Configurar a segurança IPSec do RAIO para WLC & servidor de IAS de Microsoft Windows 2003

Índice

Introdução

Documentos deste guia como configurar a característica do IPsec do RAIO apoiada pelo WCS e pelos estes controladores de WLAN:

- 4400 Series
- WiSM
- 3750G

A característica do IPsec do RAIO do controlador é ficada situada no controlador GUI sob a **Segurança > o AAA > a** seção dos **servidores de autenticação RADIUS**. A característica fornece um método para que você cifre todas as comunicações do RAIO entre controladores e servidores Radius (IAS) com o IPsec.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento no LWAPP
- Conhecimento na autenticação RADIUS e no IPsec

- Conhecimento em como configurar serviços no sistema operacional do server de Windows 2003

Componentes Utilizados

Este a rede e os componentes de software devem ser instalados e configurado a fim distribuir a característica do IPsec do RAIO do controlador:

- WLC 4400, WiSM, ou controladores 3750G. Este exemplo usa o WLC 4400 que executa a versão de software 5.2.178.0
- Lightweight Access Points (regaços). Este exemplo usa o REGAÇO do 1231 Series.
- Comute com DHCP
- Server de Microsoft 2003 configurado como um controlador de domínio instalado com Microsoft Certificate Authority e com Internet Authentication Service de Microsoft (IAS).
- Segurança do domínio Microsoft
- Adaptador de cliente Wireless do a/b/g do 802.11 de Cisco com a versão ADU 3.6 configurada com WPA2/ PEAP

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configuração RADIUS do IPsec

Este manual de configuração não endereça a instalação ou a configuração de Microsoft WinServer, Certificate Authority, diretório ativo ou cliente do 802.1x WLAN. Estes componentes devem ser instalados e configurado antes do desenvolvimento da característica do RAIO do IPsec do controlador. O restante de documentos deste guia como configurar o RAIO do IPsec nestes componentes:

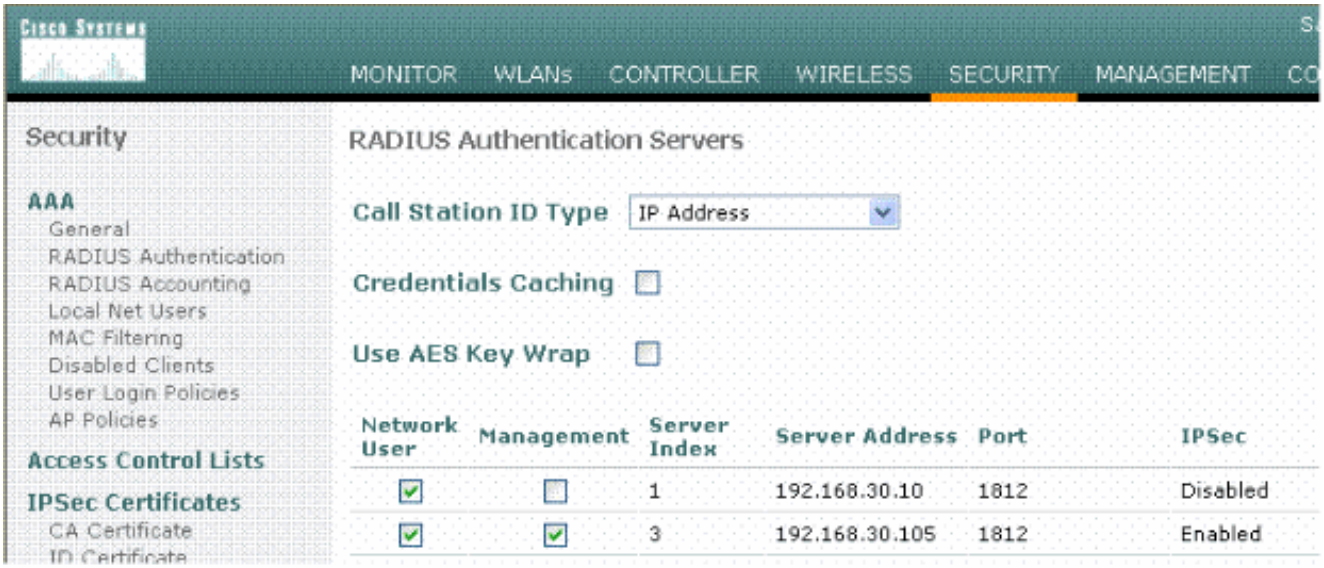
1. Controladores de WLAN de Cisco
2. Windows 2003 IAS
3. Configurações de segurança do domínio de Microsoft Windows

Configurar o WLC

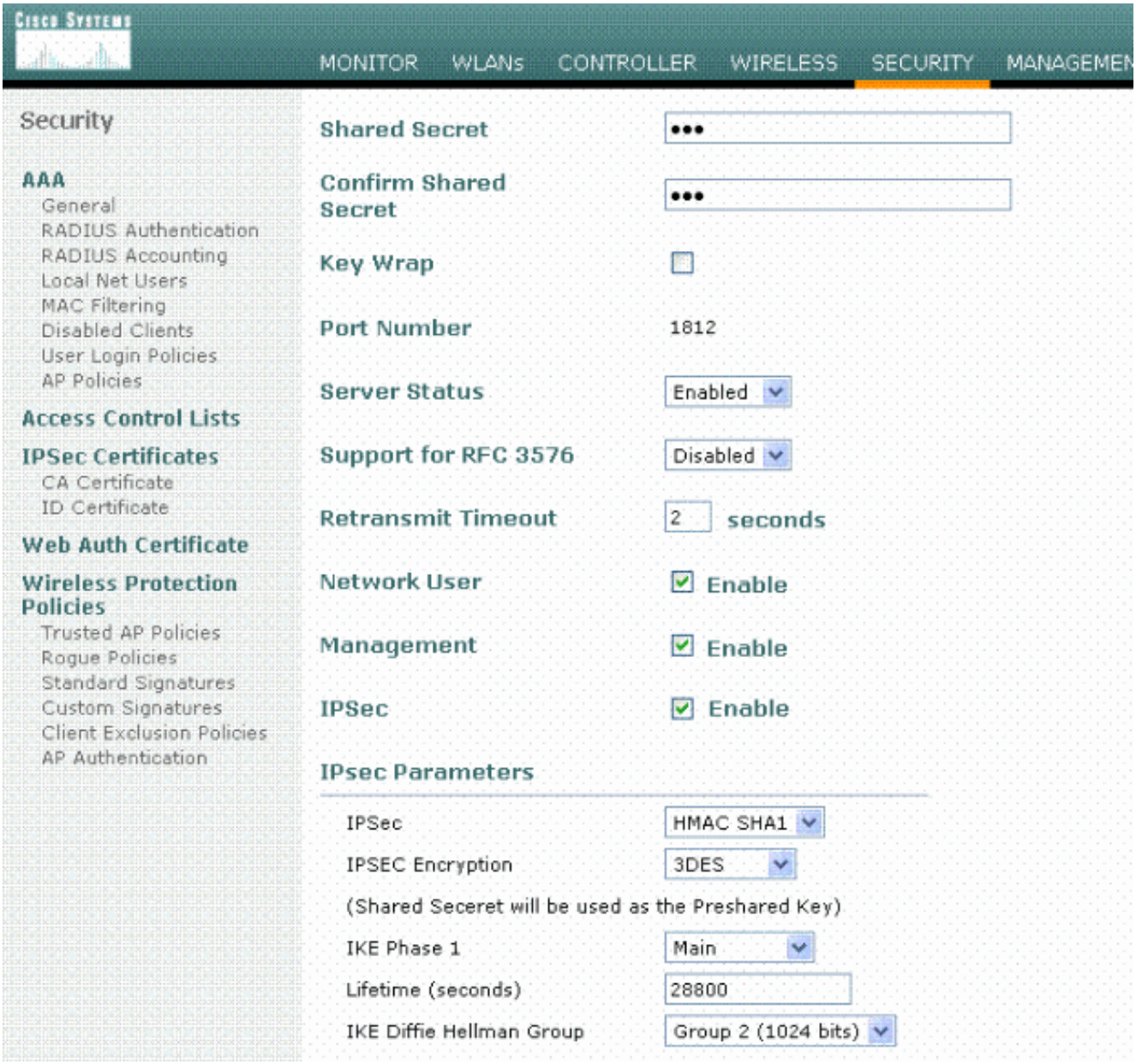
Esta seção explica como configurar o IPsec no WLC com o GUI.

Do controlador GUI, termine estas etapas.

1. Navegue à **Segurança > ao AAA > à** aba da **autenticação RADIUS no** controlador GUI, e adicionar um servidor Radius
   novo.



