RADIUS IPSec-beveiliging voor WLC's en Microsoft Windows 2003 IAS-server configureren

Inhoud

Inleiding

Deze handleiding beschrijft hoe de RADIUS IPSec-functie moet worden geconfigureerd die wordt ondersteund door WCS en deze WLAN-controllers:

- 4400 Series
- WiSM
- 3750G

De functie Controller RADIUS IPSec bevindt zich op de Controller GUI onder de sectie **Security > AAA > RADIUS-verificatieservers**. Deze voorziening biedt u een methode om alle RADIUS-communicatie tussen controllers en RADIUS-servers (IAS) te versleutelen met IPSec.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis over LWAPP
- Kennis van RADIUS-verificatie en IPSec
- Kennis over het configureren van services op het besturingssysteem Windows 2003 Server

Gebruikte componenten

Deze netwerk- en softwarecomponenten moeten worden geïnstalleerd en geconfigureerd om de controller RADIUS IPSec-functie te kunnen implementeren:

- WLC 4400, WiSM of 3750G controllers. In dit voorbeeld wordt WLC 4400 gebruikt, dat softwareversie 5.2.178.0 uitvoert
- Lichtgewicht access points (LAP's). In dit voorbeeld wordt de 1231-serie LAP gebruikt.
- Switch met DHCP
- Microsoft 2003-server geconfigureerd als een domeincontroller die is geïnstalleerd met Microsoft Certificate Authority en met Microsoft Internet Verification Service (IAS).
- Microsoft Domain Security Appliance
- Cisco 802.11 a/b/g draadloze clientadapter met ADU versie 3.6 geconfigureerd met WPA2/PEAP

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Configuratie van IPSec RADIUS

Deze configuratiehandleiding is niet van toepassing op de installatie of configuratie van Microsoft WinServer, Certificate Authority, Active Directory of WLAN 802.1x-client. Deze componenten moeten voorafgaand aan de implementatie van de controller IPSec RADIUS-functie worden geïnstalleerd en geconfigureerd. De rest van deze handleiding legt uit hoe IPSec RADIUS op deze componenten moet worden geconfigureerd:

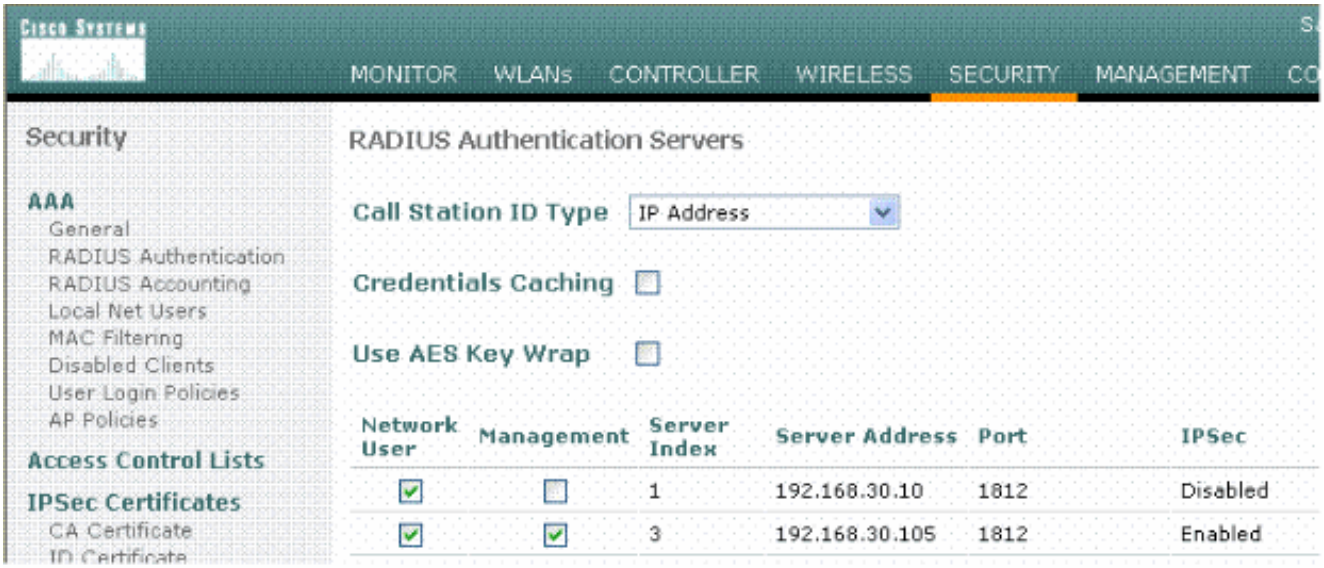
1. Cisco WLAN-controllers
2. Windows 2003 IAS
3. Beveiligingsinstellingen Microsoft Windows-domein

