Configuración RADIUS seguridad IPSec para el WLCs y el servidor IAS de Microsoft Windows 2003

Contenido

Introducción

Documentos de esta guía cómo configurar la característica del IPSec RADIUS soportada por el WCS y estos controladores de WLAN:

- 4400 Series
- WiSM
- 3750G

La característica del IPSec del regulador RADIUS está situada en el regulador GUI bajo **Seguridad >AAA >** sección de los **servidores de autenticación de RADIUS**. La característica proporciona un método para que usted cifre todas las comunicaciones RADIUS entre los reguladores y los servidores de RADIUS (IAS) con el IPSec.

prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento en el LWAPP
- Conocimiento en la autenticación de RADIUS y el IPSec

- Conocimiento en cómo configurar los servicios en el sistema operativo del servidor de Windows 2003

Componentes Utilizados

Este la red y los componentes del software se deben instalar y configurar para desplegar la característica del IPSec del regulador RADIUS:

- WLC 4400, WiSM, o reguladores 3750G. Este ejemplo utiliza el WLC 4400 que funciona con la versión de software 5.2.178.0
- Puntos de acceso ligeros (revestimientos). Este ejemplo utiliza el REVESTIMIENTO de las 1231 Series.
- Switch con el DHCP
- Servidor de Microsoft 2003 configurado como controlador de dominio instalado con Microsoft Certificate Authority y con el Internet Authentication Service de Microsoft (IAS).
- Seguridad del dominio de Microsoft
- Adaptador de red inalámbrica de cliente del a/b/g del 802.11 de Cisco con la versión de ADU 3.6 configurada 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). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Configuración de RADIUS del IPSec

Esta guía de configuración no dirige la instalación o la configuración cliente del 802.1x de Microsoft WinServer, del Certificate Authority, del Active Directory o de la red inalámbrica (WLAN). Estos componentes se deben instalar y configurar antes del despliegue de la característica del IPSec RADIUS del regulador. El resto de los documentos de esta guía cómo configurar el IPSec RADIUS en estos componentes:

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

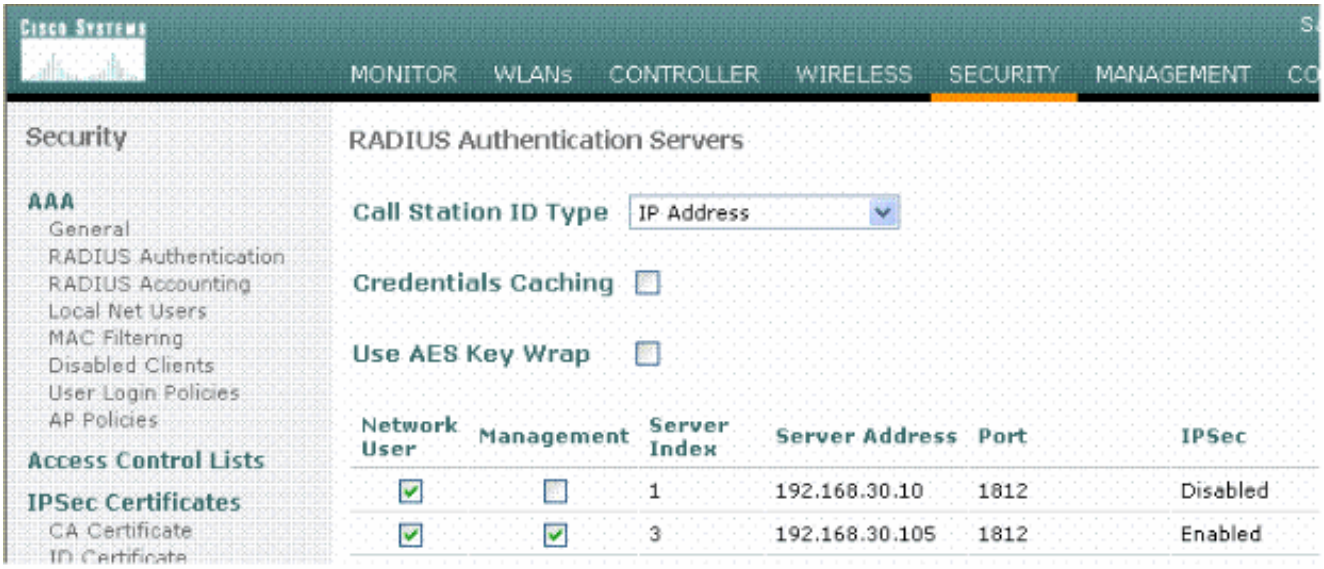
Configure el WLC

Esta sección explica cómo configurar el IPSec en el WLC con el GUI.

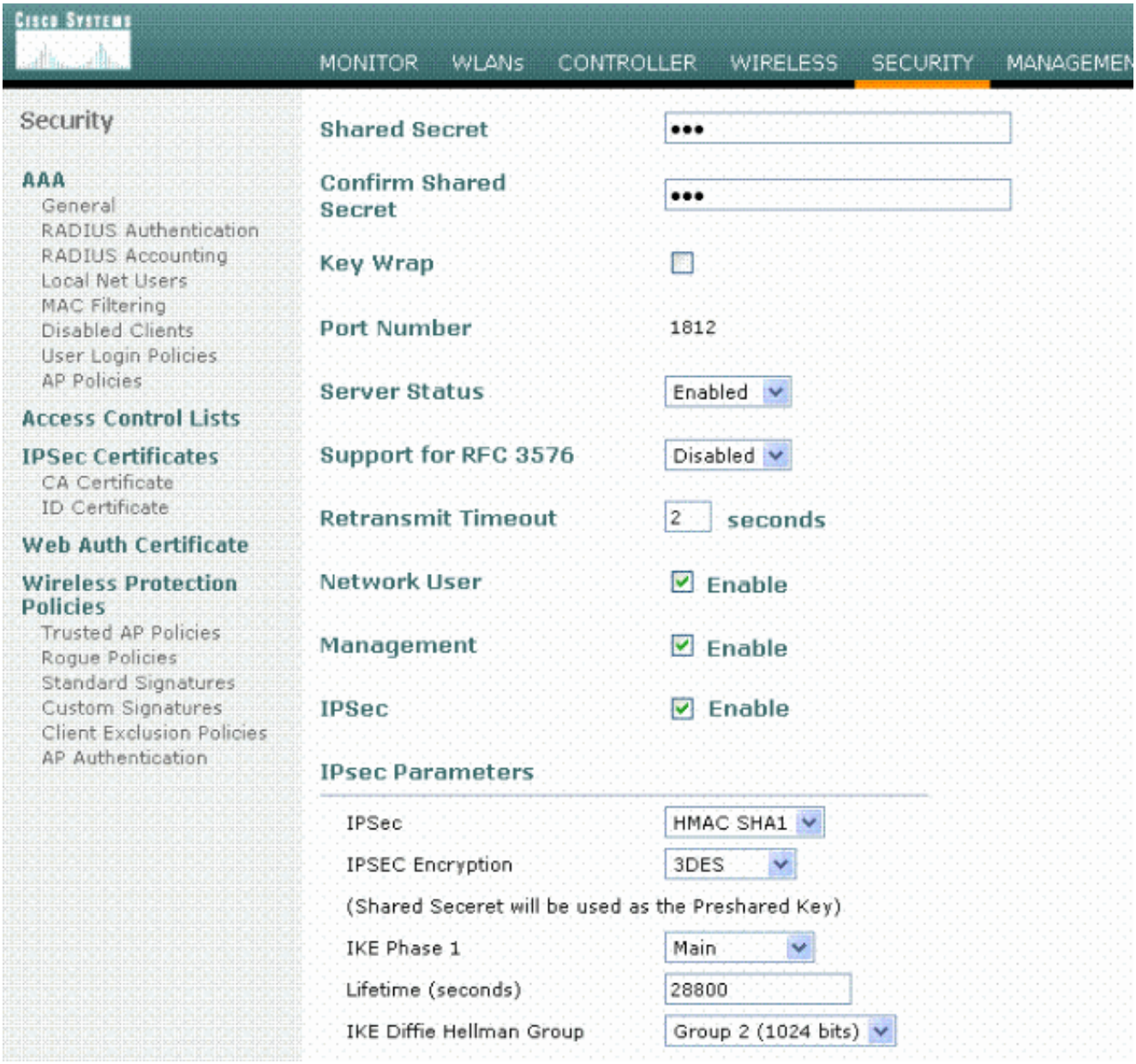
Del regulador GUI, complete estos pasos.

1. Navegue a la **Seguridad >AAA >** lengueta de la **autenticación de RADIUS** en el regulador GUI, y agregue a un nuevo servidor de

RADIUS.



