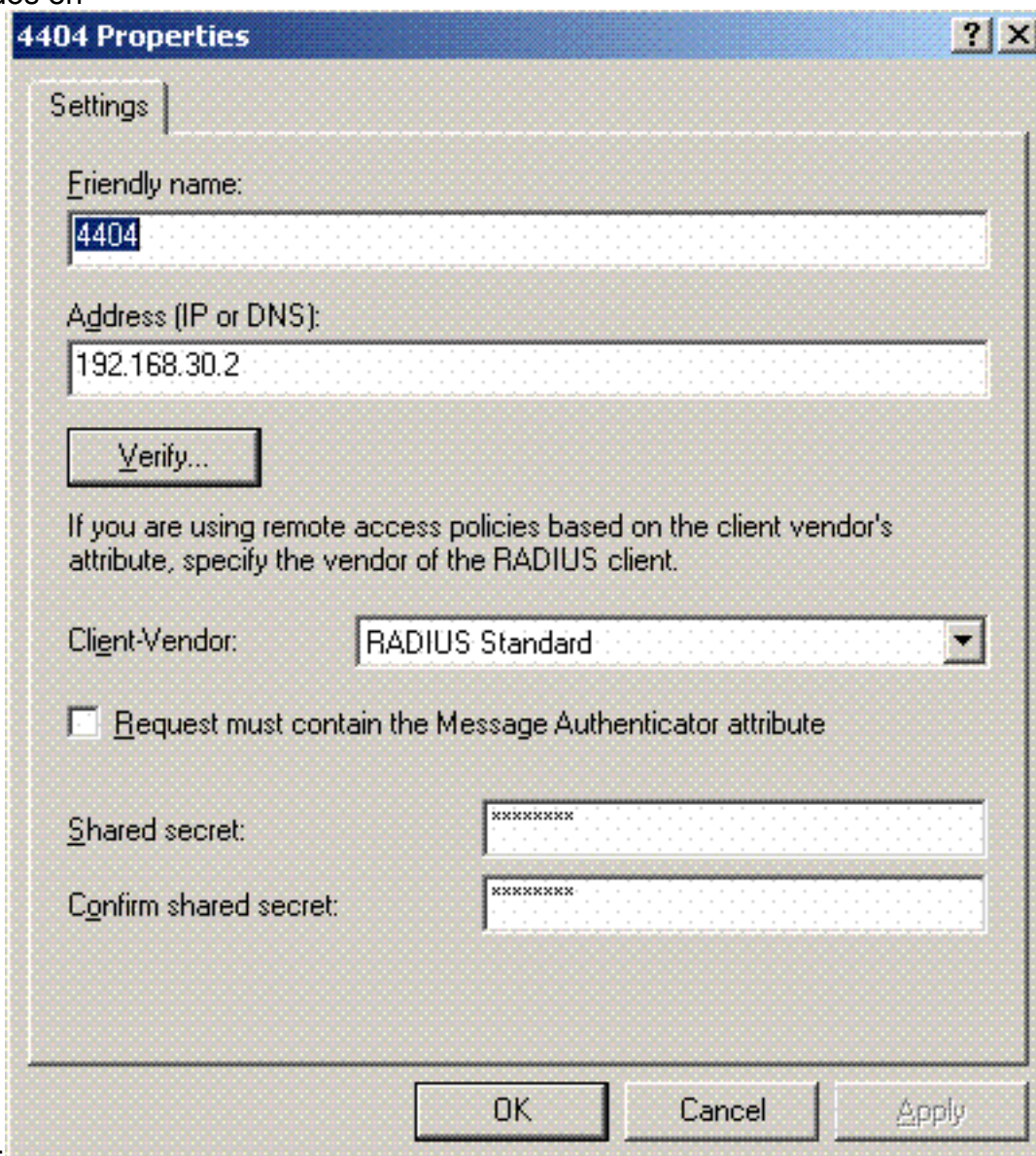
Configuración de IAS

Complete estos pasos en el IAS:

1. Desplácese hasta el administrador IAS en Win2003 y agregue un nuevo cliente RADIUS.



2. Configure las propiedades del cliente RADIUS con la dirección IP y el secreto compartido configurados en



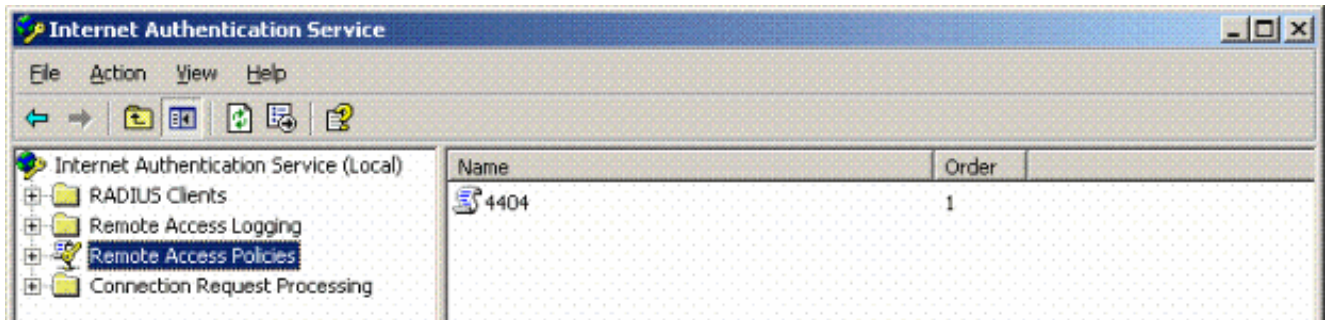
The screenshot shows the '4404 Properties' dialog box. The 'Settings' tab is active. The fields are filled with the following information:

- Friendly name: 4404
- Address (IP or DNS): 192.168.30.2
- Client-Vendor: RADIUS Standard
- Request must contain the Message Authenticator attribute:
- Shared secret: [Redacted]
- Confirm shared secret: [Redacted]

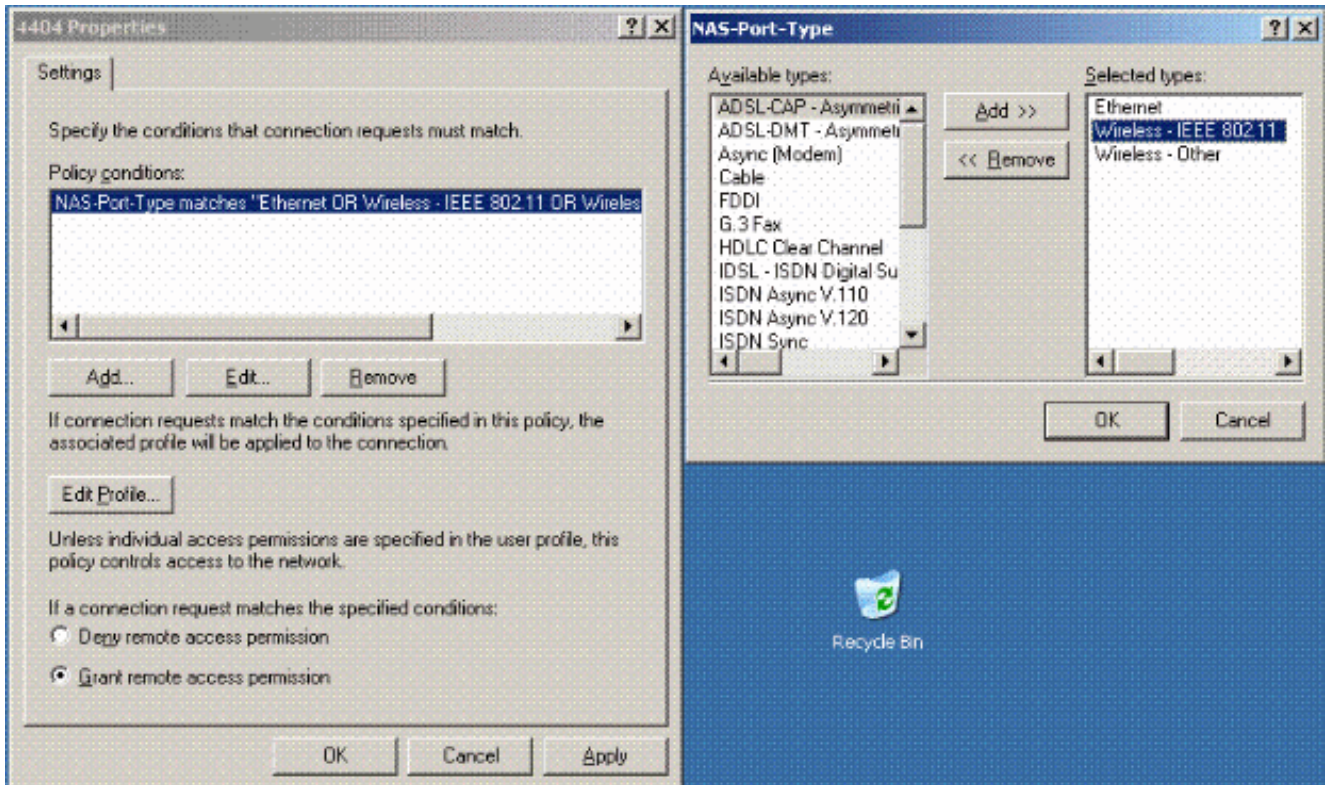
Buttons at the bottom: OK, Cancel, Apply.