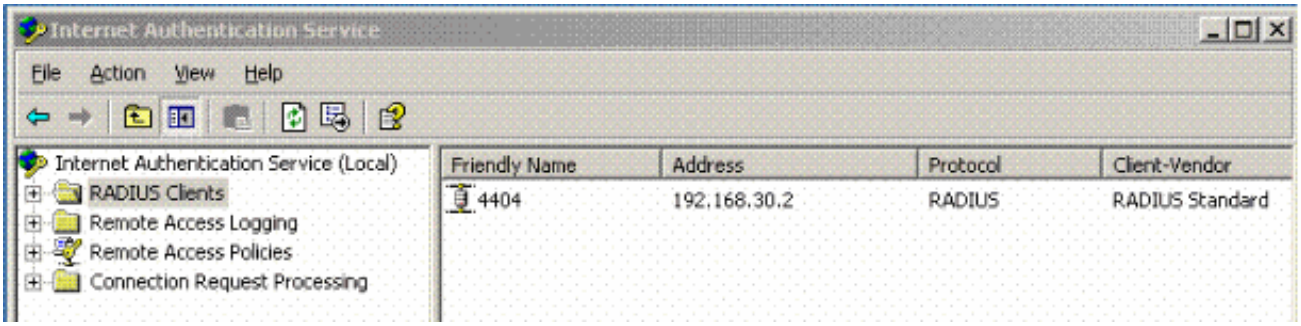
2. Configurar o endereço IP de Um ou Mais Servidores Cisco ICM NT, a porta 1812, e um segredo compartilhado do servidor Radius novo. Verifique o **IPsec permitem a** caixa de verificação, configuram estes parâmetros IPSec, e clicam-nos então **aplicam-se**.**Nota:** O segredo compartilhado é usado para autenticar o servidor Radius e como a chave pré-compartilhada (PSK) para a autenticação
IPSec.



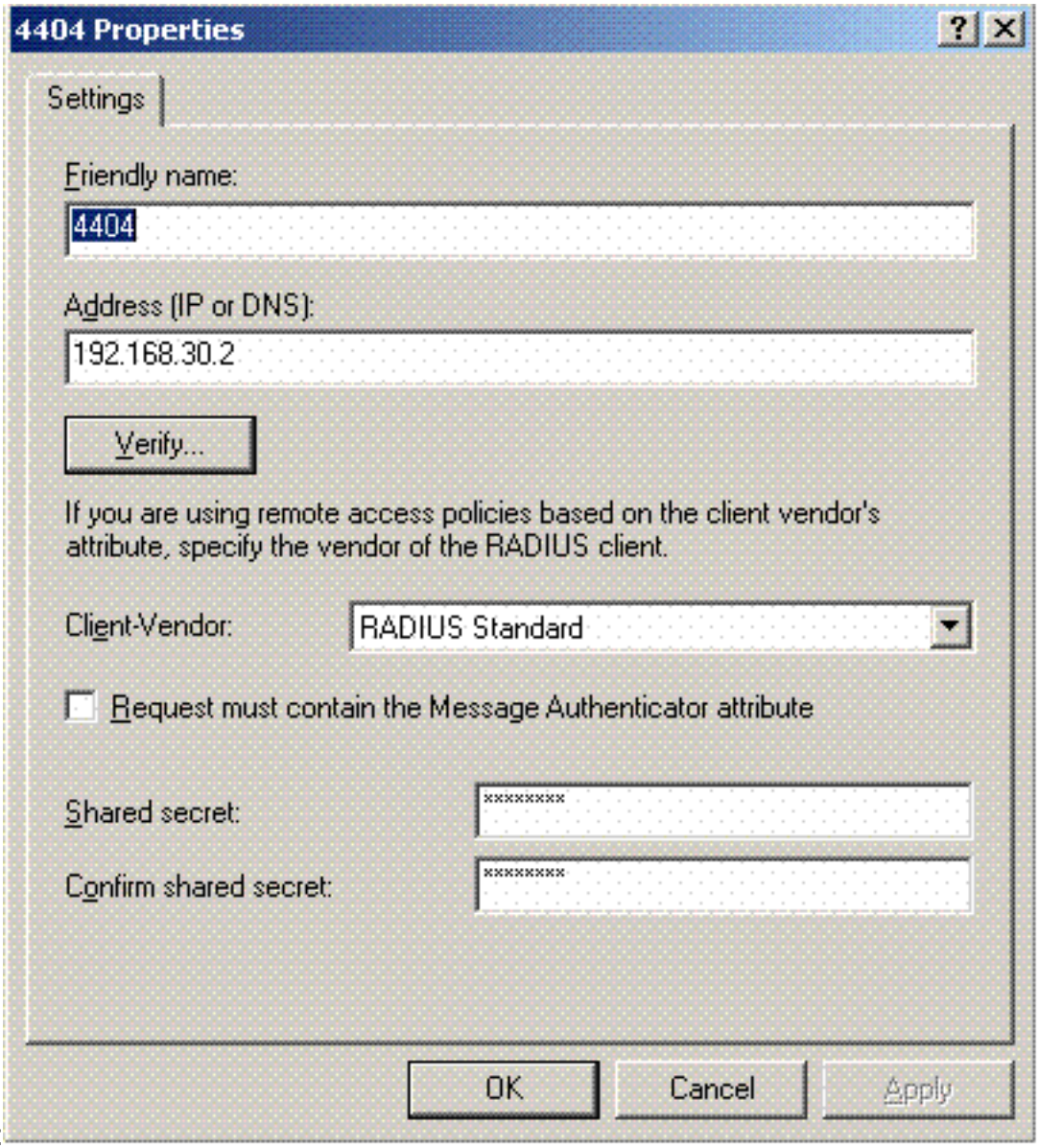
Configurar IAS

Termine estas etapas em IAS:

1. Navegue ao gerente de IAS em Win2003 e adicionar um cliente RADIUS novo.

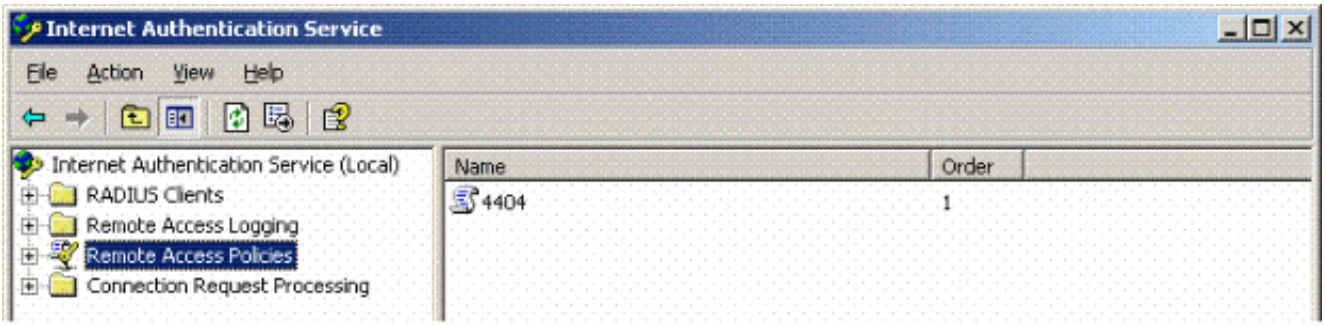


2. Configurar as propriedades do cliente RADIUS com o endereço IP de Um ou Mais Servidores Cisco ICM NT e o segredo compartilhado configurados no

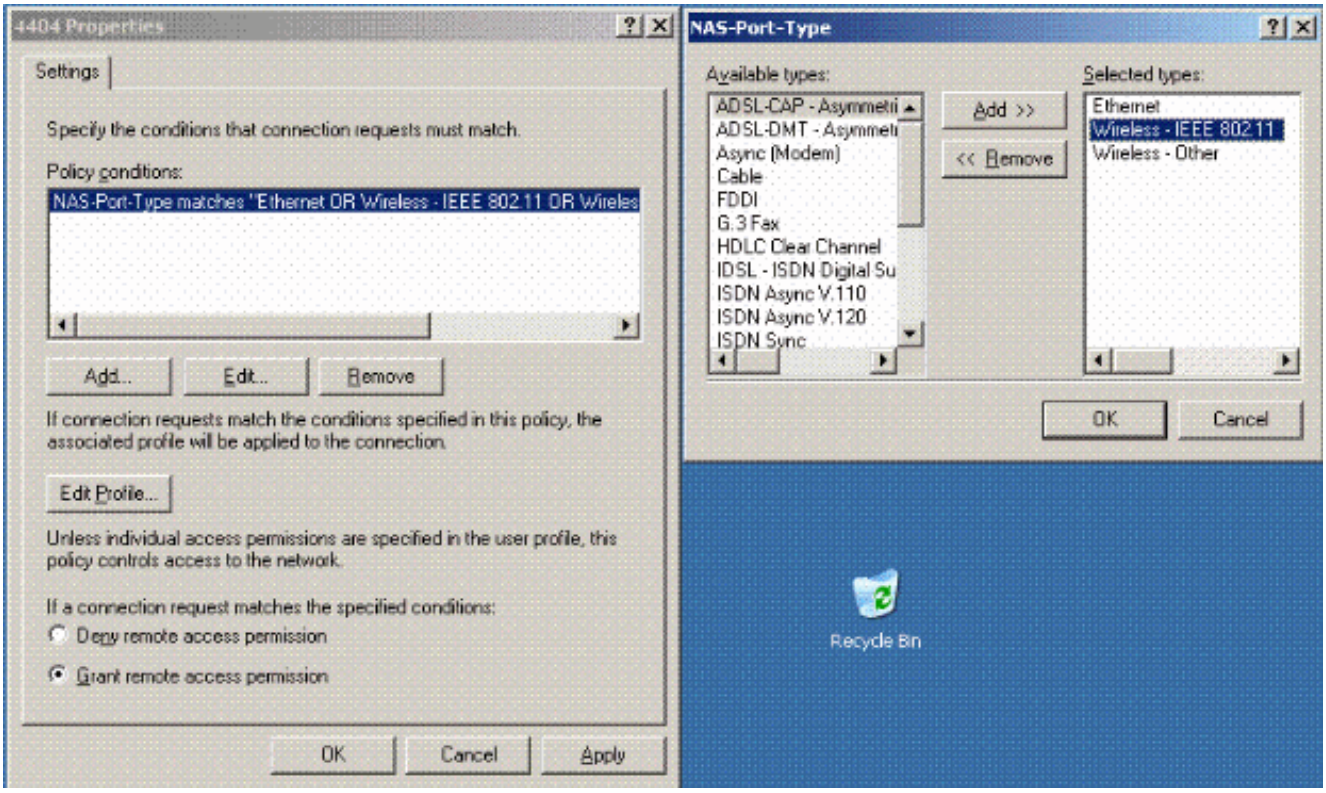


controlador:

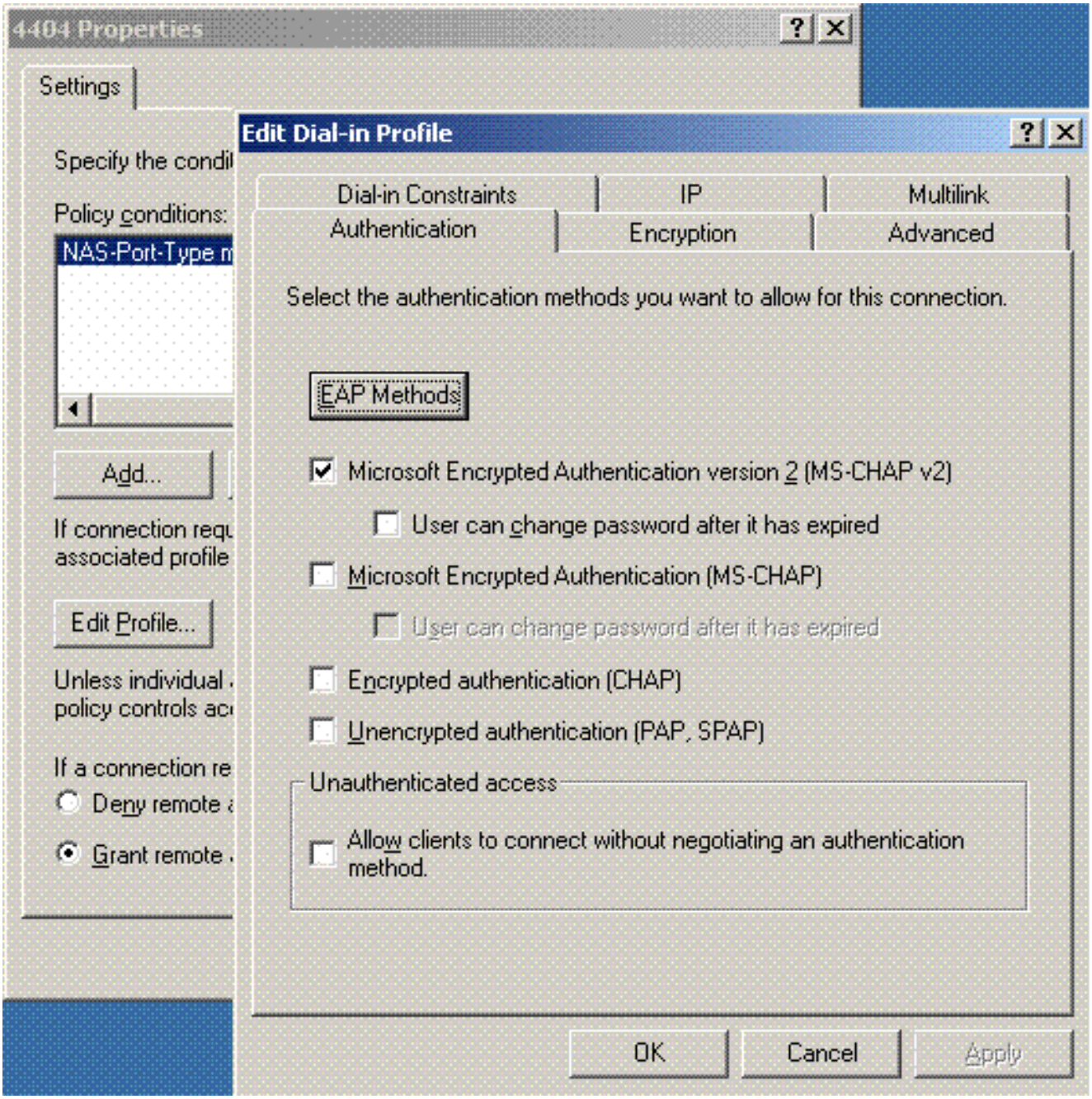
3. Configurar uma política de acesso remoto nova para o controlador:



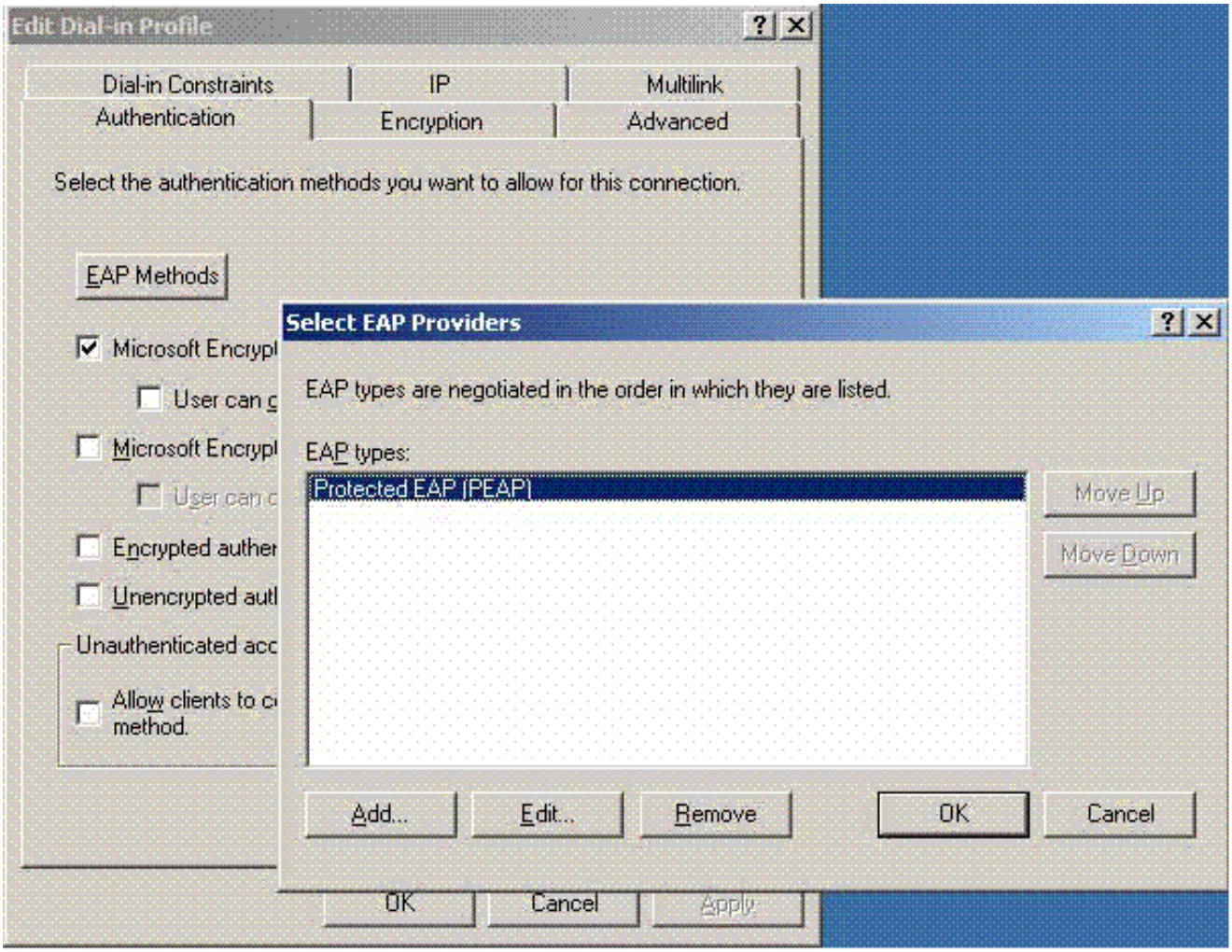
4. Edite as propriedades da política de acesso remoto do controlador. Certifique-se adicionar o tipo da NAS-porta - Sem fio – IEEE 802.11:



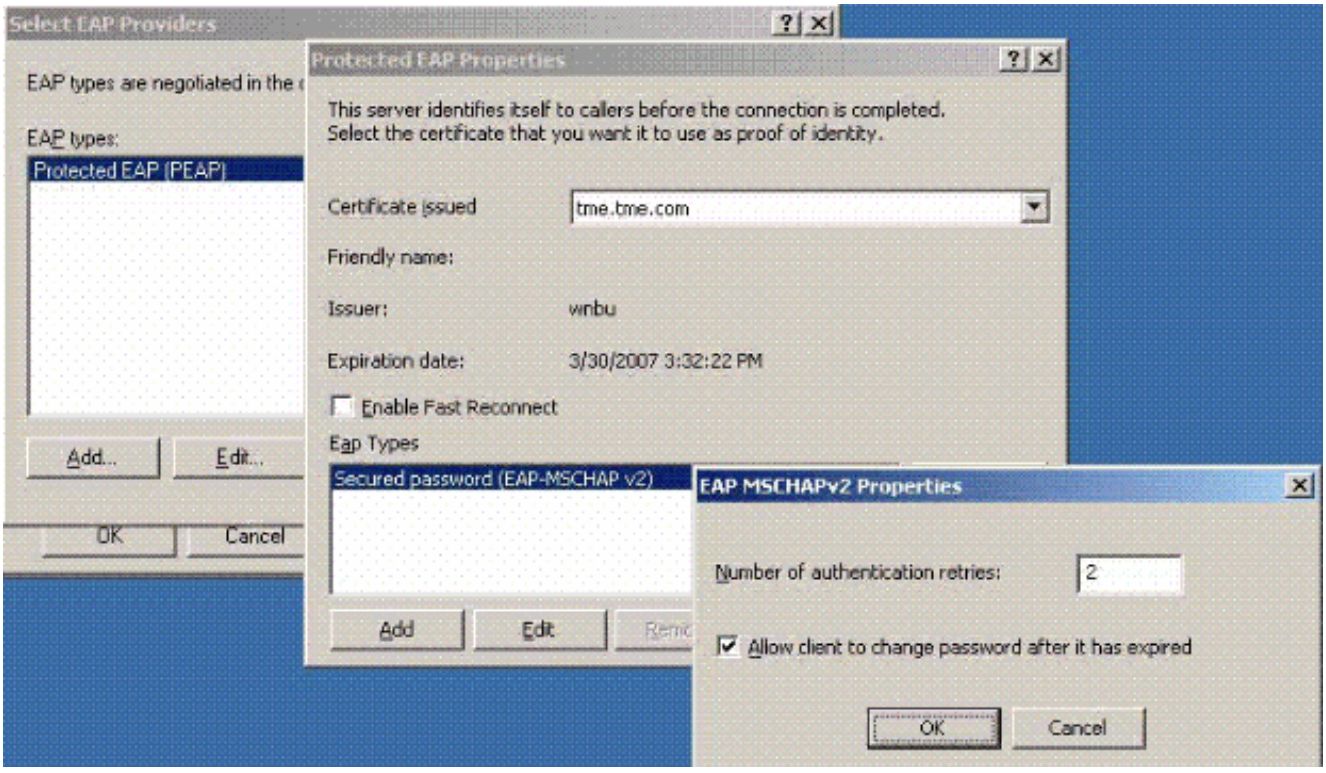
5. O clique **edita o perfil**, clica a aba da **autenticação**, e a verificação MS-CHAP v2 para a autenticação:



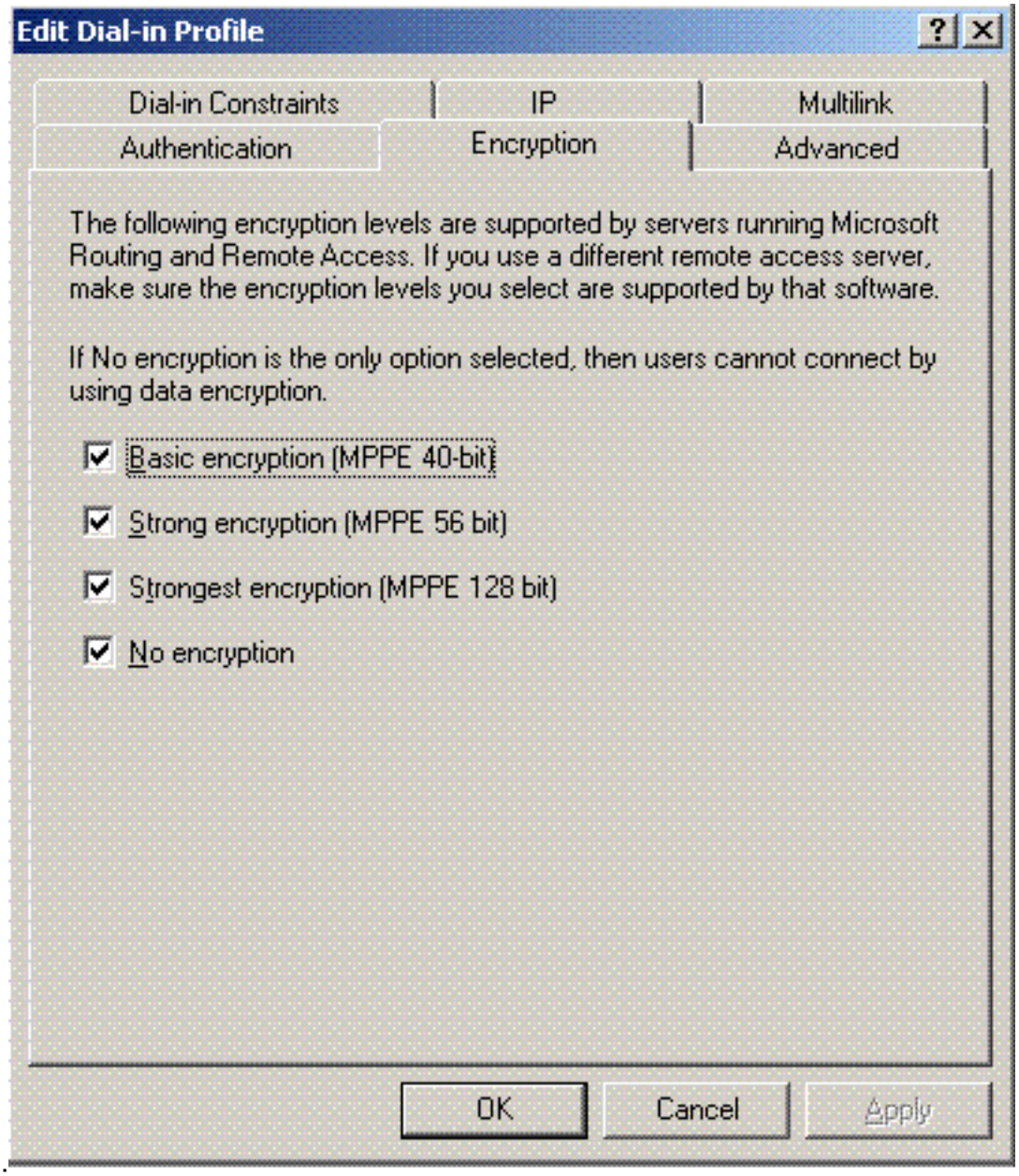
6. Clique **métodos de EAP**, selecione fornecedores EAP, e adicionar o PEAP como um tipo EAP:



7. O clique **edita em** fornecedores Select EAP e escolhe do menu que da tração para baixo o server associou com suas contas de usuário do diretório ativo e CA (por exemplo tme.tme.com). Adicionar o tipo MSCHAP v2
EAP:

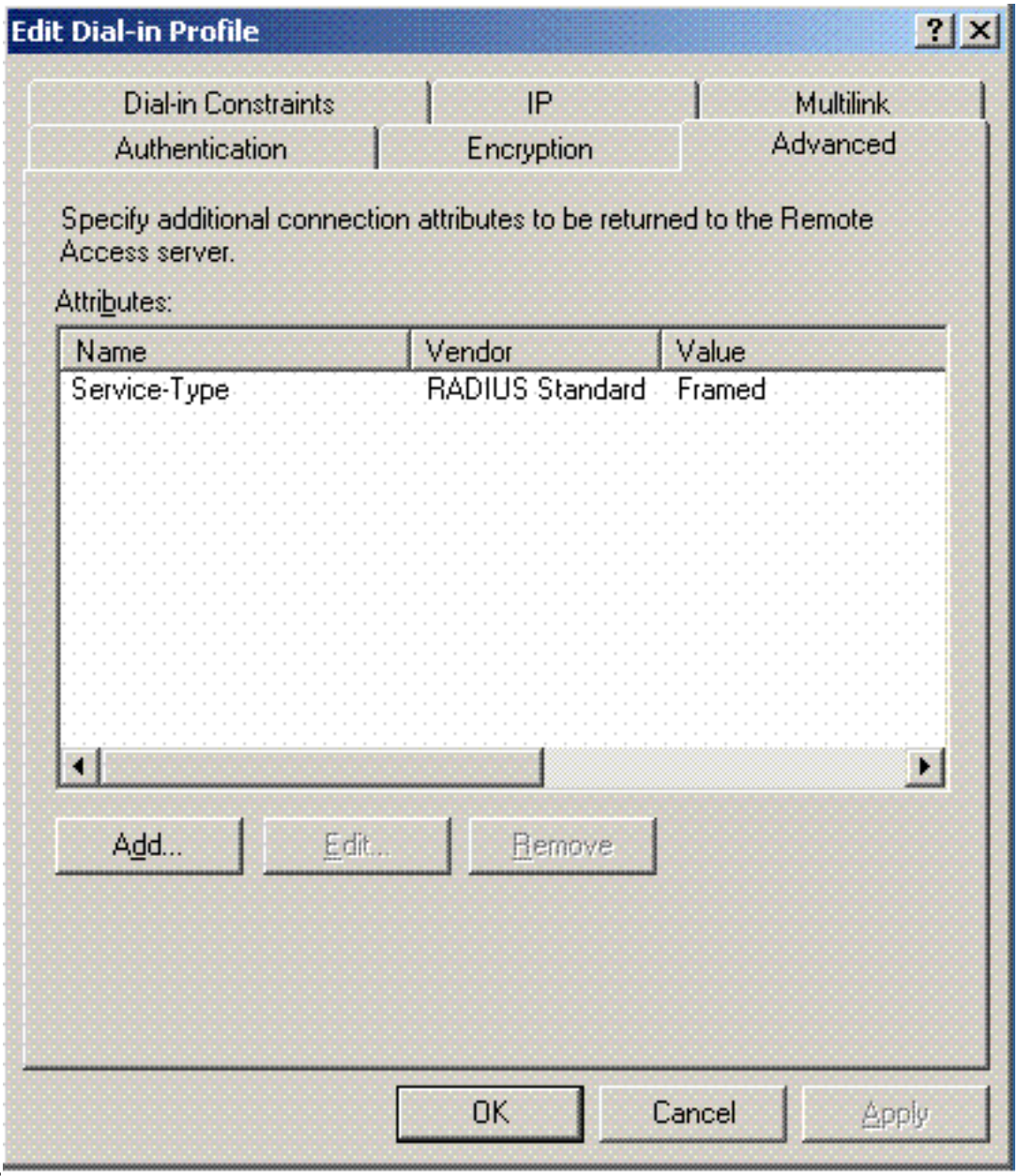


8. Clique a aba da **criptografia**, e verifique todos os tipos de criptografia para ver se há o



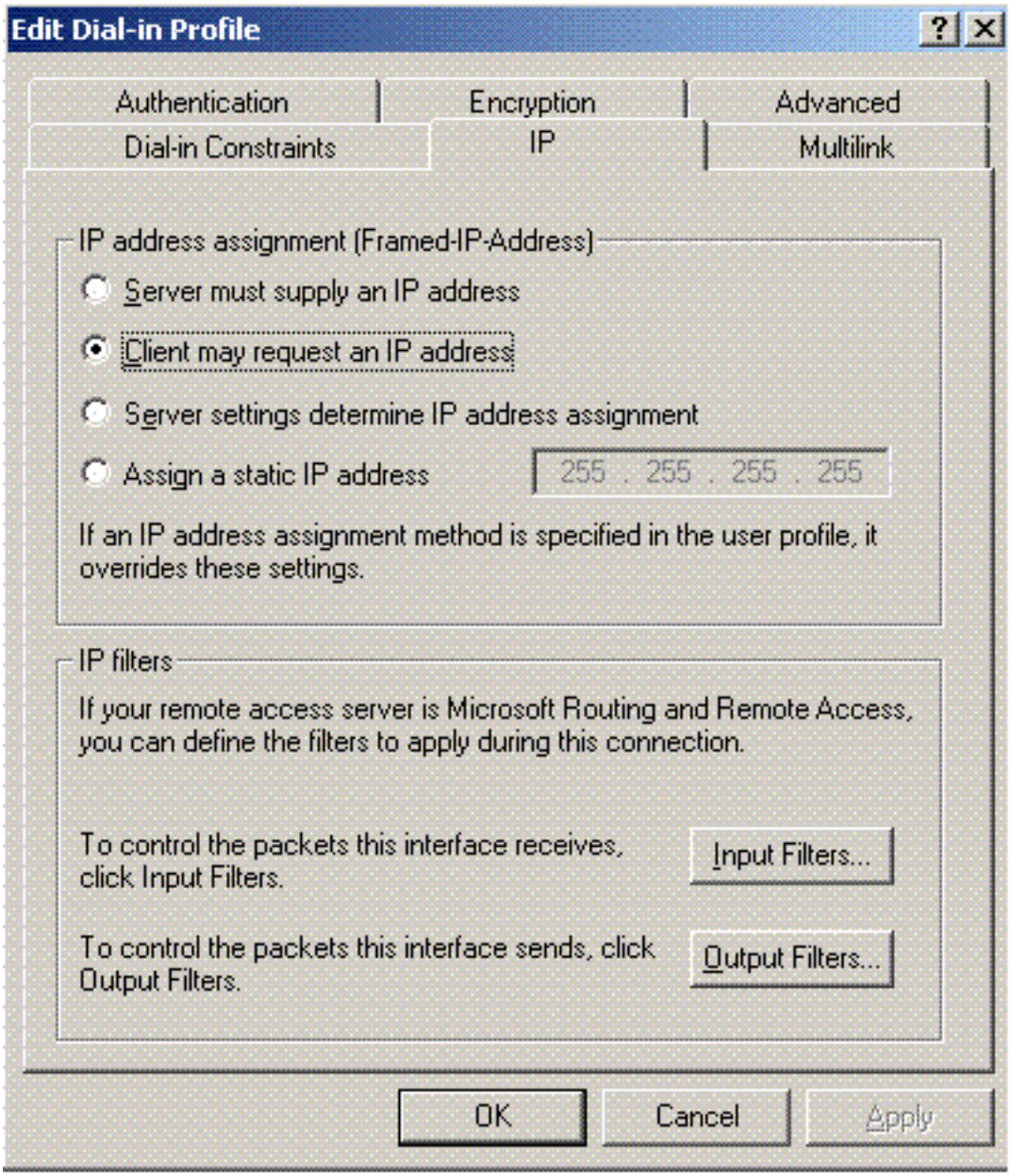
Acesso remoto:

9. Clique o **guia avançada**, e adicionar o padrão RADIUS/quadro como o tipo de



serviço:

10. Clique a aba **IP**, e o **cliente da** verificação **pode pedir um endereço IP de Um ou Mais Servidores Cisco ICM NT**. Isto supõe que você tem o DHCP permitido em um interruptor ou em um

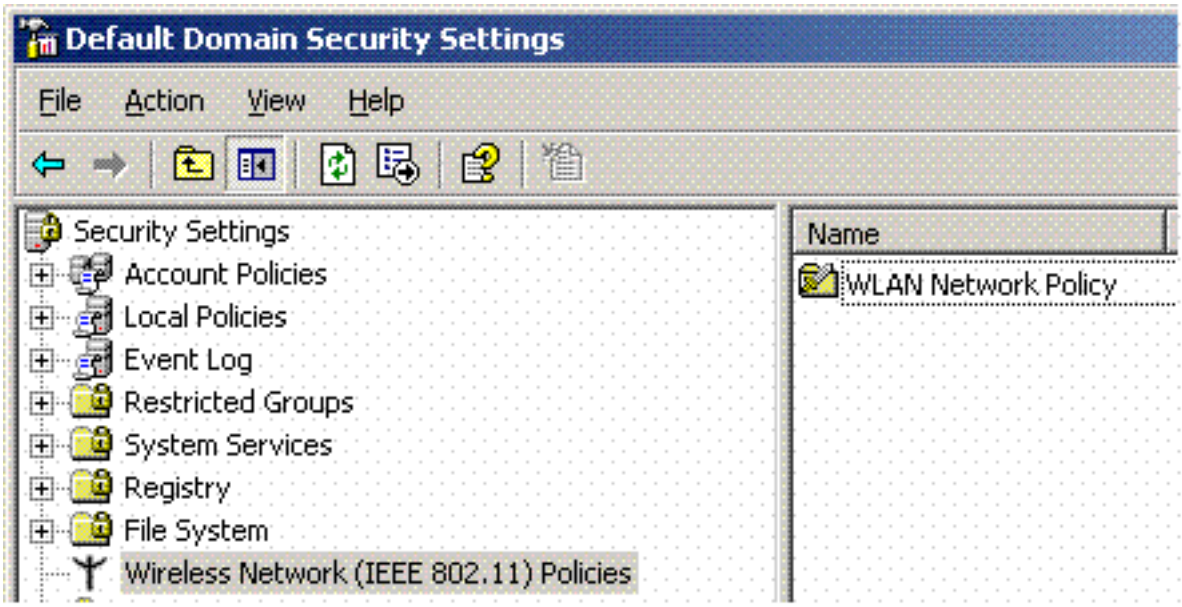


WinServer.