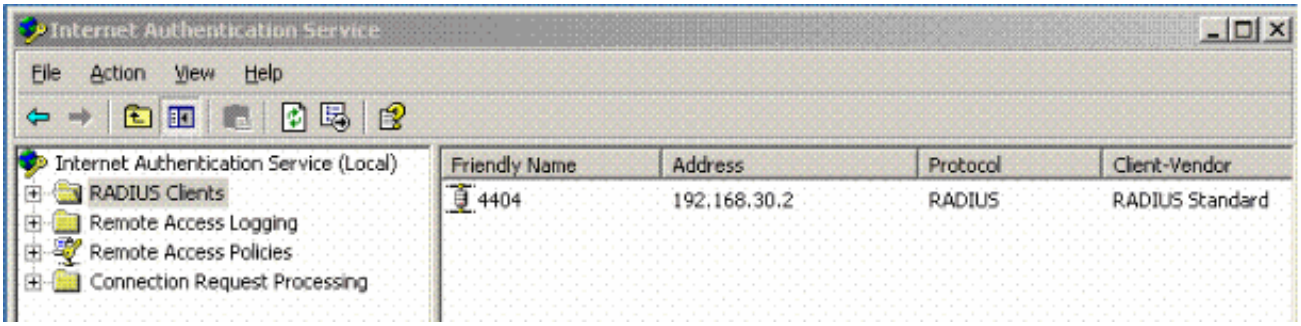
2. Configure la dirección IP, el puerto 1812, y un secreto compartido del nuevo servidor de RADIUS. Marque el **IPSec activan la** casilla de verificación, configuran estos parámetros de IPSec, y después hacen clic **se aplican**.**Nota:** El secreto compartido se utiliza para autenticar al servidor de RADIUS y como la clave previamente compartida (PSK) para la Autenticación IPSec.



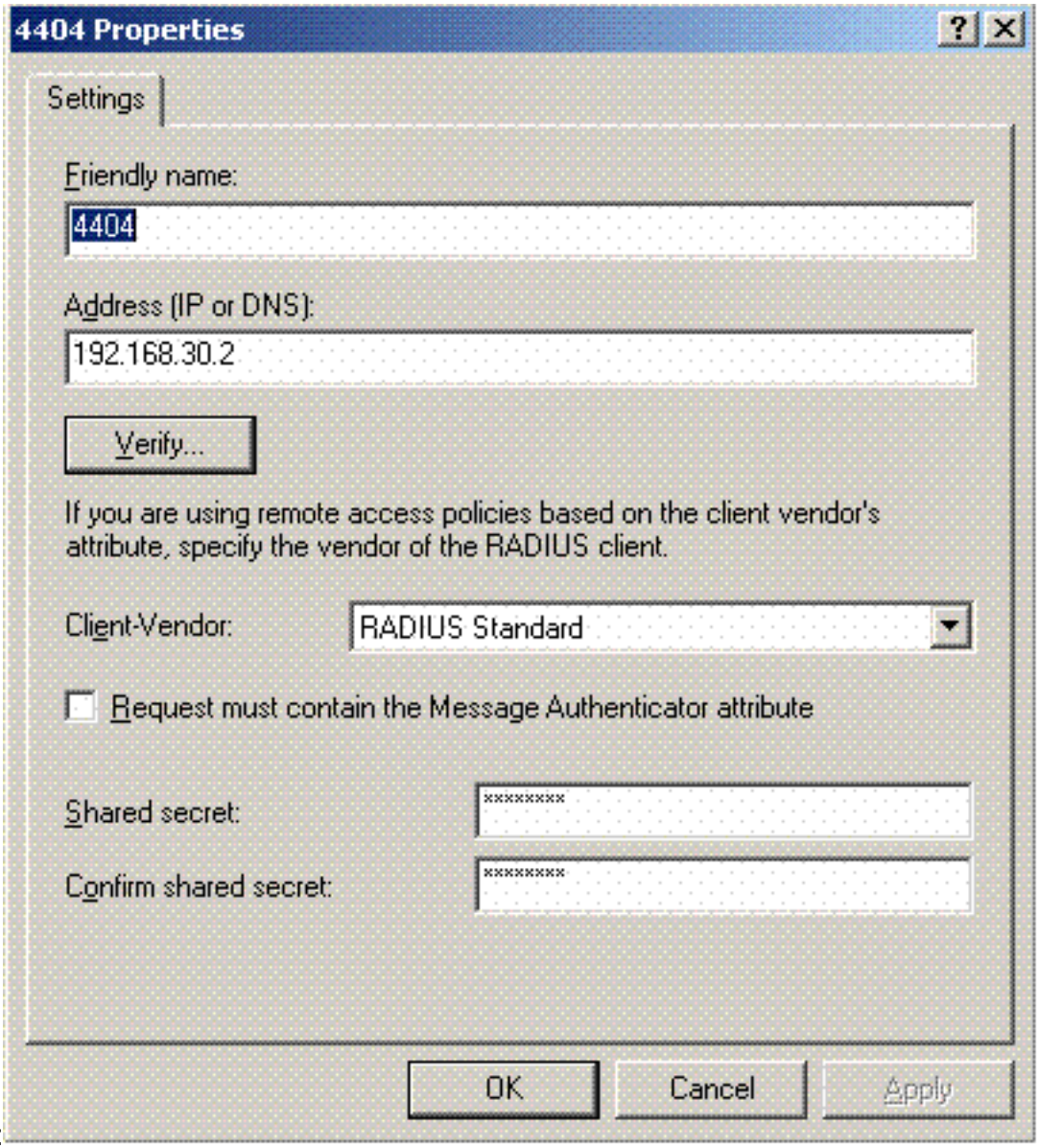
Configure IAS

Complete estos pasos en IAS:

1. Navegue al administrador de IAS en Win2003 y agregue a un nuevo cliente RADIUS.

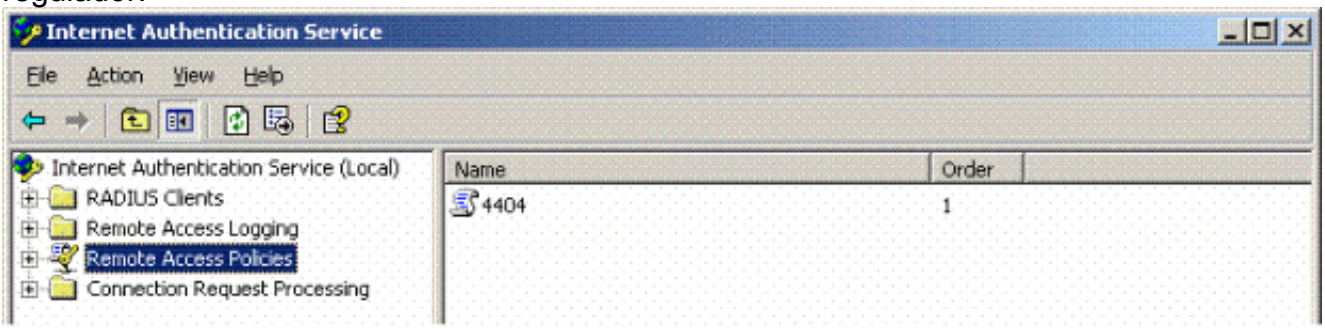


2. Configure las propiedades del cliente RADIUS con la dirección IP y el secreto compartido configurados en el

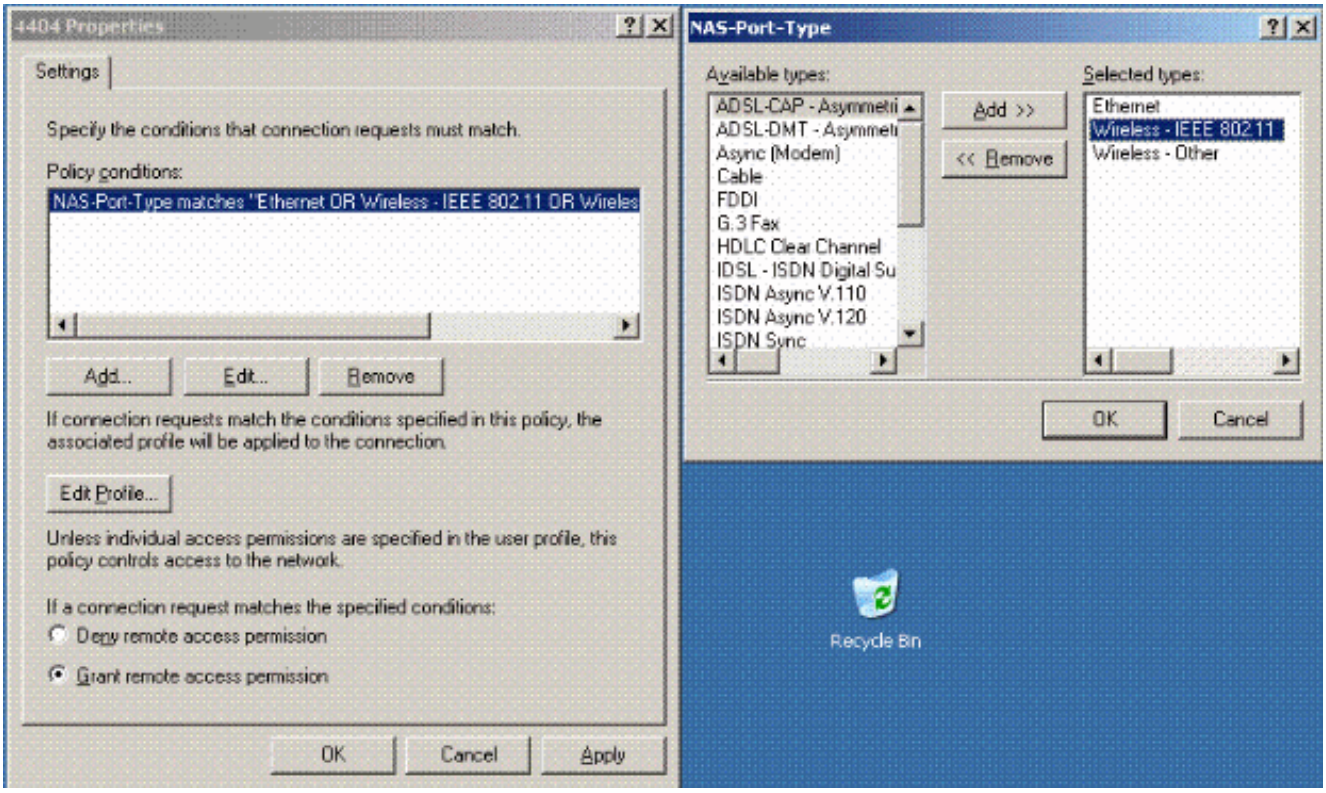


regulador:

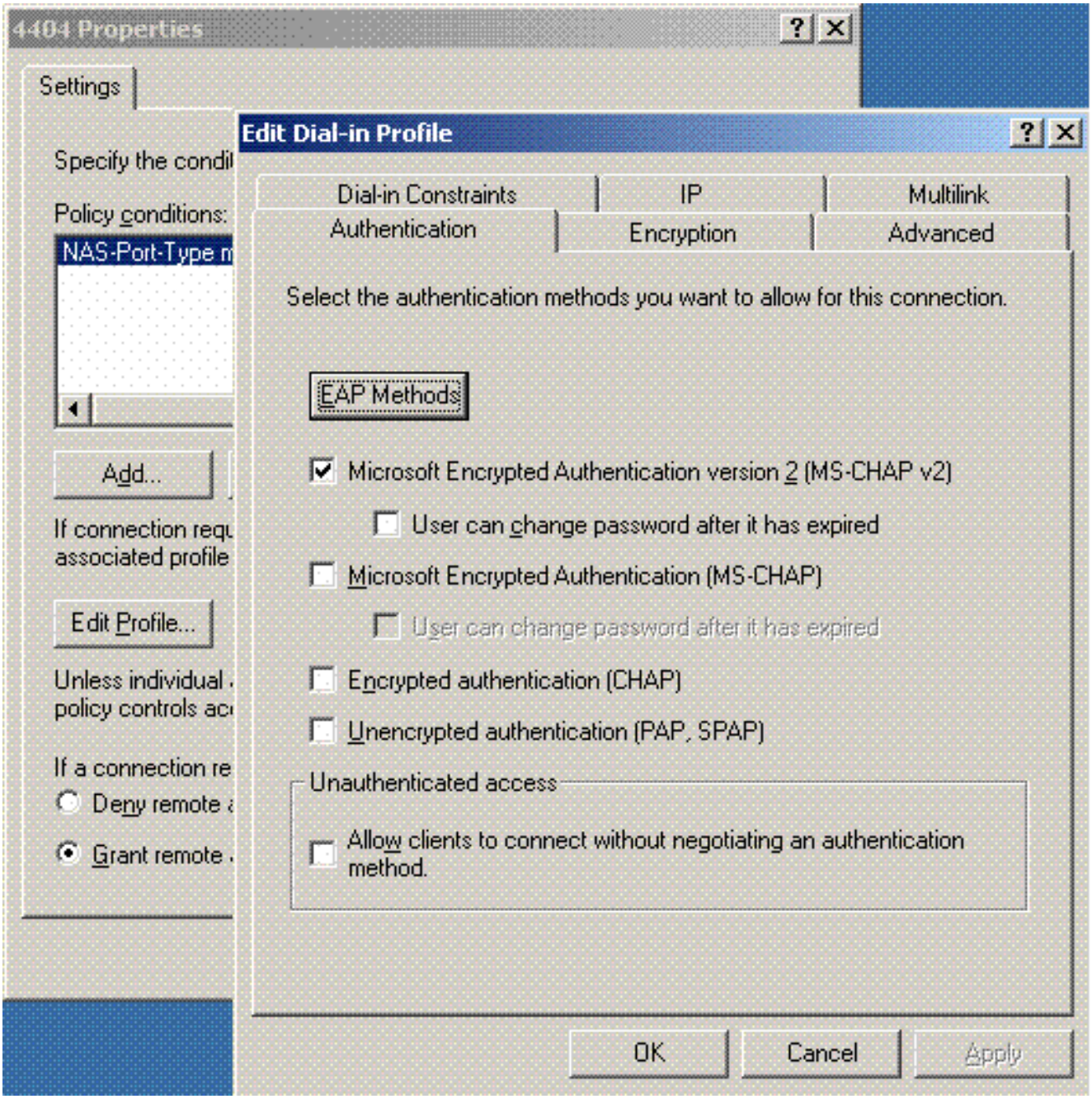
3. Configure una nueva política de acceso remoto para el regulador:



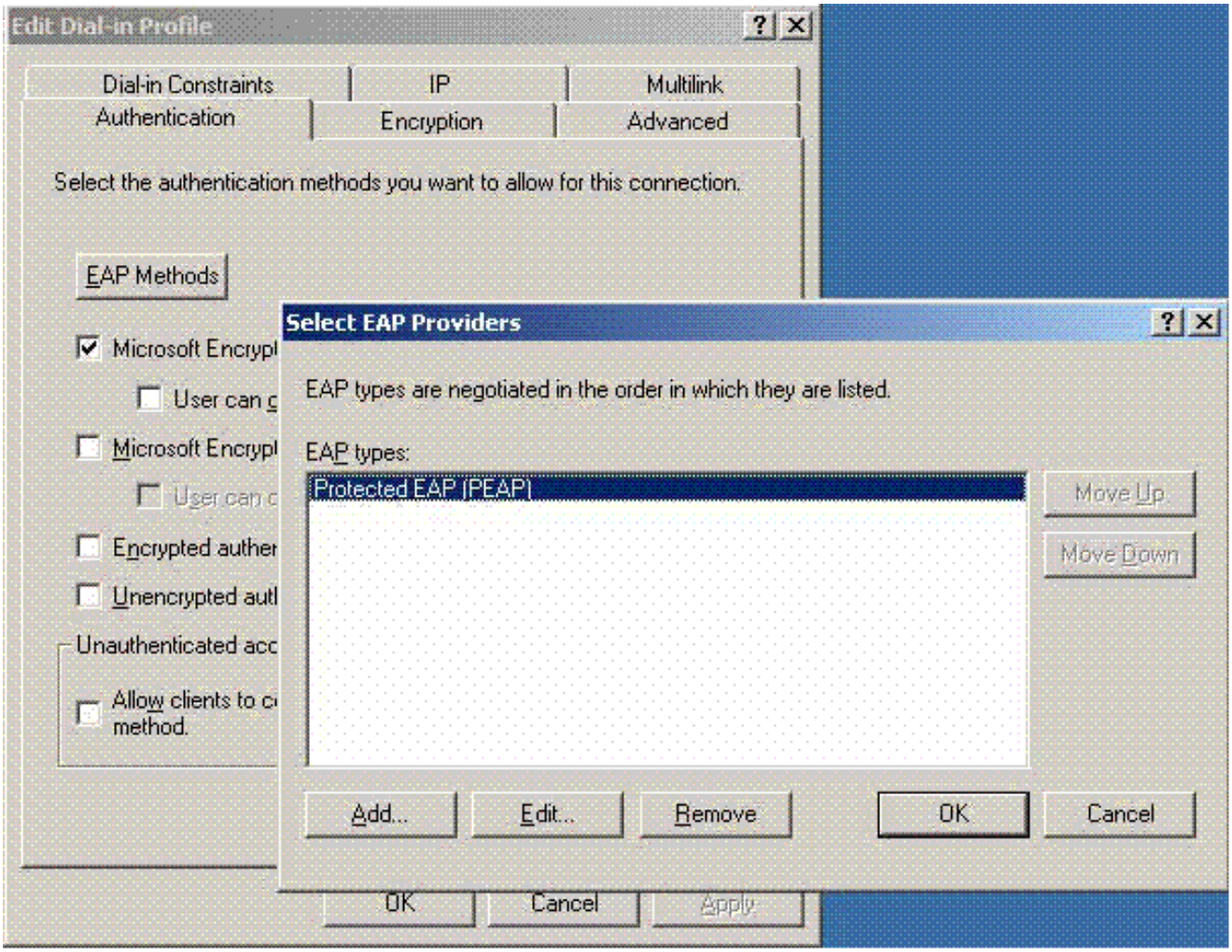
4. Edite las propiedades de la política de acceso remoto del regulador. Aseegurese agregar el tipo del NAS-puerto - Tecnología inalámbrica – IEEE 802.11:



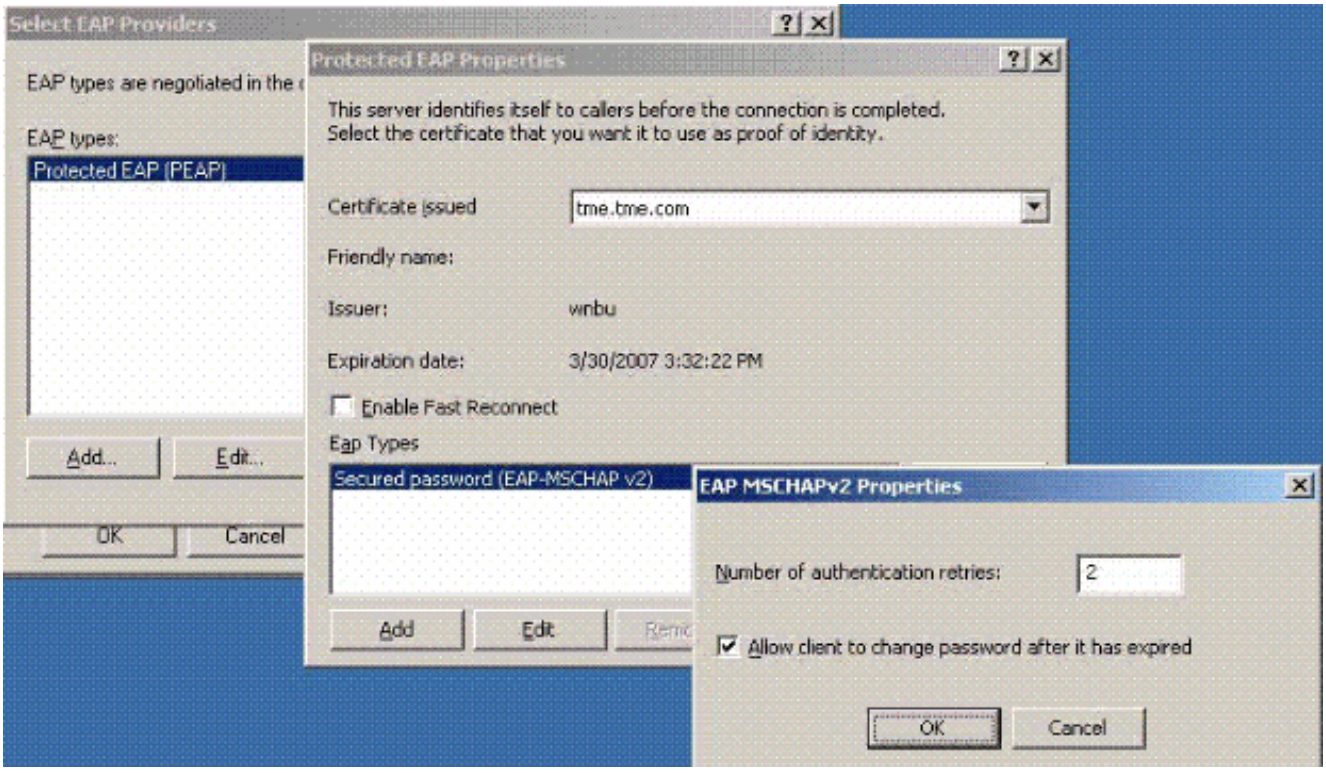
5. El tecleo **edita el perfil**, hace clic la lengueta de la **autenticación**, y el v2 del control MS-CHAP para la
autenticación:



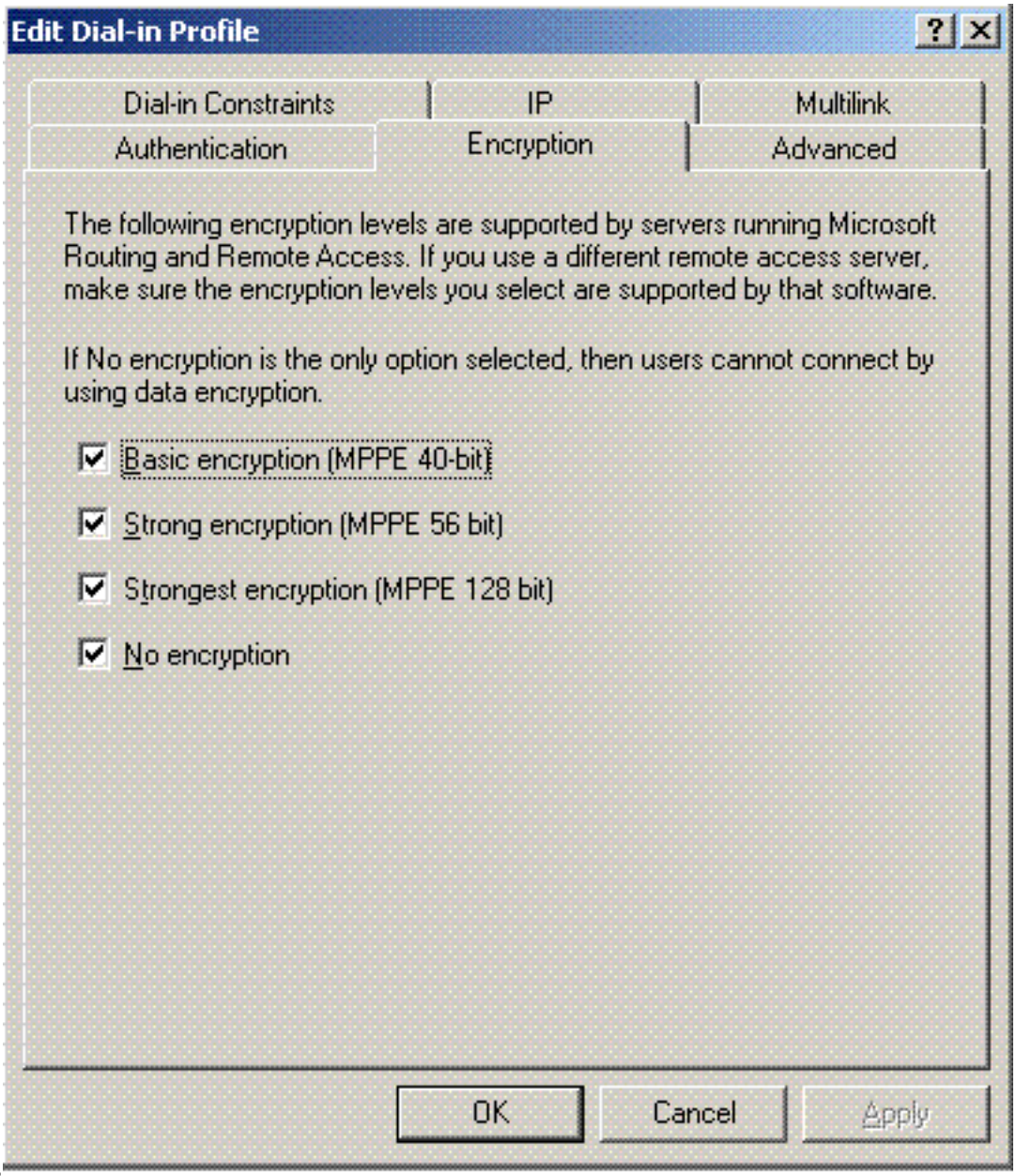
6. Haga clic los **métodos EAP**, seleccione los proveedores EAP, y agregue el PEAP como tipo EAP:



7. El tecleo **edita** en los proveedores Select EAP y elige del menú de la extracción abajo que el servidor se asoció a sus cuentas de usuario y a CA (e.g. tme.tme.com) del Active Directory. Agregue el v2 del tipo MSCHAP
EAP:

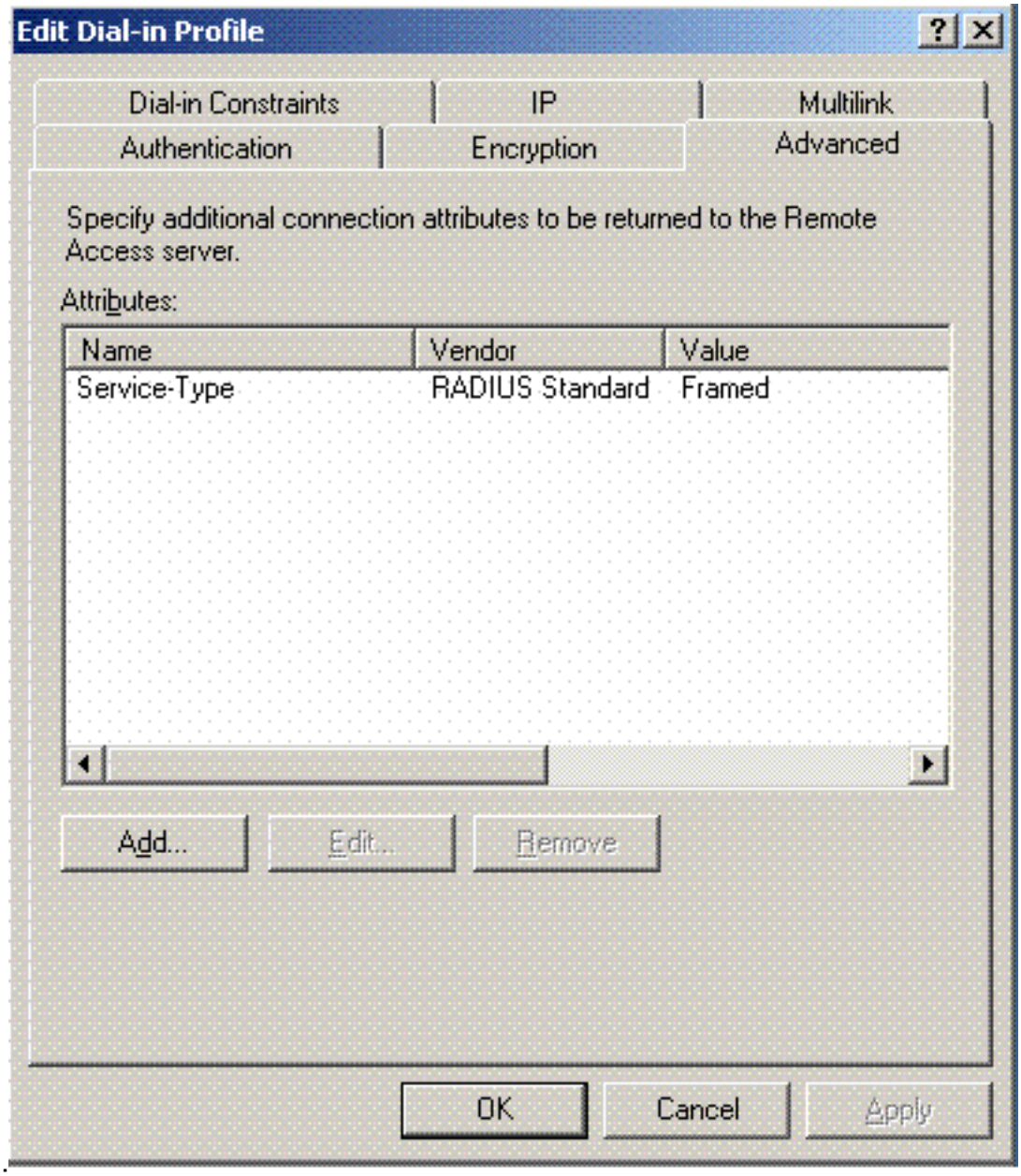


8. Haga clic la lengueta del **cifrado**, y marque todos los tipos de encripción para el Acceso



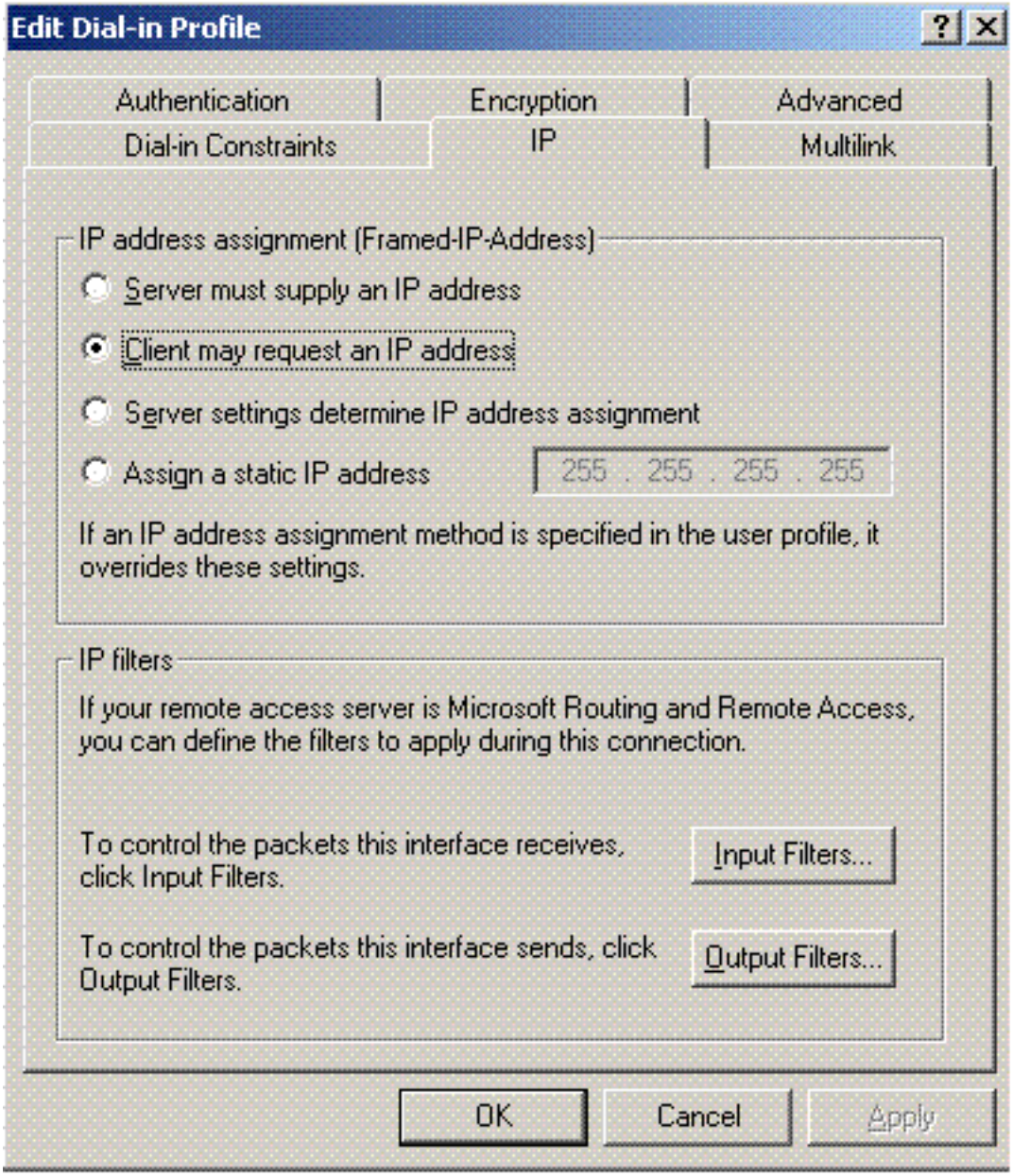
Remoto:

9. Haga clic la **ficha Avanzadas**, y agregue la norma RADIUS/capítulo como el tipo de



servicio:

10. Haga clic la lengueta **IP**, y el **cliente del** control **puede pedir una dirección IP**. Esto asume que usted tiene DHCP habilitado en un Switch o un

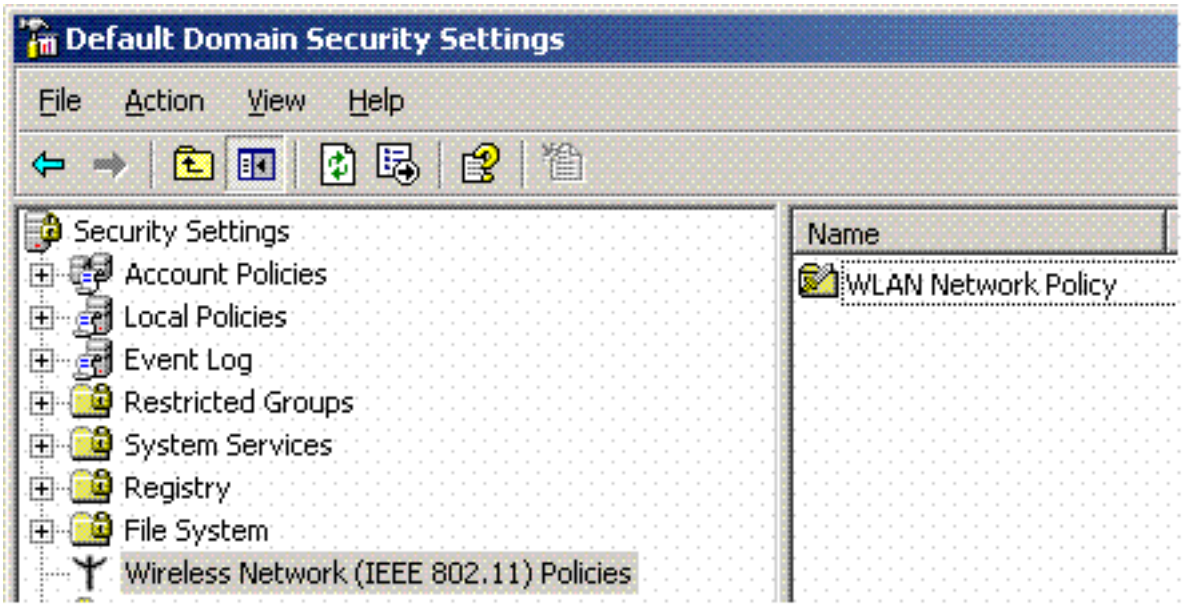


WinServer.