Controller:

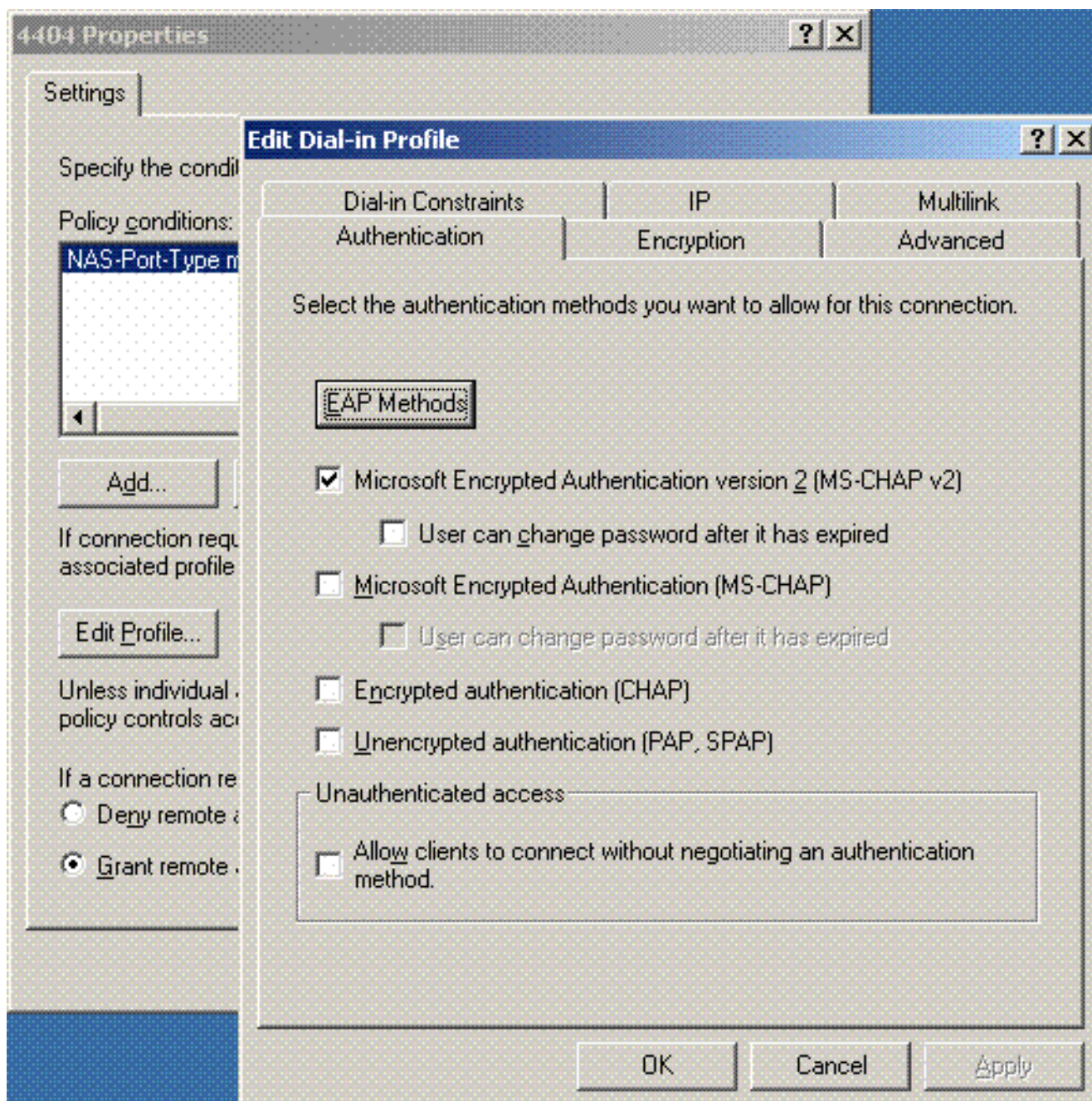
3. Configurar una nueva directiva de acceso remoto para el controlador:



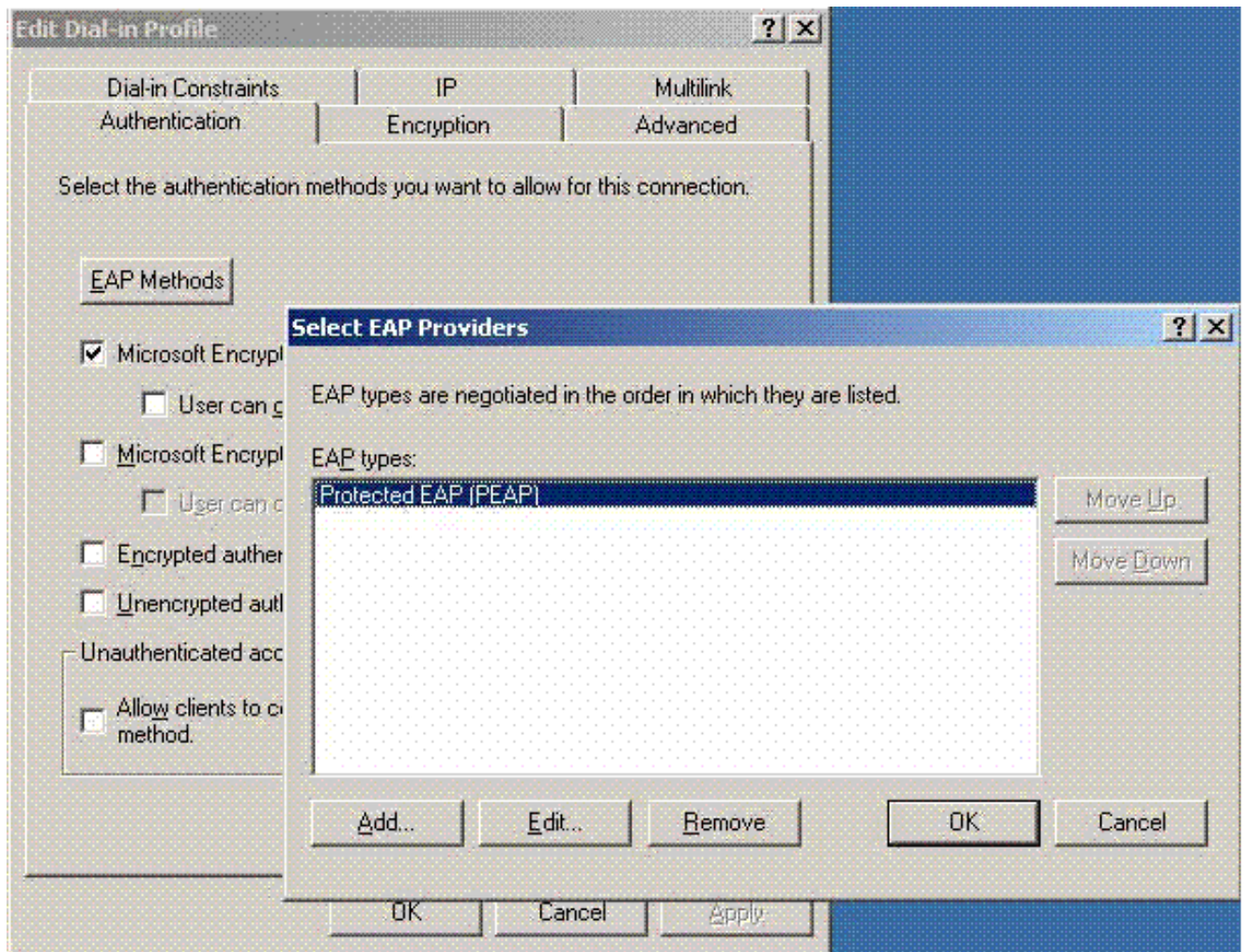
4. Edite las propiedades de la directiva de acceso remoto del controlador. Asegúrese de agregar el tipo de puerto NAS - Wireless - IEEE 802.11:



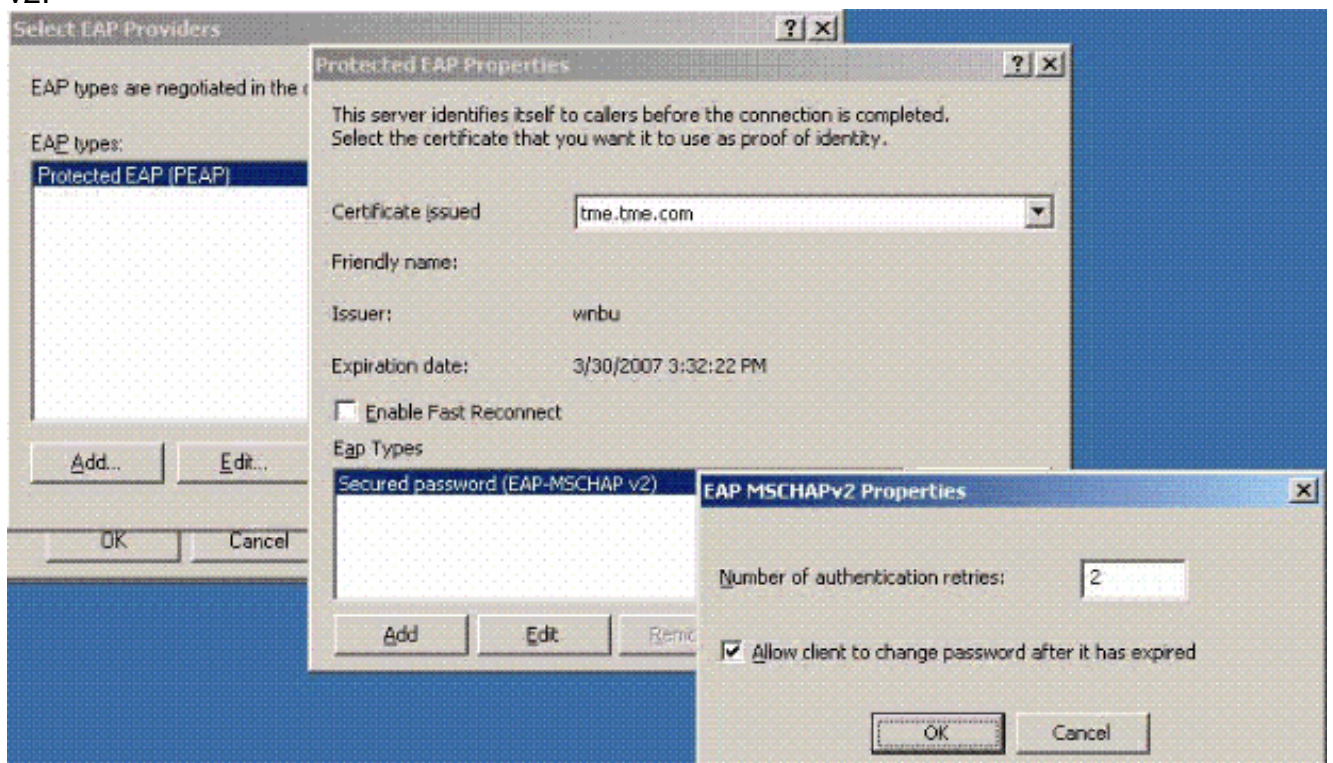
5. Haga clic en **Edit Profile**, haga clic en la pestaña **Authentication** y verifique MS-CHAP v2 for Authentication:



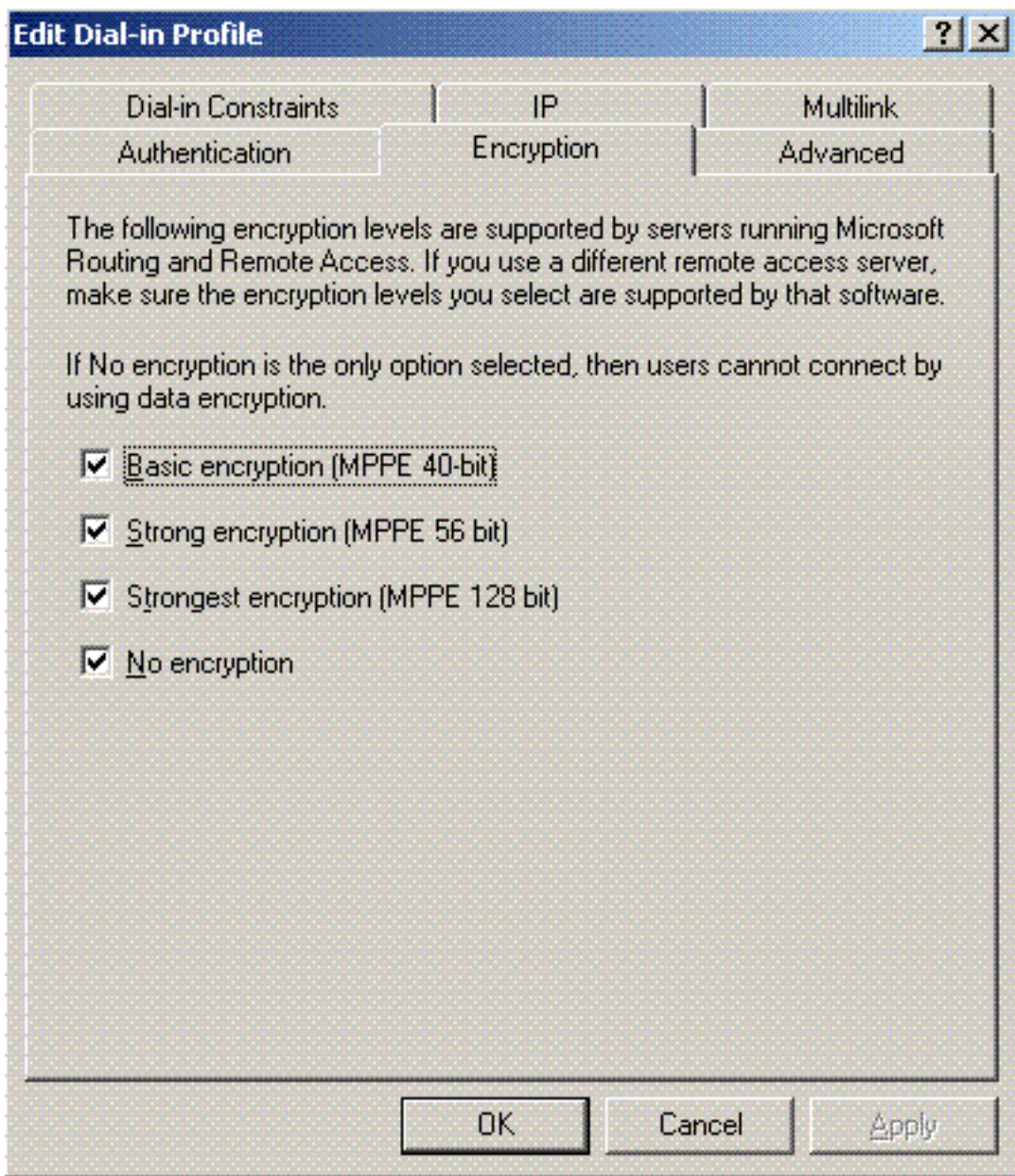
6. Haga clic en **Métodos EAP**, seleccione Proveedores EAP y agregue PEAP como un tipo EAP:



7. Haga clic en **Edit** en Select EAP Providers y elija en el menú desplegable el servidor asociado con sus cuentas de usuario y CA de Active Directory (por ejemplo, tme.tme.com). Agregue el tipo de EAP MSCHAP v2:

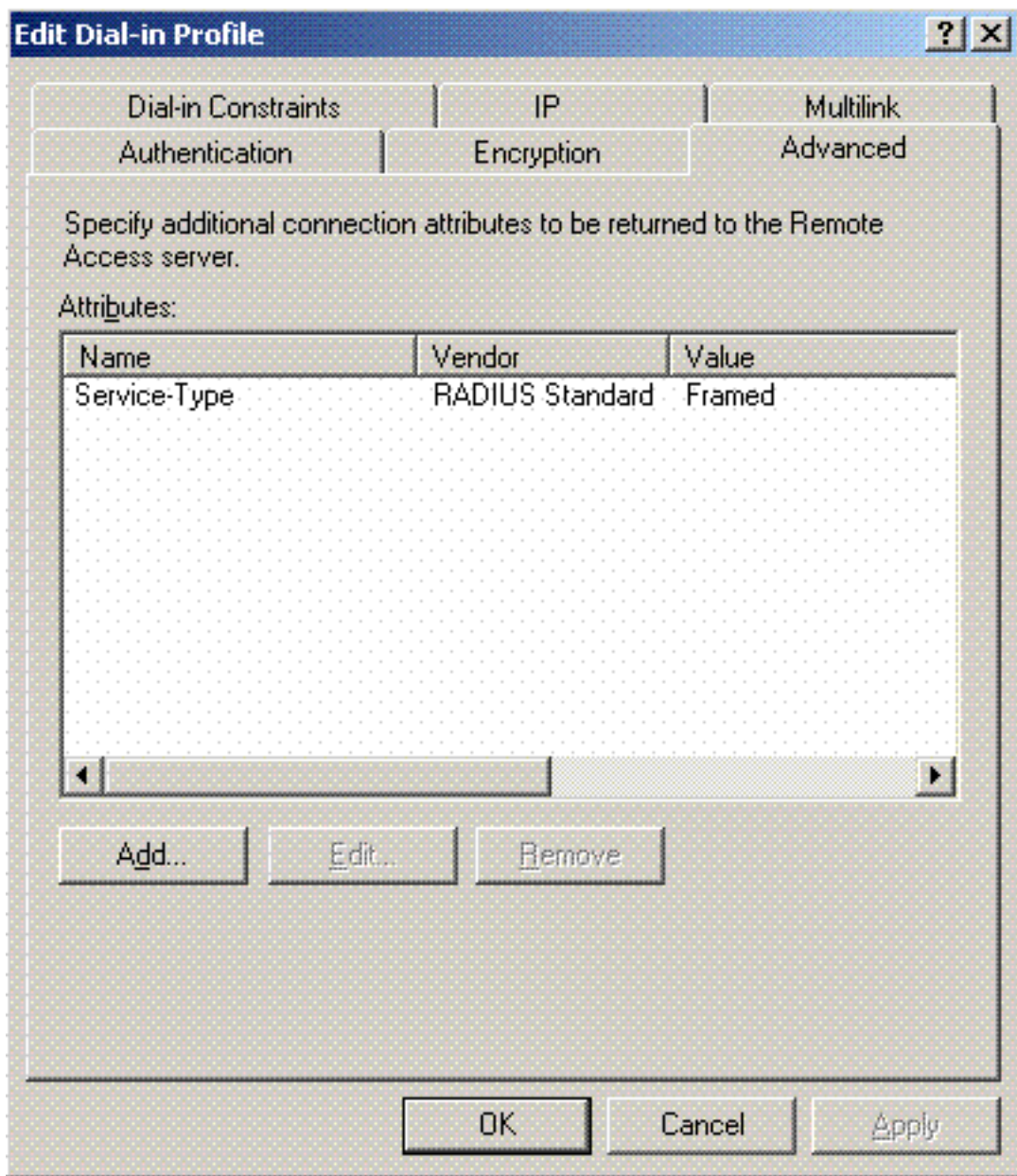


8. Haga clic en la pestaña **Encryption** y verifique todos los tipos de cifrado para el acceso



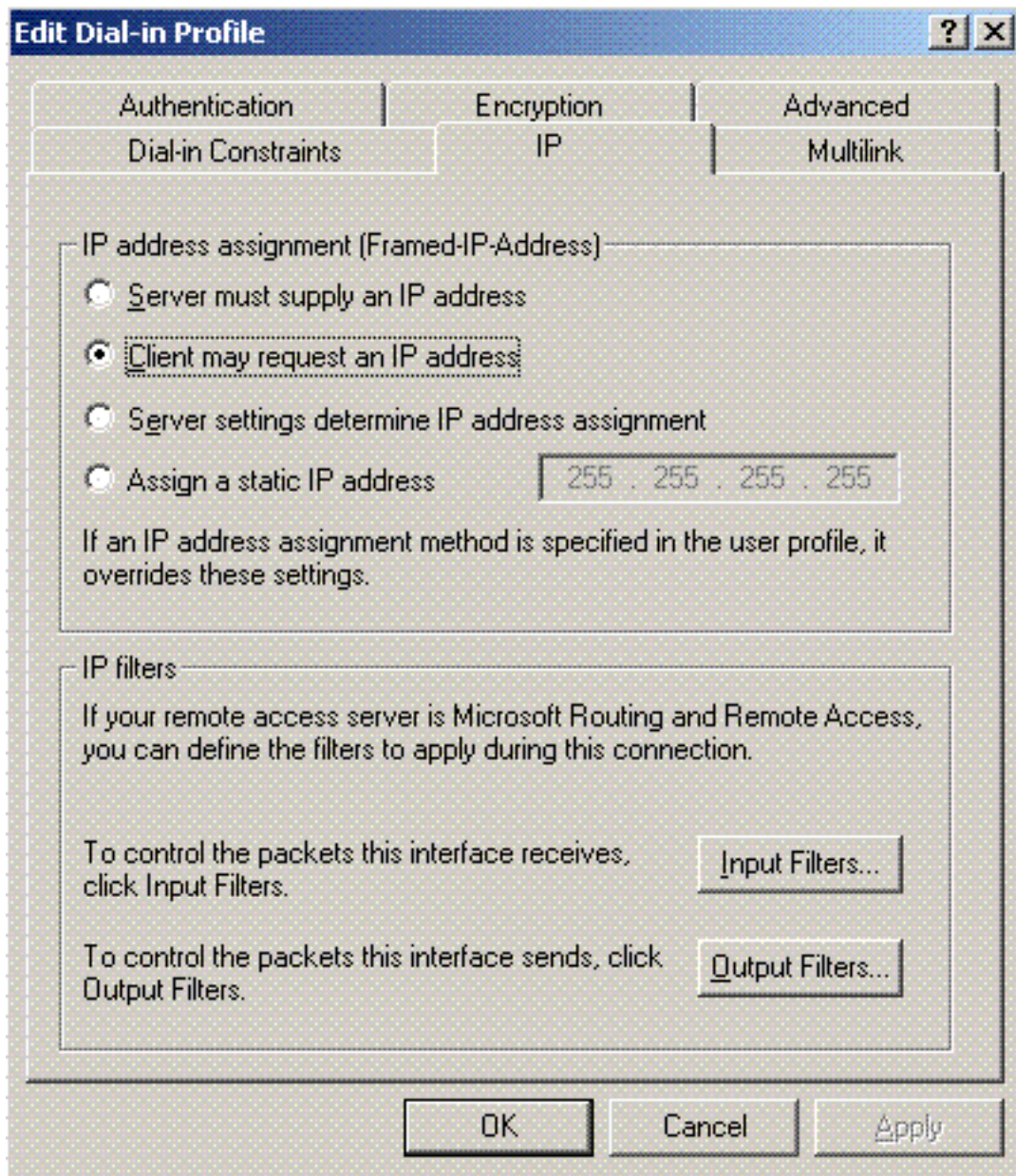
remoto:

9. Haga clic en la pestaña **Advanced** y agregue RADIUS Standard/Framed como Service-



Type:

10. Haga clic en la pestaña **IP** y marque **El cliente puede solicitar una dirección IP**. Esto supone que tiene DHCP habilitado en un switch o

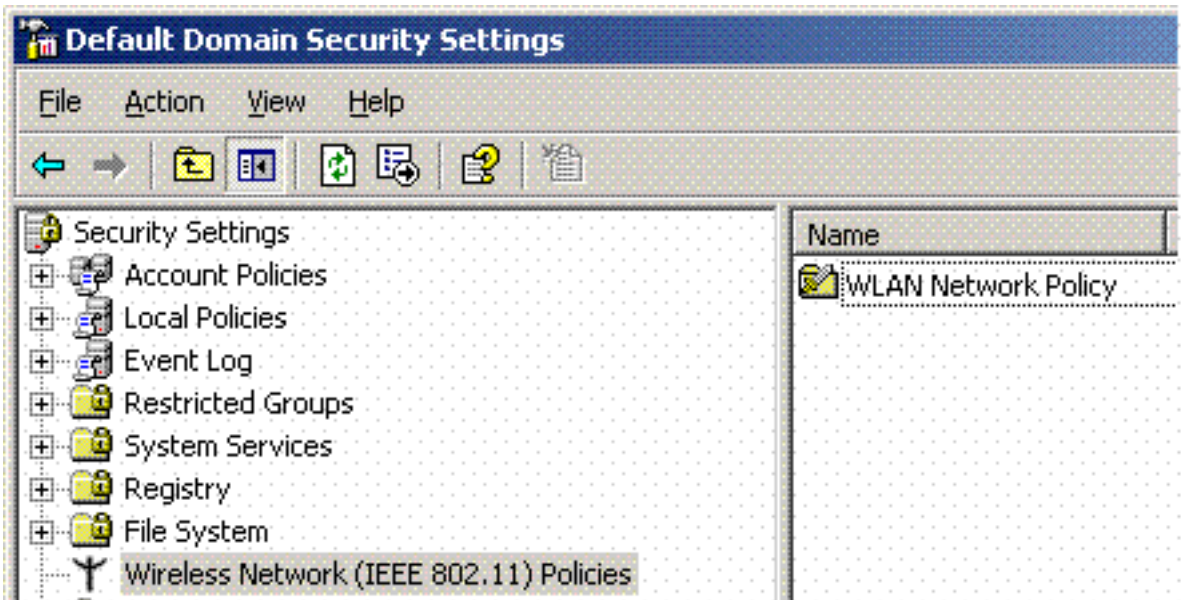


WinServer.

[Configuración de seguridad del dominio de Microsoft Windows 2003](#)

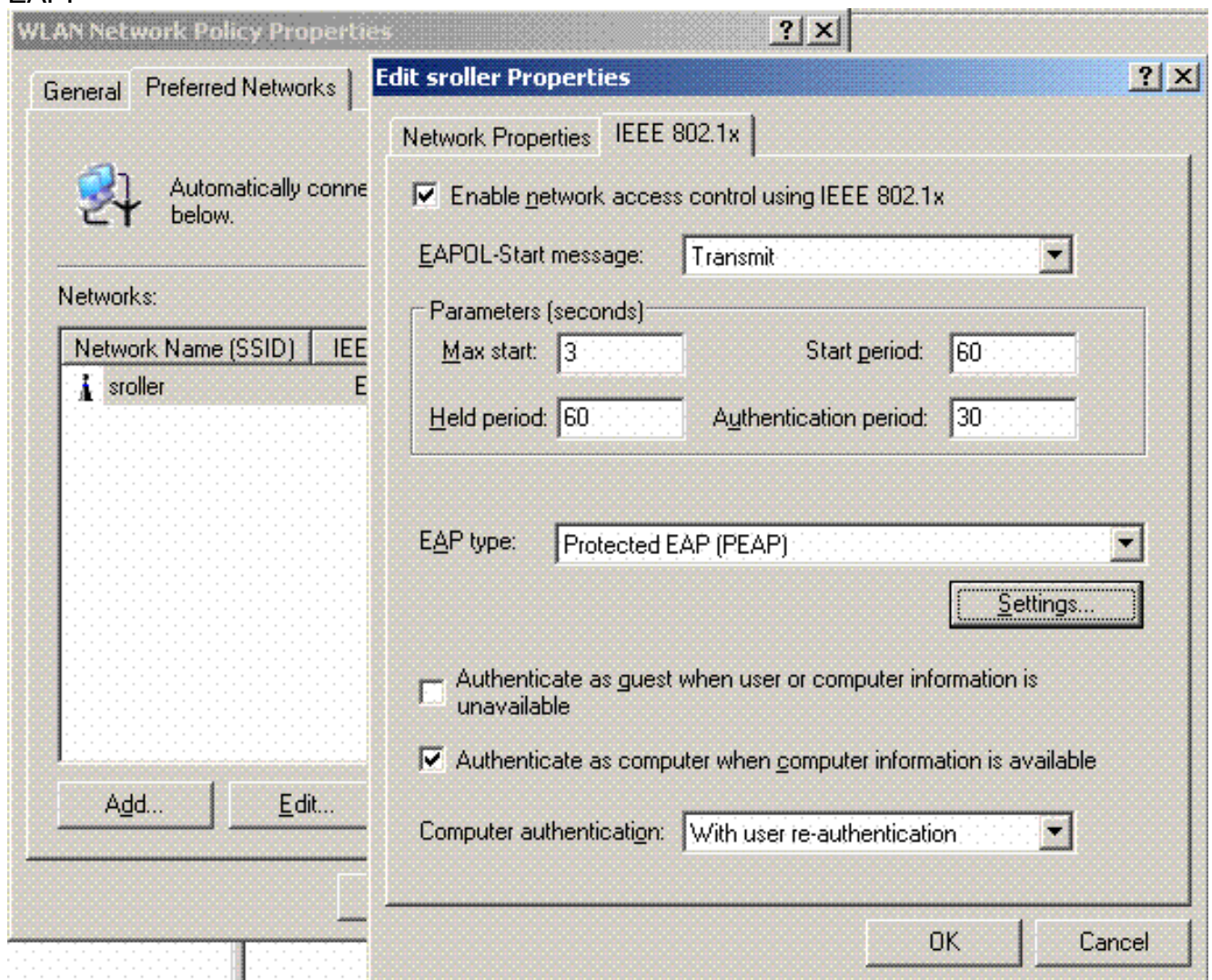
Complete estos pasos para configurar las configuraciones de seguridad de dominio de Windows 2003:

1. Inicie el Administrador de configuración de seguridad de dominio predeterminada y cree una nueva directiva de seguridad para Directivas de red inalámbrica (IEEE