Microsoft Windows 2003 configurações de segurança do domínio

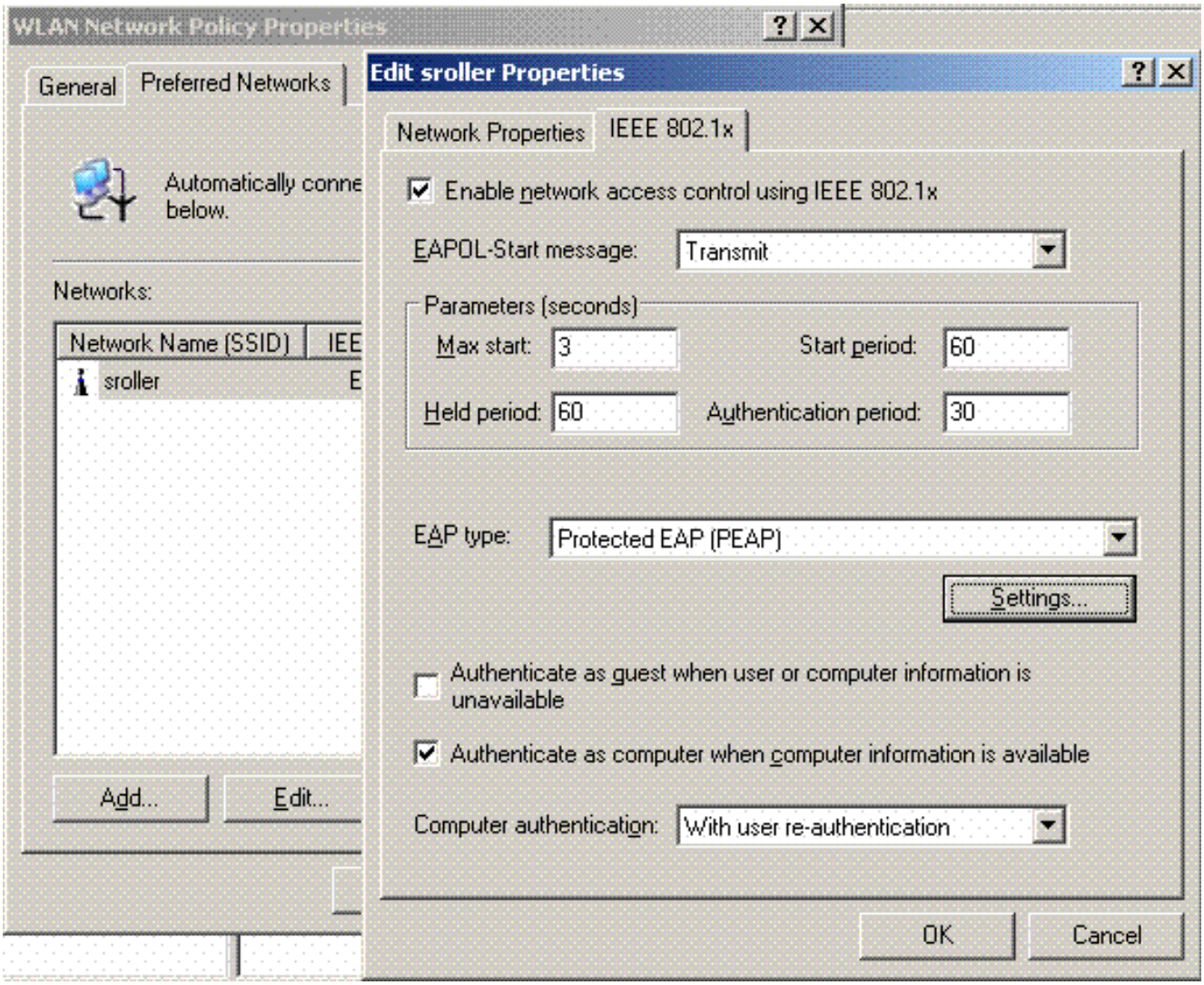
Termine estas etapas a fim configurar Windows 2003 configurações de segurança do domínio:

1. Lance o gerente das configurações de segurança do domínio padrão, e crie uma política de segurança nova para políticas da rede Wireless (IEEE



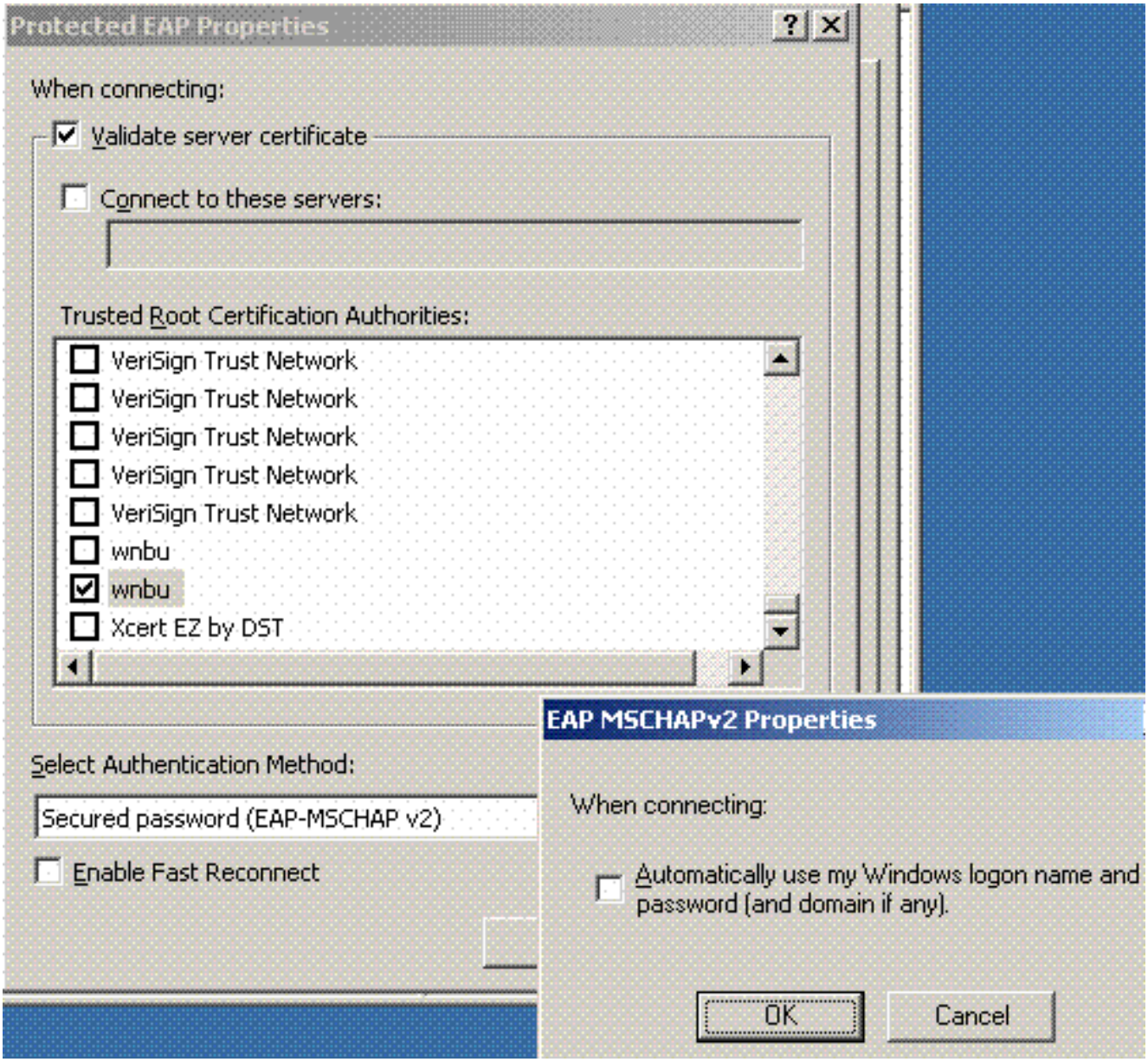
802.11).

2. As propriedades da política da rede de WLAN aberta, e o clique **preferiram redes**. Adicionar um WLAN preferido novo e datilografe o nome de seu WLAN SSID, tal como o `Sem fio`. Fazer duplo clique essa rede preferida nova, e clique a aba do **IEEE 802.1X**. Escolha o PEAP como o tipo
EAP:

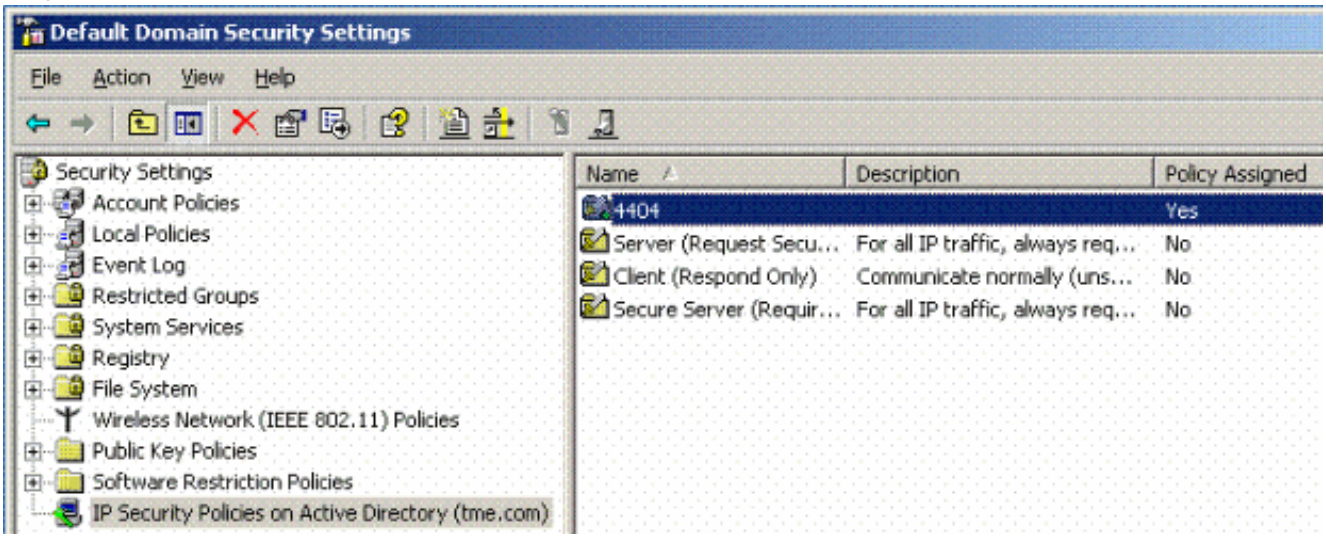


3. Clique **ajustes PEAP**, a verificação **valida o certificado de servidor**, e seleciona o CERT do root confiável instalado no Certificate Authority. Para propósitos testando, desmarcar a caixa da RACHADURA v2 MS para automaticamente usam meus início de uma sessão e senha

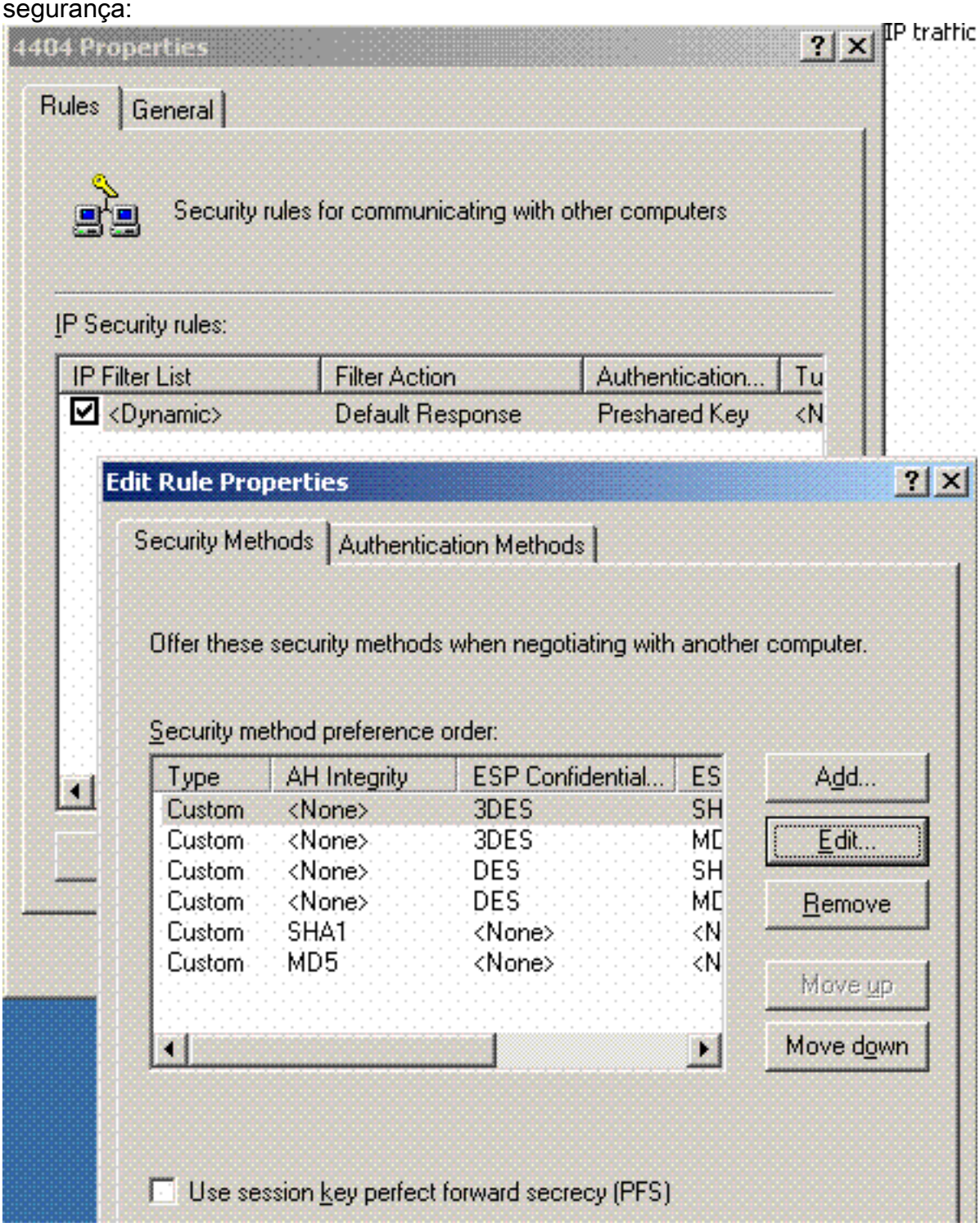
de
Windows.



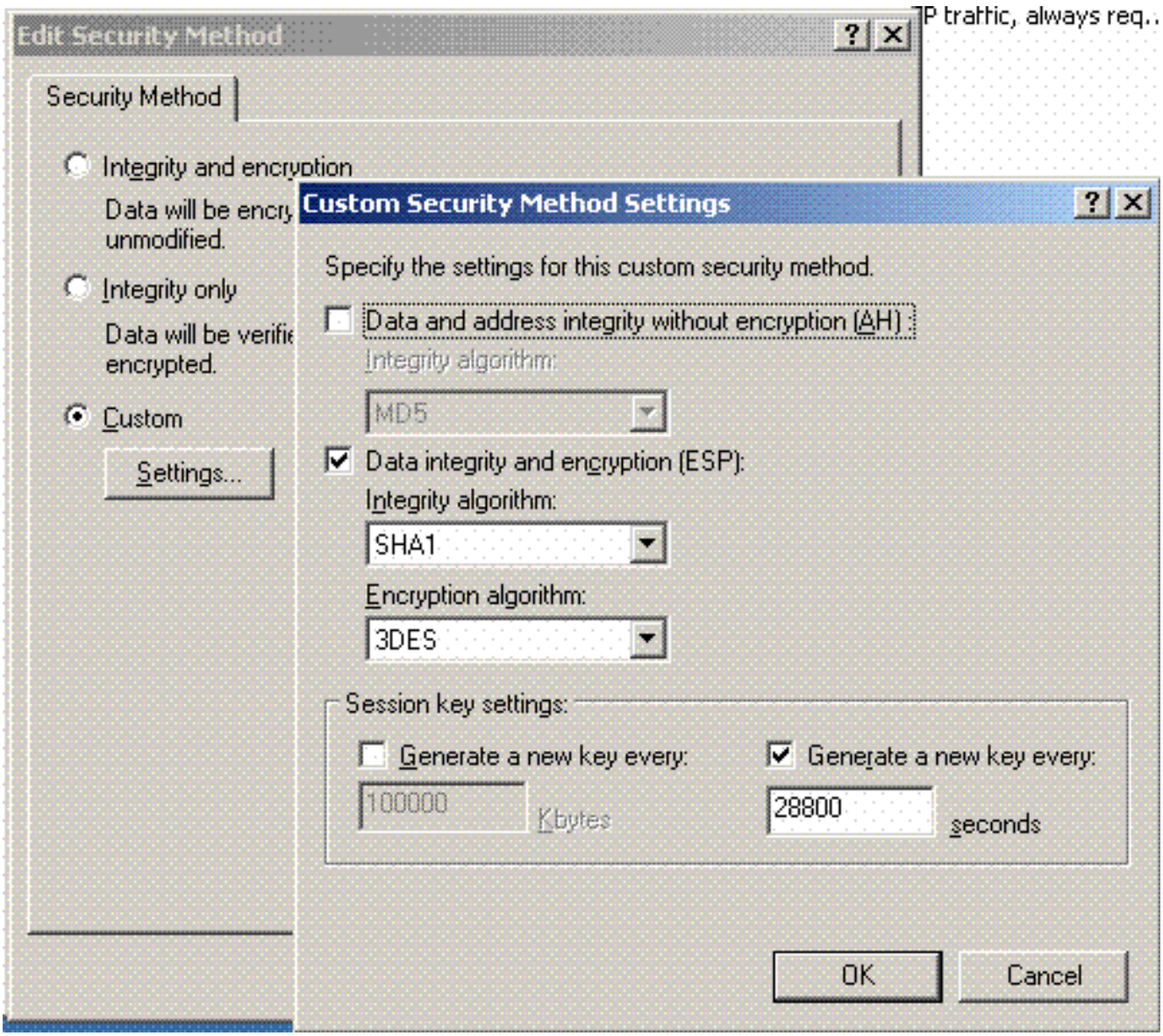
4. Na janela de gerenciador das configurações de segurança do domínio padrão de Windows 2003, crie umas outras políticas de Segurança IP novas na política do diretório ativo, tal como
4404.