Microsoft Windows 2003 ajustes de seguridad del dominio

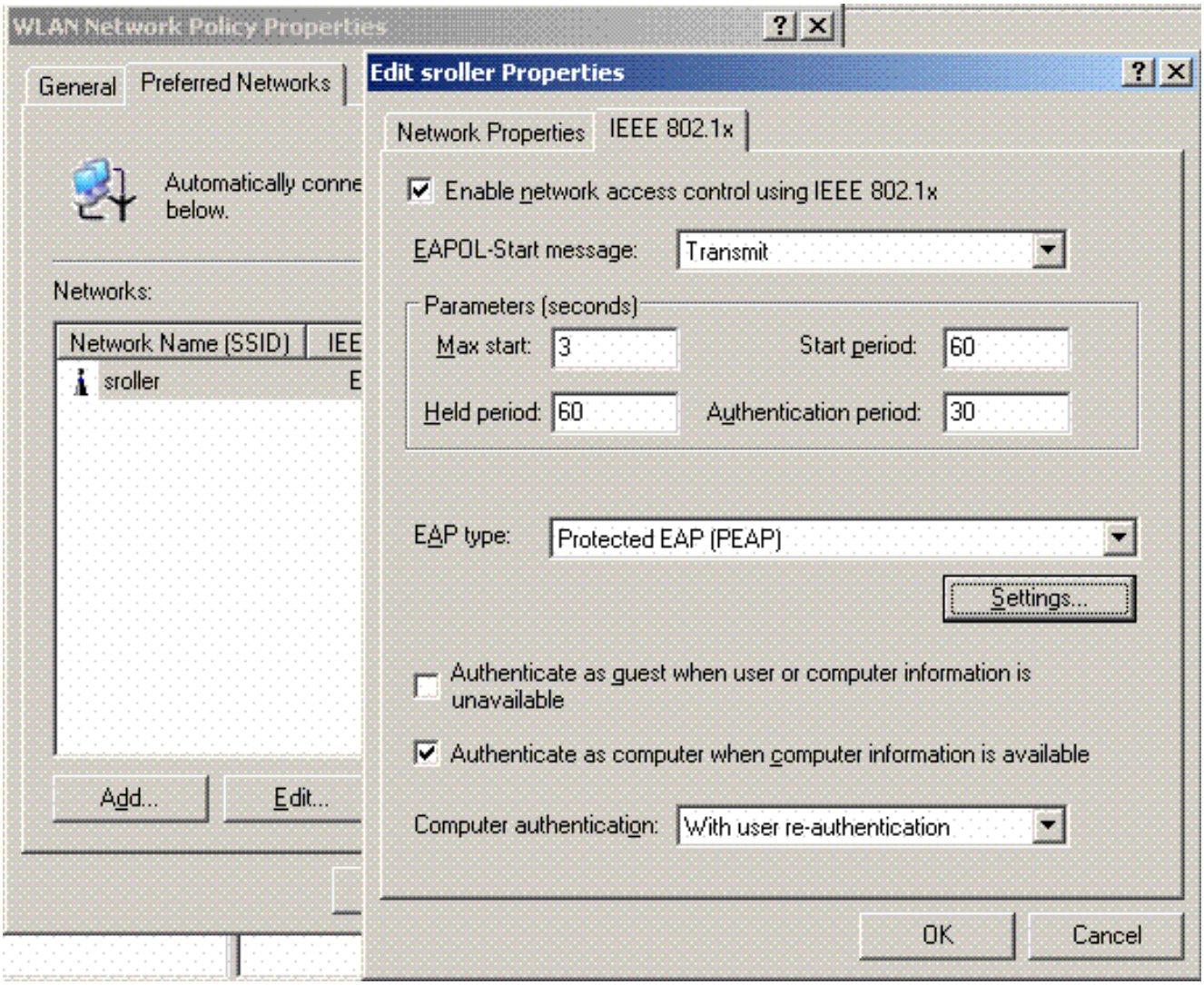
Complete estos pasos para configurar Windows 2003 ajustes de seguridad del dominio:

1. Inicie al administrador de los ajustes de seguridad del Default Domain, y cree una nueva política de seguridad para las directivas de la red inalámbrica (IEEE



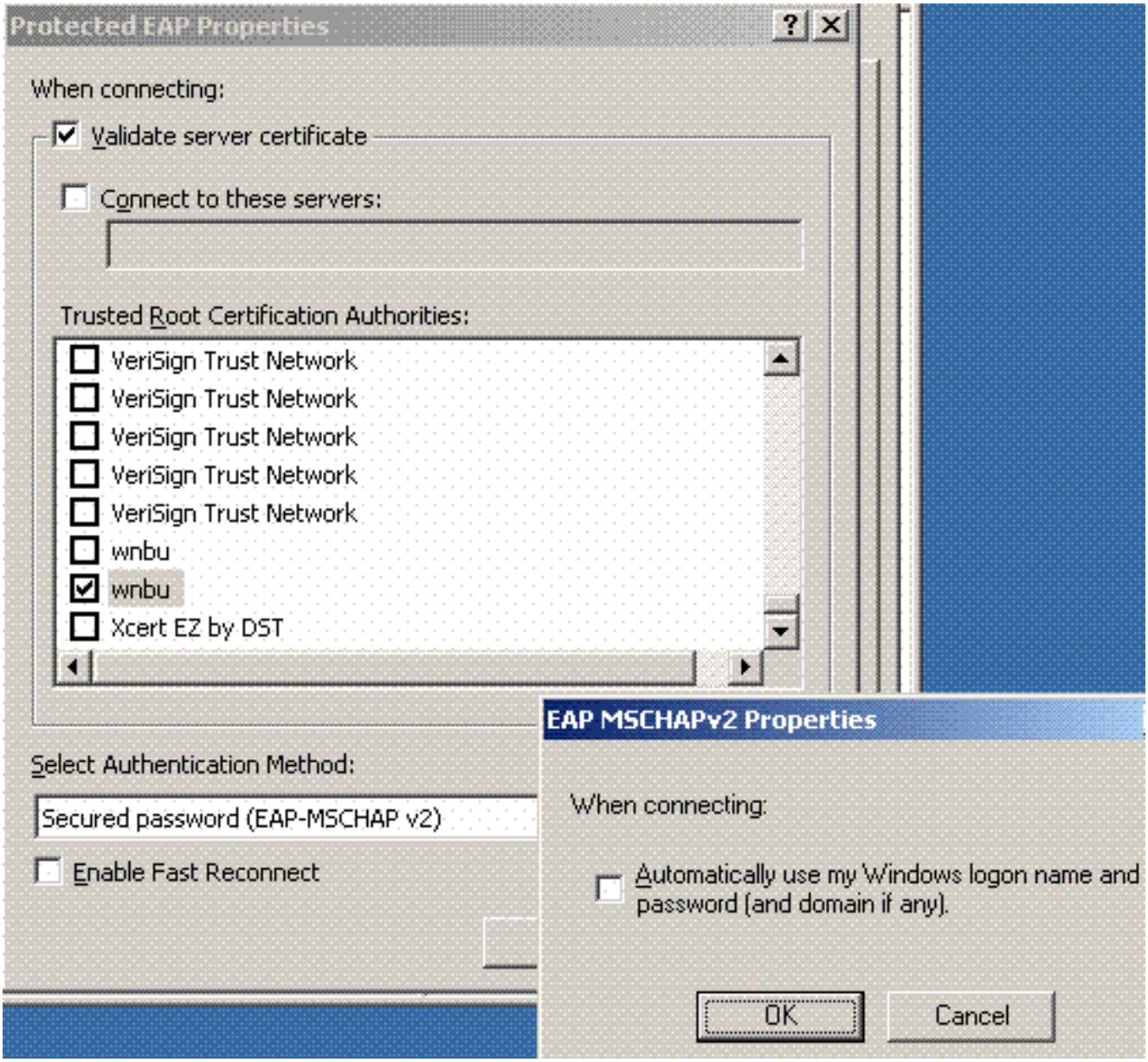
802.11).