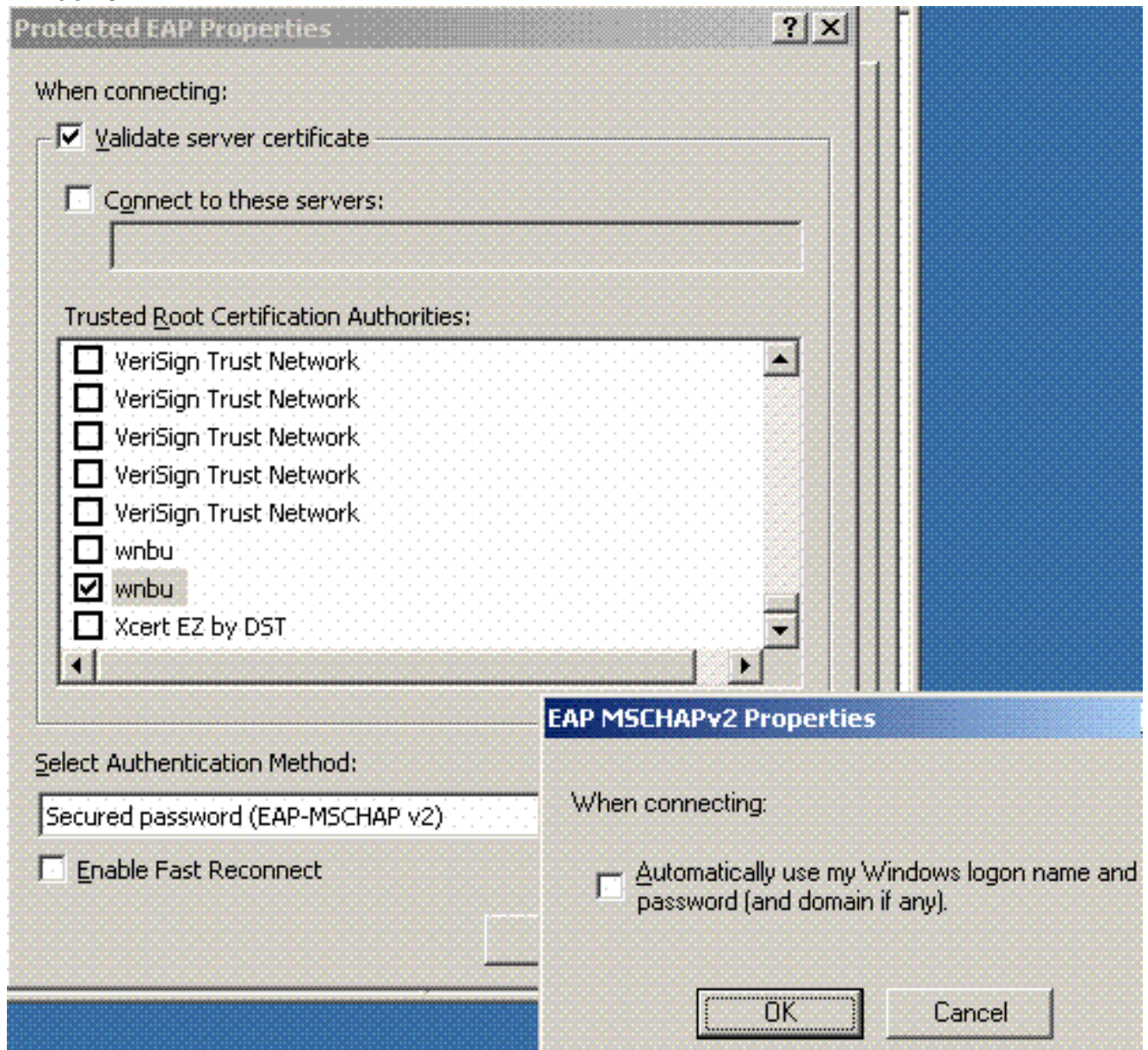
802.11).

- Abra Propiedades de directiva de red WLAN y haga clic en **Redes preferidas**. Agregue una nueva WLAN preferida y escriba el nombre de su WLAN SSID, como `wireless`. Haga doble clic en la nueva red preferida y, a continuación, haga clic en la ficha **IEEE 802.1x**. Elija PEAP como tipo de EAP:

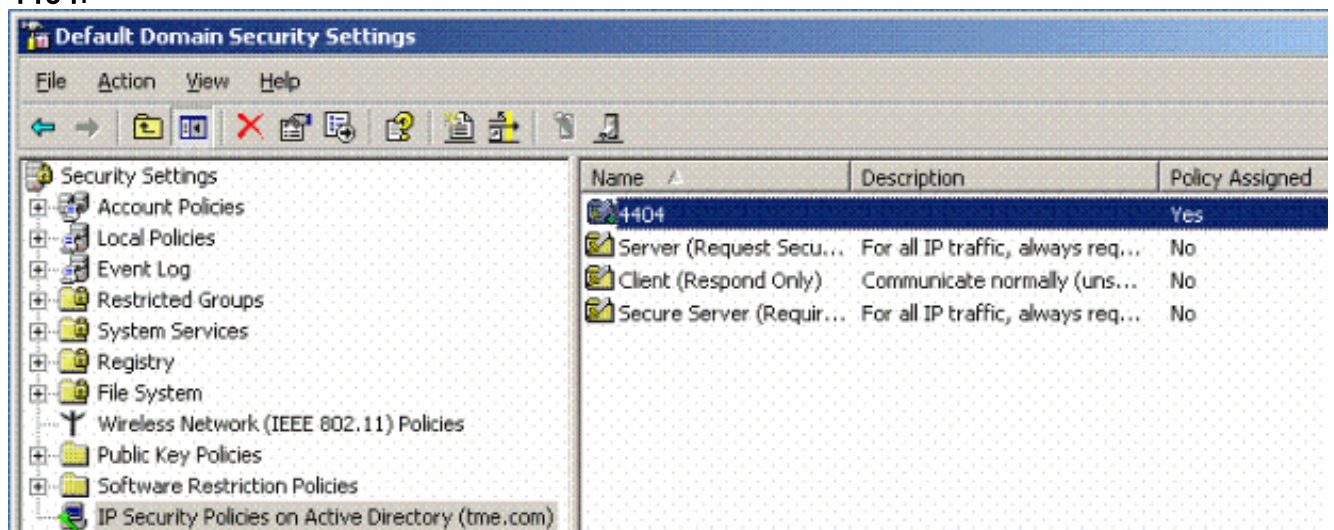


- Haga clic en **Configuración PEAP**, marque **Validar certificado de servidor** y seleccione el Certificado raíz de confianza instalado en la Autoridad de certificación. Para realizar pruebas, desactive la casilla MS CHAP v2 para Usar automáticamente mi inicio de sesión y