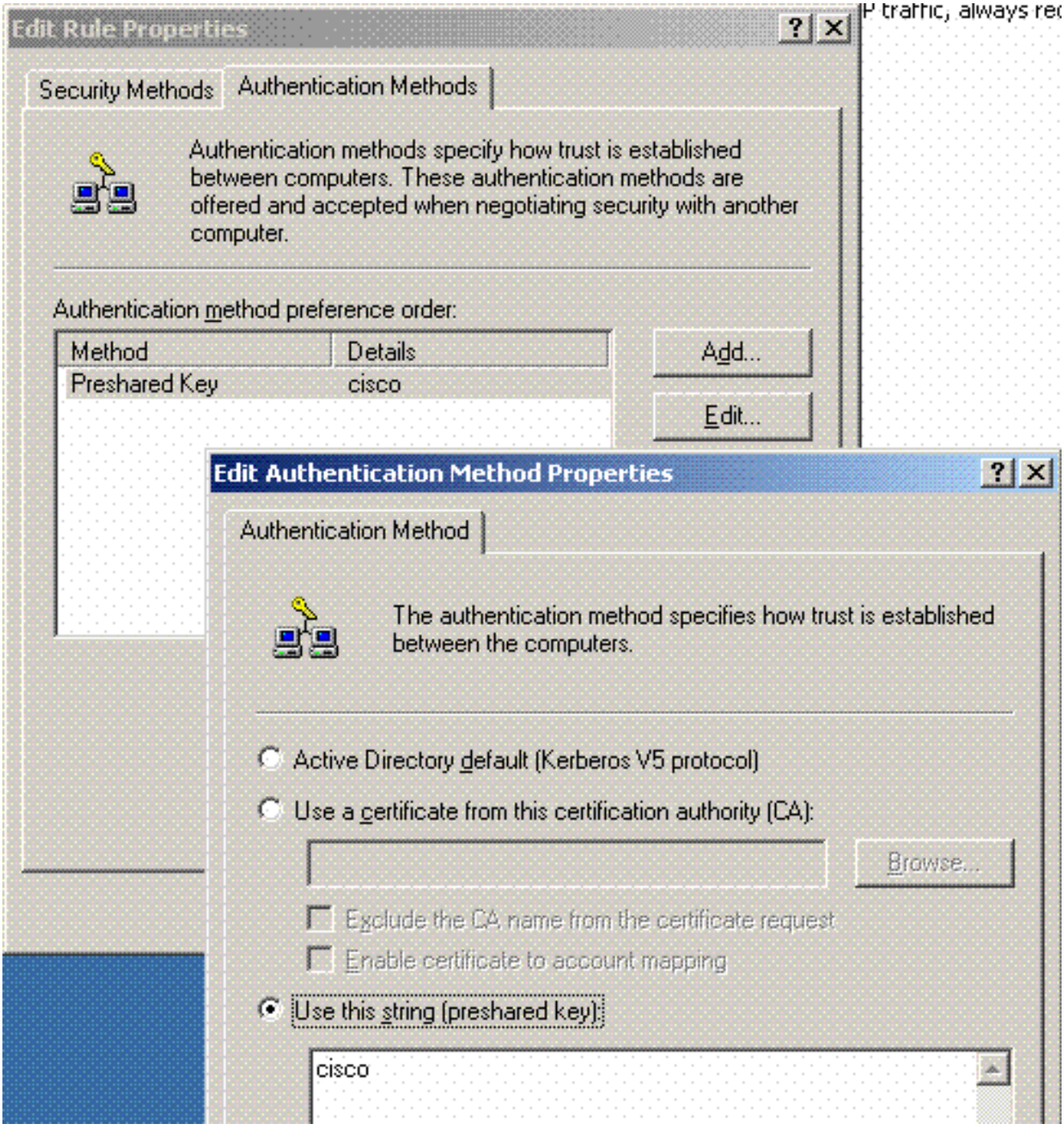
5. Edite as 4404 propriedades novas da política, e clique a aba das **regras**. Adicionar uma regra de filtro nova - O IP enfaixa a lista (dinâmica); Ação do filtro (resposta do padrão); Autenticação (PSK); Túnel (nenhum). Fazer duplo clique a regra de filtro recém-criado e selecione métodos de
segurança:



6. O clique **edita o método de segurança**, e clica o botão de rádio das **configurações personalizadas**. Escolha estes ajustes.**Nota:** Estes ajustes devem combinar os ajustes da segurança IPSec do RAIO do
controlador.



7. Clique a aba do **método de autenticação** sob as propriedades da regra da edição. Incorpore o mesmo segredo compartilhado que você incorporou previamente na configuração RADIUS do
controlador.



Neste momento, todas as configurações para o controlador, IAS e as configurações de segurança do domínio são terminados. Salvar todas as configurações no controlador e em WinServer e recarregue todas as máquinas. No cliente de WLAN que é usado testando, instale o CERT da raiz e configurar-lo para WPA2/PEAP. Depois que o CERT da raiz é instalado no cliente, recarregue a máquina cliente. Afinal as máquinas recarregam, conectam o cliente ao WLAN e capturam estes eventos do log.

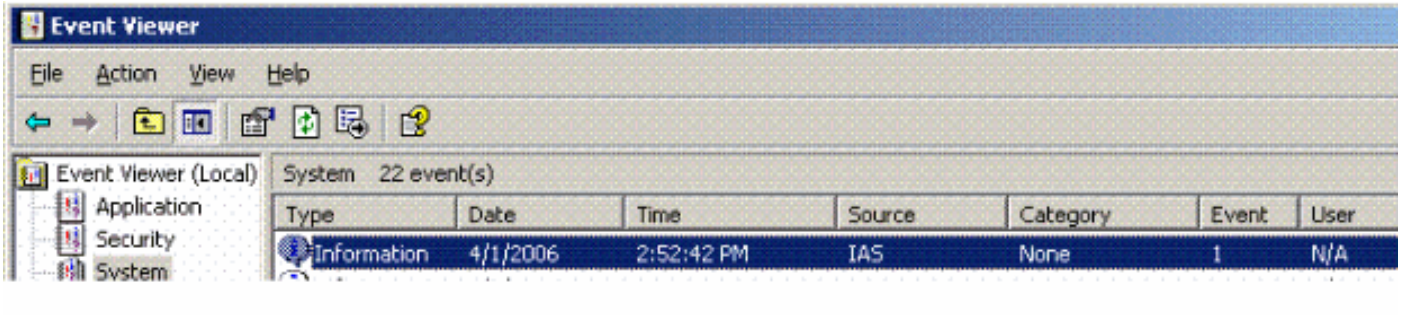
Nota: Uma conexão de cliente é exigida a fim estabelecer a conexão IPSec entre o RAIO do controlador e do WinServer.

Windows 2003 eventos do log de sistema

Uma conexão bem sucedida do cliente de WLAN configurada para WPA2/PEAP com o RAIO do IPsec permitido gerencie este evento do sistema no WinServer:

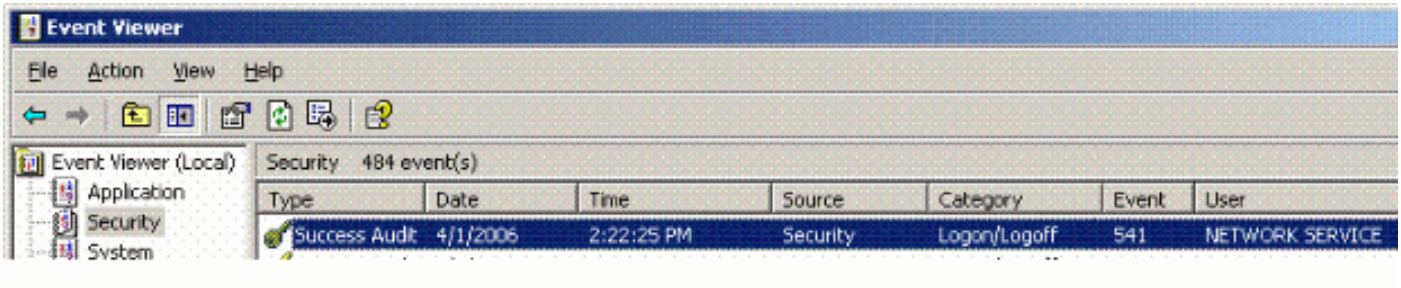
```
192.168.30.105 = WinServer
```

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)
```

Uma conexão IPSec bem sucedida do RAIO do <> do controlador gerencie este evento de segurança nos logs 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
```

O sucesso do IPsec do RAIO do controlador do Wireless LAN debuga o exemplo

Você pode usar o comando debug **debuga o ikemsg pm permite no** controlador a fim verificar esta configuração. Exemplo:

```
(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
```

Captação de Ethreal

Está aqui uma captação de Ethreal da amostra.

```
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
```

Informações Relacionadas

- Manual de configuração do controlador de LAN do Cisco Wireless, liberação 5.2
- Suporte Técnico e Documentação - Cisco Systems