2. Las propiedades de la directiva de la red WLAN abierta, y el tecleo **prefirieron las redes**. Agregue una nueva red inalámbrica (WLAN) preferida y teclee el nombre de su red inalámbrica (WLAN) SSID, tal como `Tecnología inalámbrica`. Doble el tecleo que la nueva red preferida, y hace clic el **IEEE 802.1X** cuadro elige el PEAP como el tipo EAP:

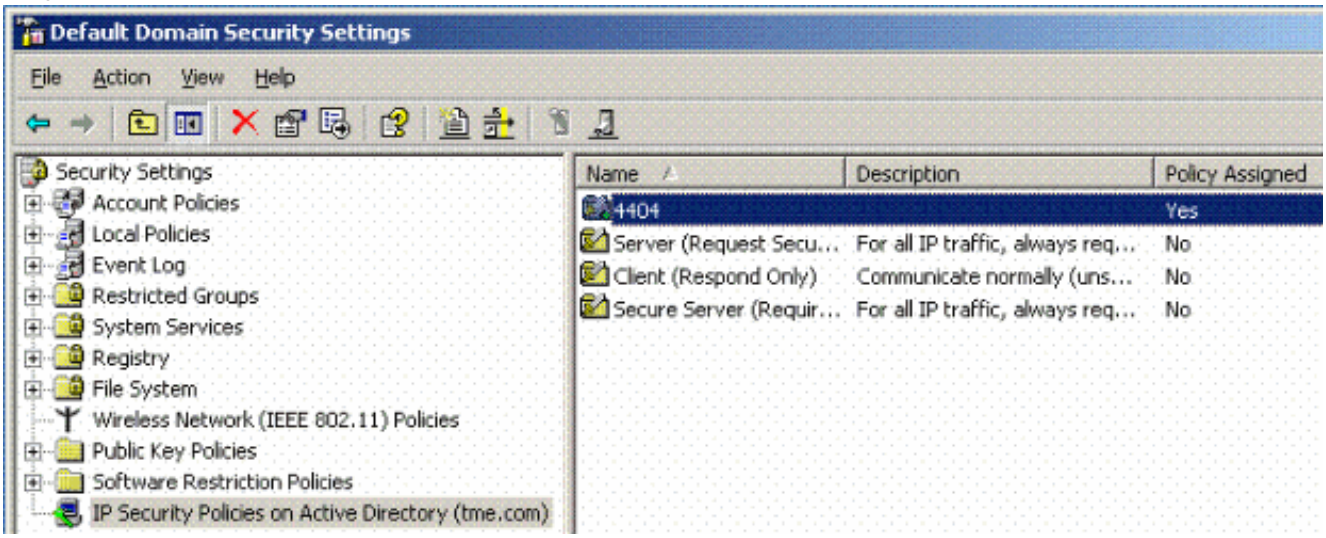


3. Haga clic las **configuraciones PEAP**, el control **valida el certificado de servidor**, y selecciona el CERT de la Raíz confiable instalado en el Certificate Authority. Para comprobar, desmarque el cuadro del v2 de la GRIETA MS para automáticamente utilizan mi login y

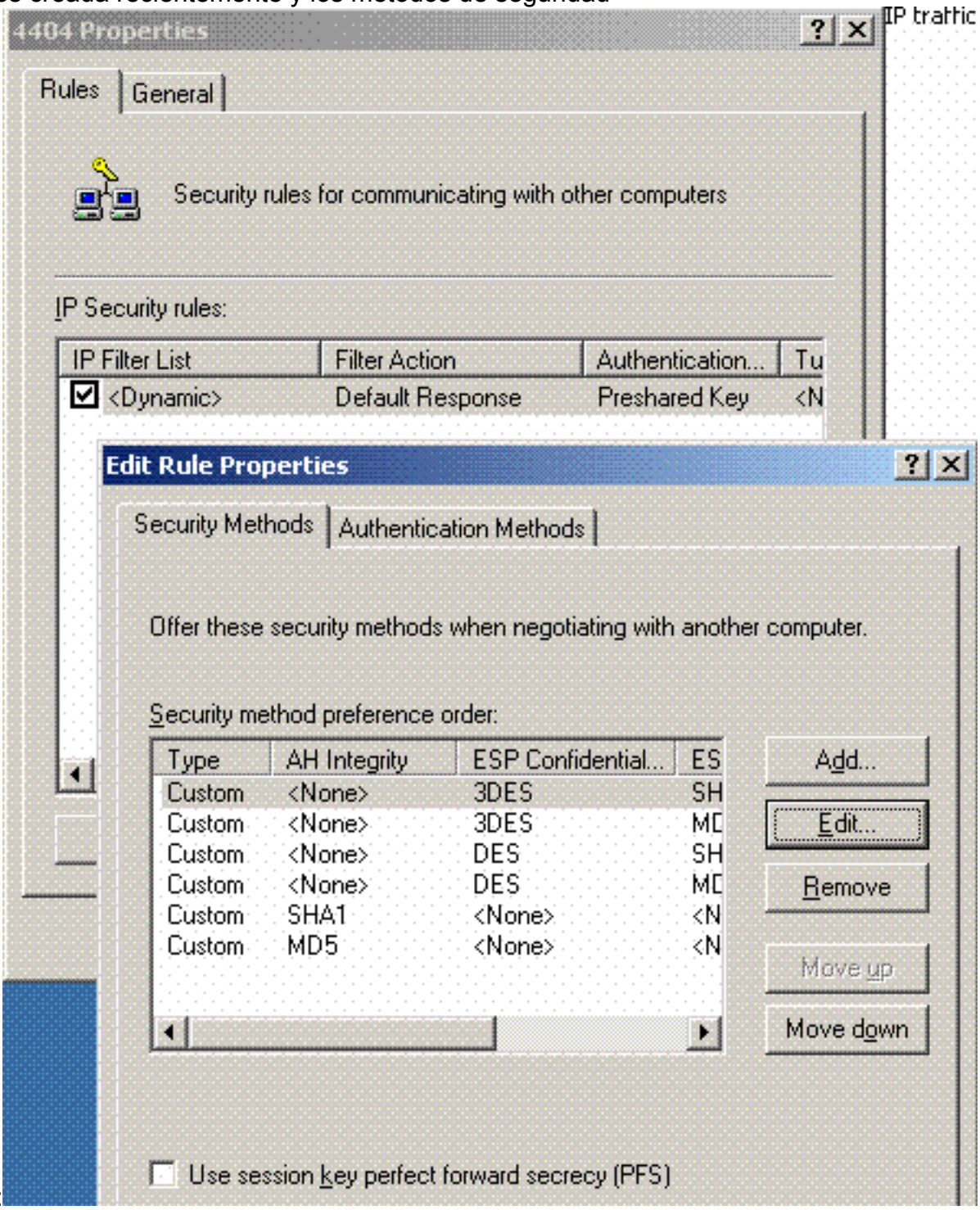
contraseña de
Windows.



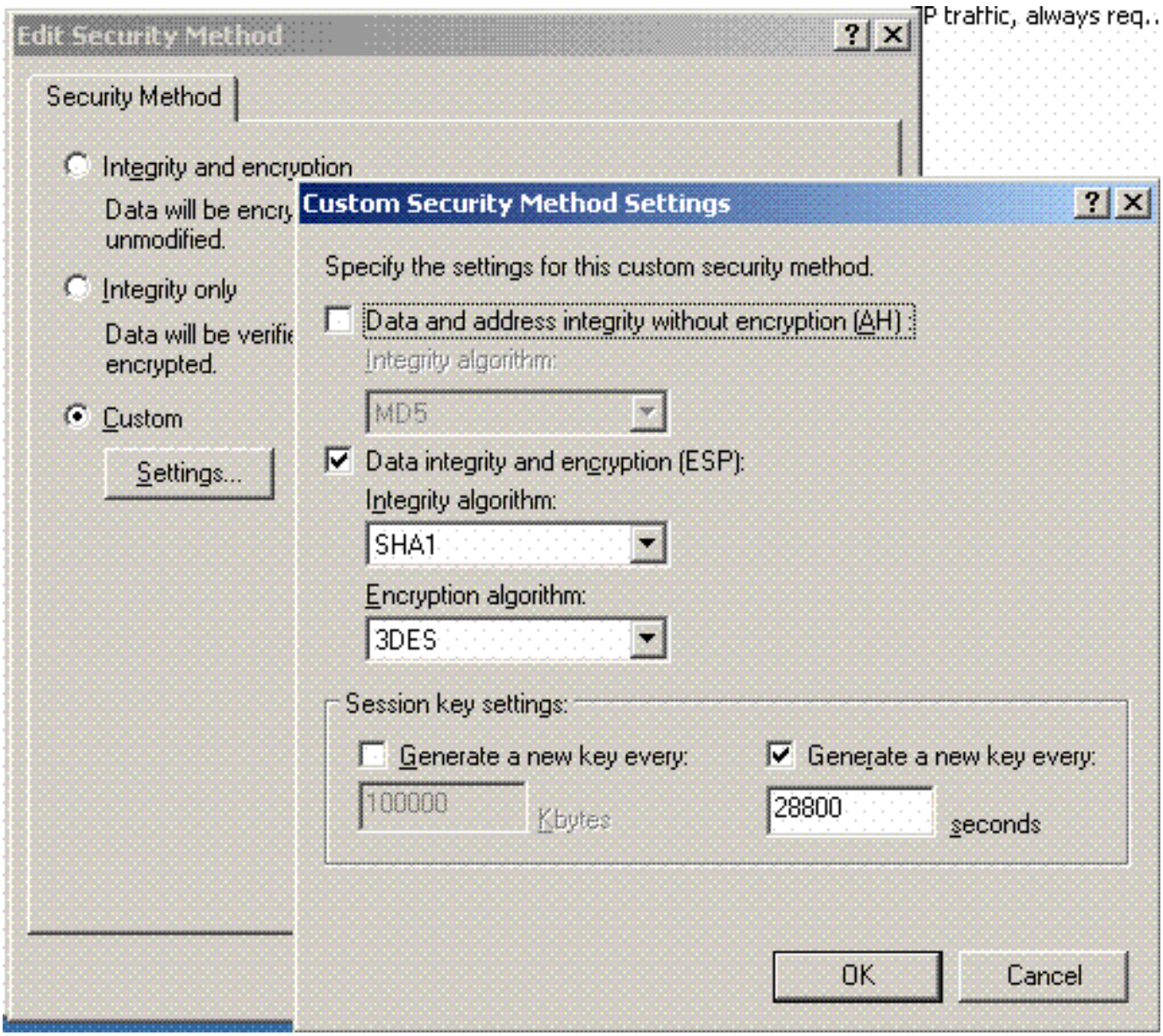
4. En la ventana de administrador de los ajustes de seguridad del Default Domain de Windows 2003, cree otras nuevas directivas de seguridad IP en la directiva del Active Directory, tal como
4404.