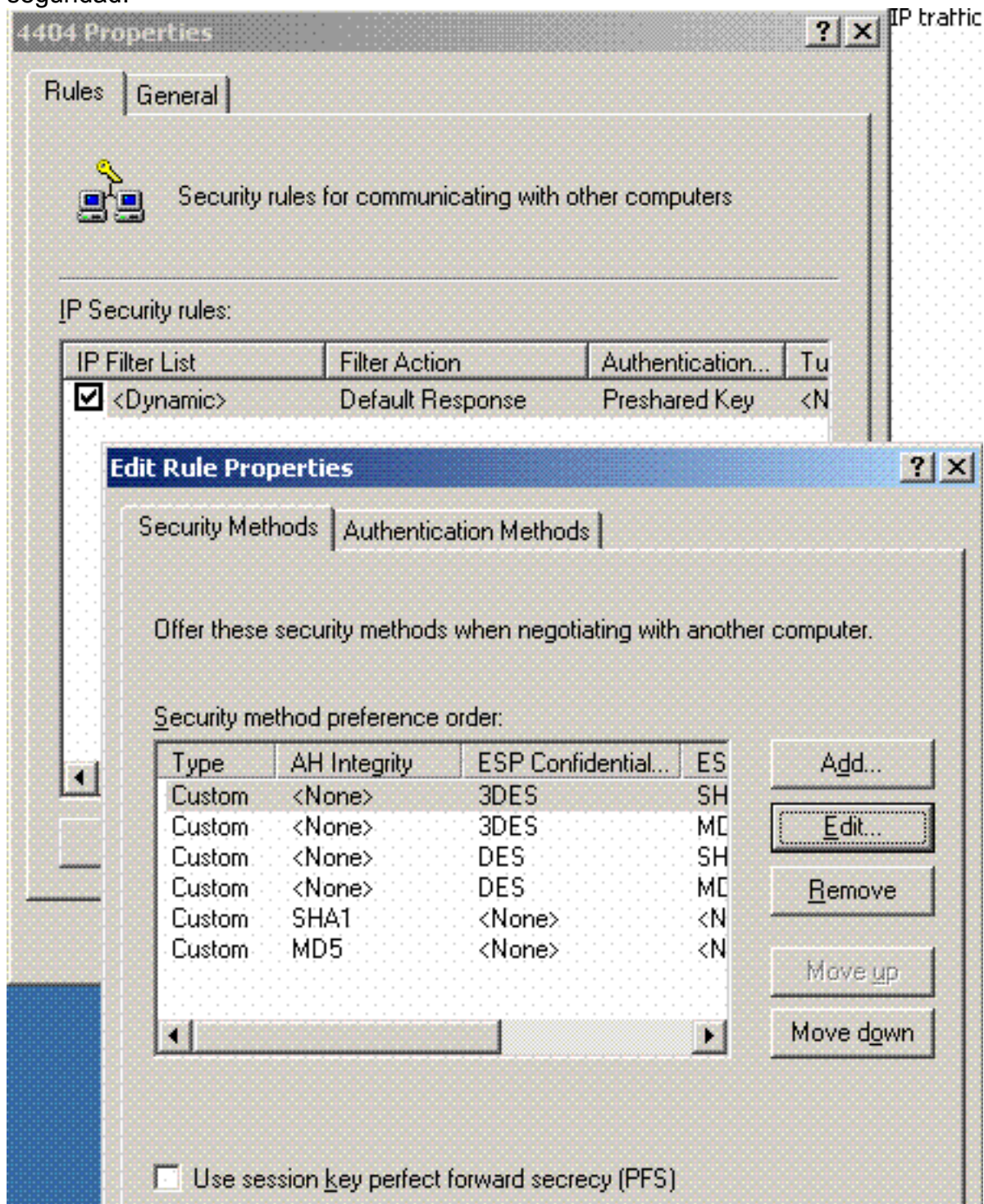
contraseña de Windows.



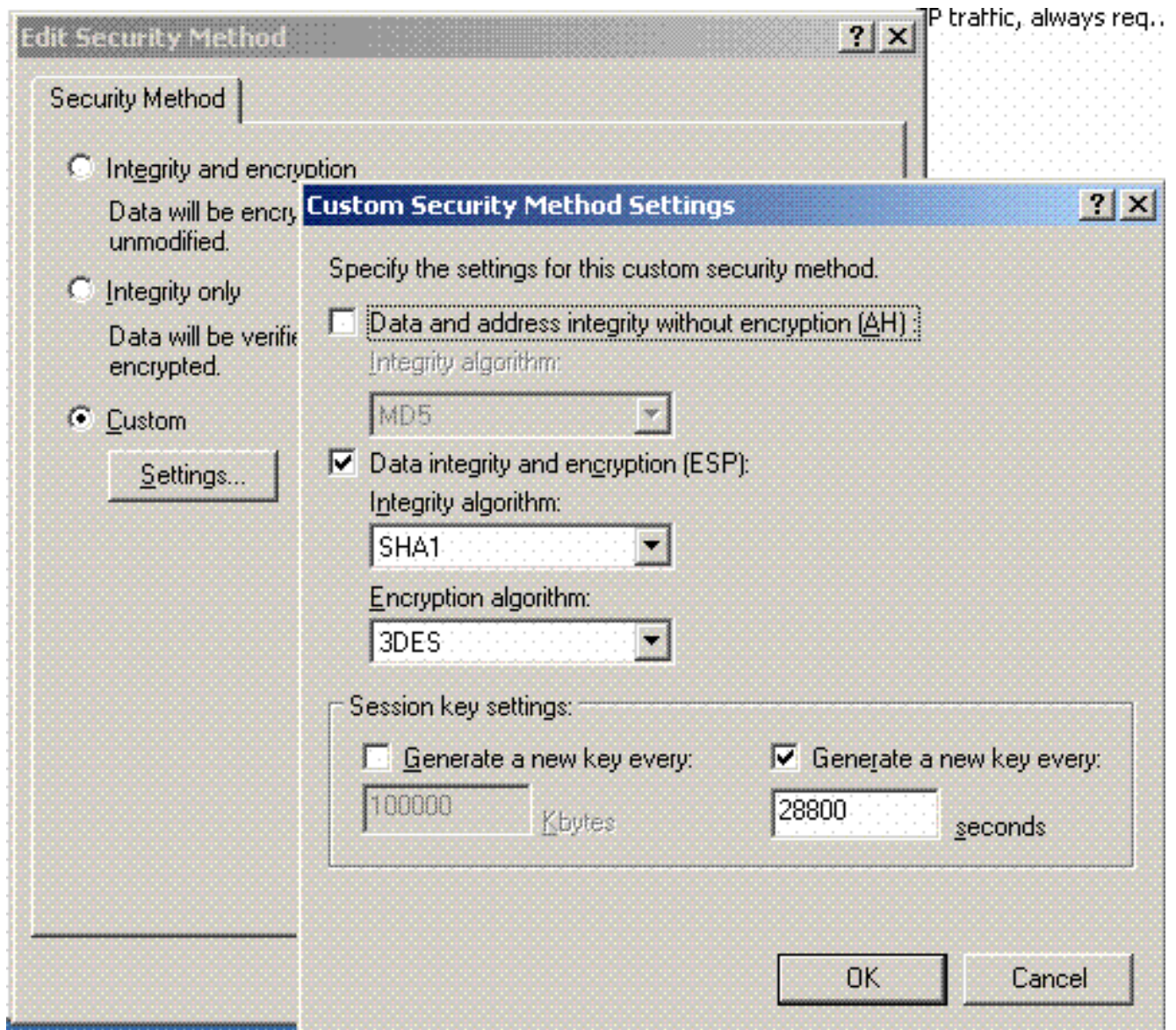
4. En la ventana Administrador de configuración de seguridad de dominio predeterminada de Windows 2003, cree otras directivas de seguridad IP nuevas en la directiva de Active Directory, como 4404.



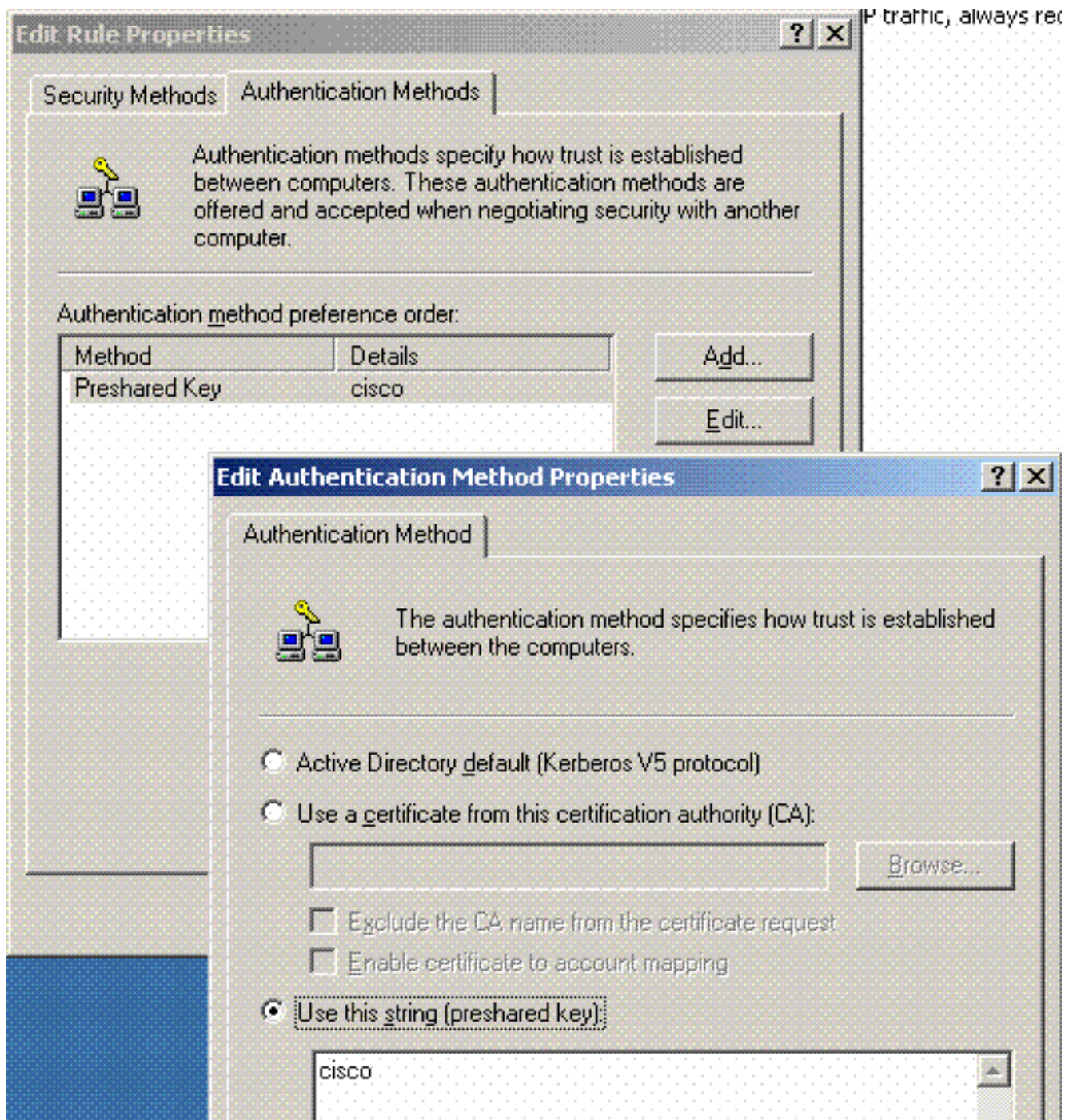
5. Edite las nuevas propiedades de la directiva 4404 y haga clic en la pestaña **Reglas**. Agregar una nueva regla de filtrado: lista de filtros IP (dinámica); acción de filtro (respuesta predeterminada); autenticación (PSK); túnel (ninguno). Haga doble clic en la regla de filtro recién creada y seleccione Métodos de seguridad:



6. Haga clic en **Edit Security Method** y en el botón de opción **Custom Settings**. Seleccione esta configuración. **Nota:** Estos parámetros deben coincidir con los parámetros de seguridad IPsec de RADIUS del controlador.



7. Haga clic en la pestaña **Método de autenticación** en Editar propiedades de regla. Introduzca el mismo secreto compartido que introdujo anteriormente en la configuración RADIUS del controlador.



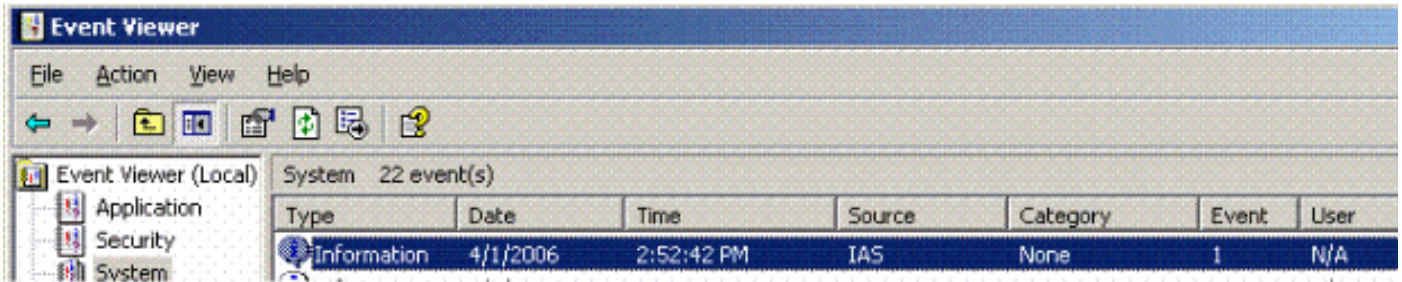
Llegados a este punto, se completan todas las configuraciones de Controller, IAS y Domain Security Settings. Guarde todas las configuraciones en Controller y WinServer y reinicie todas las máquinas. En el cliente WLAN que se utiliza para la prueba, instale el certificado raíz y configure para WPA2/PEAP. Una vez instalado el certificado raíz en el cliente, reinicie el equipo cliente. Después de que todas las máquinas se reinicien, conecte el cliente a la WLAN y capture estos eventos de registro.

Nota: se requiere una conexión de cliente para configurar la conexión IPsec entre Controller y WinServer RADIUS.

[Eventos del registro del sistema de Windows 2003](#)

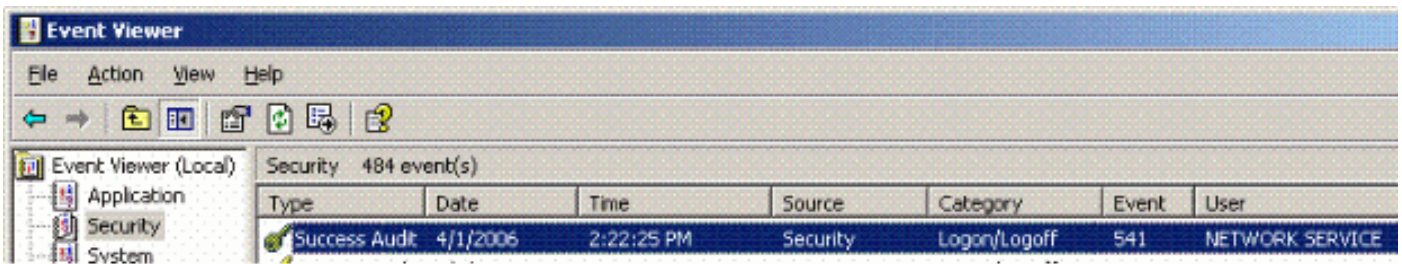
Una conexión de cliente WLAN correcta configurada para WPA2/PEAP con IPsec RADIUS habilitado genera este evento de sistema en WinServer:

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)

Una conexión IPsec RADIUS del controlador <> correcta genera este evento de seguridad en los registros de 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
```

[Ejemplo de Depuración Correcta de RADIUS IPsec del Controlador de LAN Inalámbrica](#)

Puede utilizar el comando debug **debug pm ikemsg enable** en el controlador para verificar esta configuración. Aquí está un ejemplo.

```
(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 1292aecf
VID: vendor id[16] = 0x4485152d 18b6bbcd 0be8a846 9579ddcc
VID: vendor id[16] = 0xcd604643 35df21f8 7cfd2b2fc 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] = 0xcfc0bbd1c 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 Rcookie=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 Rcookie=0x064bdcaf50d5f555
ID: packet[8] = 0x01000000 c0a81e69
HASH: hash[20] = 0x3b26e590 66651f13 2a86f62d 1bd1e71 064b43f6
TX QM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rcookie=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 Rcookie=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 Rcookie=0x064bdcaf50d5f555 msgid=0x73915967
HASH: hash[20] = 0x0e81093e bc26ebf3 d367297c d9f7c000 28a3662d
RX QM: 192.168.30.2 (Initiator) <-> 192.168.30.105 Icookie=0xaac8841687148dda Rcookie=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
```

[Captura de Ethernet](#)

Esta es una muestra de la captura de Ethernet.

```
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
```

[Información Relacionada](#)

- [Guía de configuración del controlador inalámbrico de LAN de Cisco, versión 5.2](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).