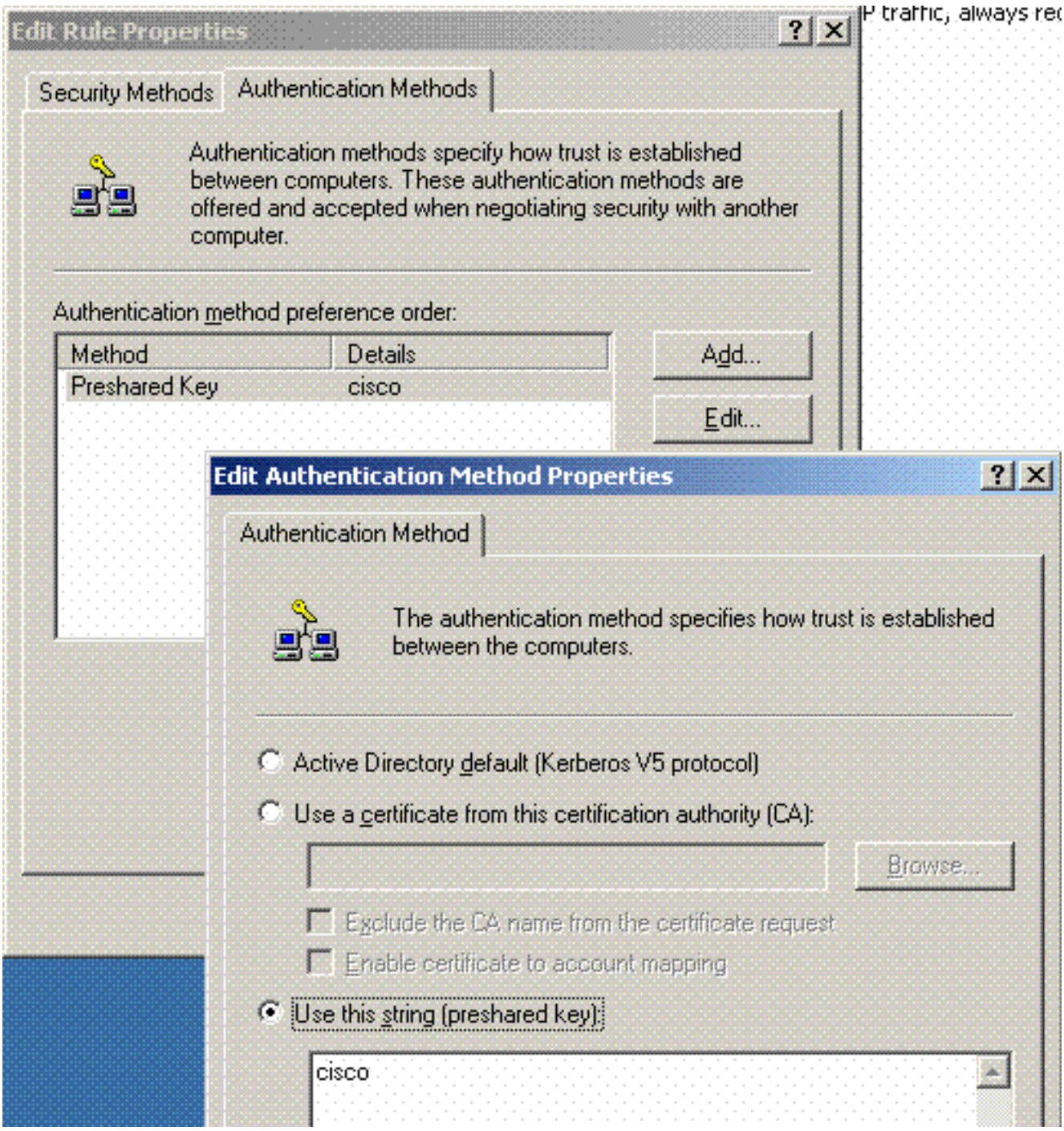
5. Edite las nuevas 4404 propiedades de la directiva, y haga clic las **reglas que** cuadro agrega una nueva regla para filtros - lista del filete IP (dinámica); Filter Action (Acción de filtro) (respuesta predeterminada); Autenticación (PSK); Túnel (ninguno). Tecleo doble la regla para filtros creada recientemente y los métodos de seguridad selectos:



6. Haga clic **editan el método de seguridad**, y hacen clic el botón de radio de las **configuraciones personalizadas**. Elija estas configuraciones.**Nota:** Estas configuraciones deben hacer juego las configuraciones del regulador RADIUS seguridad IPSec.



7. Haga clic la lengueta del **método de autentificación** bajo propiedades de la regla del editar. Ingrese el mismo secreto compartido que usted ingresó previamente en la configuración de RADIUS del
regulador.



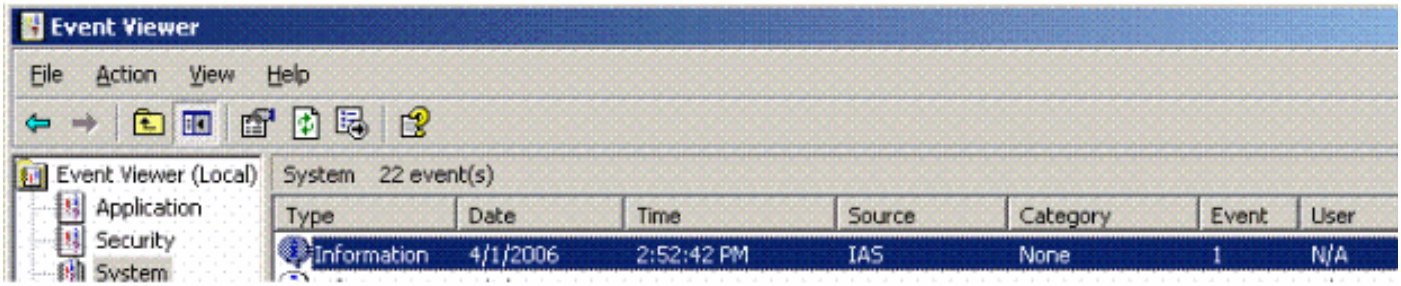
En este momento, todas las configuraciones para el regulador, IAS y los ajustes de seguridad del dominio se completan. Salve todas las configuraciones en el regulador y WinServer y reinicie todas las máquinas. En el cliente WLAN que se utiliza para probar, instale el CERT de la raíz y configurelo para WPA2/PEAP. Después de que el CERT de la raíz esté instalado en el cliente, reinicie la máquina del cliente. Después de todo las máquinas reinician, conectan al cliente con la red inalámbrica (WLAN) y capturan estos eventos del registro.

Nota: Una conexión cliente se requiere para configurar conexión IPSec en medio el regulador y el WinServer RADIUS.

Eventos del registro de 2003 System de Windows

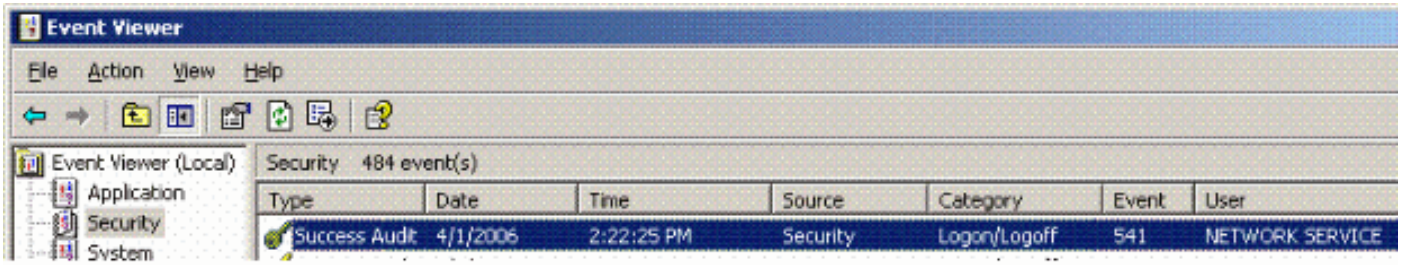
Una conexión acertada del cliente WLAN configurada para WPA2/PEAP con el IPSec RADIUS habilitado genera este evento del sistema en el WinServer:

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)
```

Un <> acertado RADIUS del regulador conexión IPSec 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 del debug del éxito del IPSec del regulador RADIUS del Wireless LAN

Usted puede utilizar el **permiso del ikemsg del debug P.M. del** comando debug en el regulador 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 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
```

Captura de Ethreal

Aquí está una captura de Ethreal de la muestra.

```
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 LAN de la tecnología inalámbrica de Cisco, versión 5.2
- Soporte Técnico y Documentación - Cisco Systems