De WLC configureren

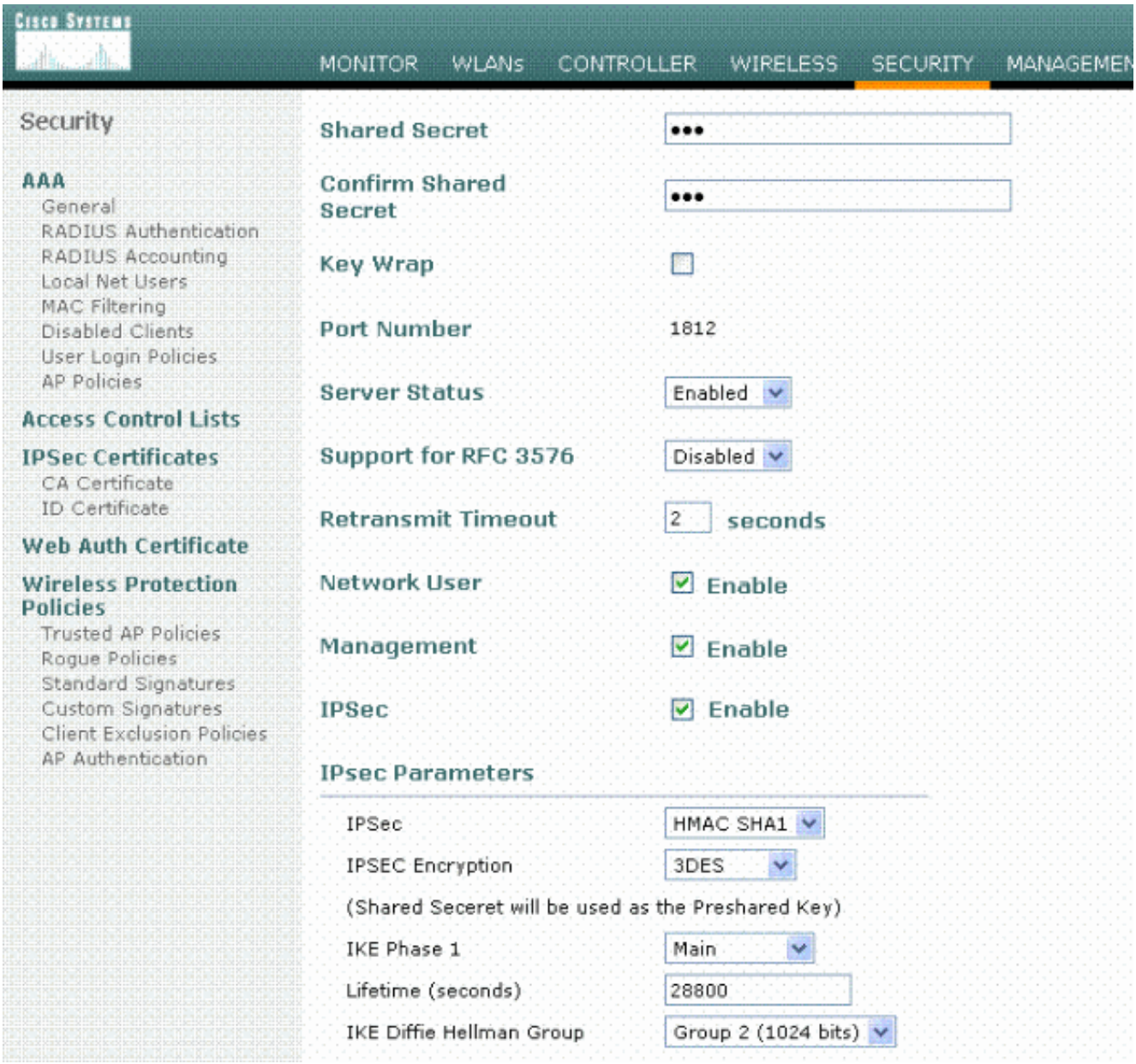
Deze sectie verklaart hoe u IPSec op de WLC kunt configureren via de GUI.

Voltooi deze stappen vanuit de controller-GUI.

1. Navigeer naar het tabblad **Security > AAA > RADIUS-verificatie** in de Controller GUI en voeg een nieuwe RADIUS-server
   toe.



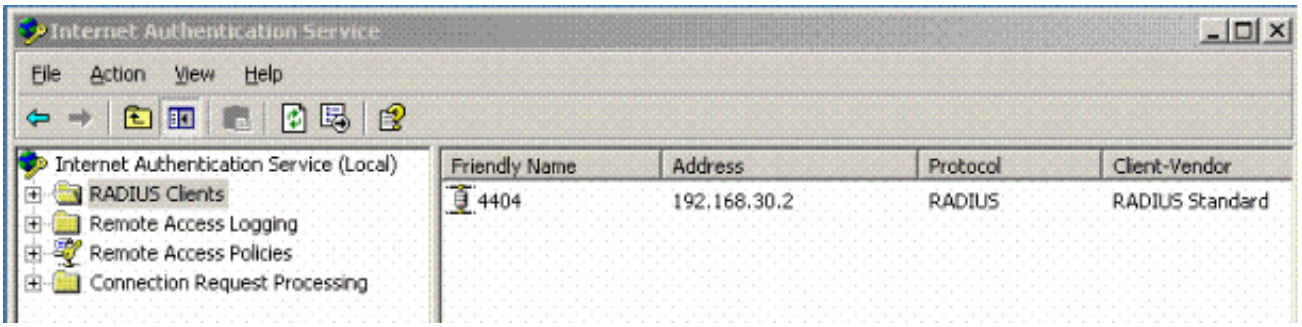
2. Configureer het IP-adres, poort 1812 en een gedeeld geheim van de nieuwe RADIUS-server. Controleer het vakje **Inschakelen**-controle van **IPSec**, configureer deze IPSec-parameters en klik vervolgens op **Toepassen**.**Opmerking:** het gedeelde geheim wordt gebruikt voor de verificatie van de RADIUS-server en als de vooraf gedeelde sleutel (PSK) voor IPSec-verificatie.



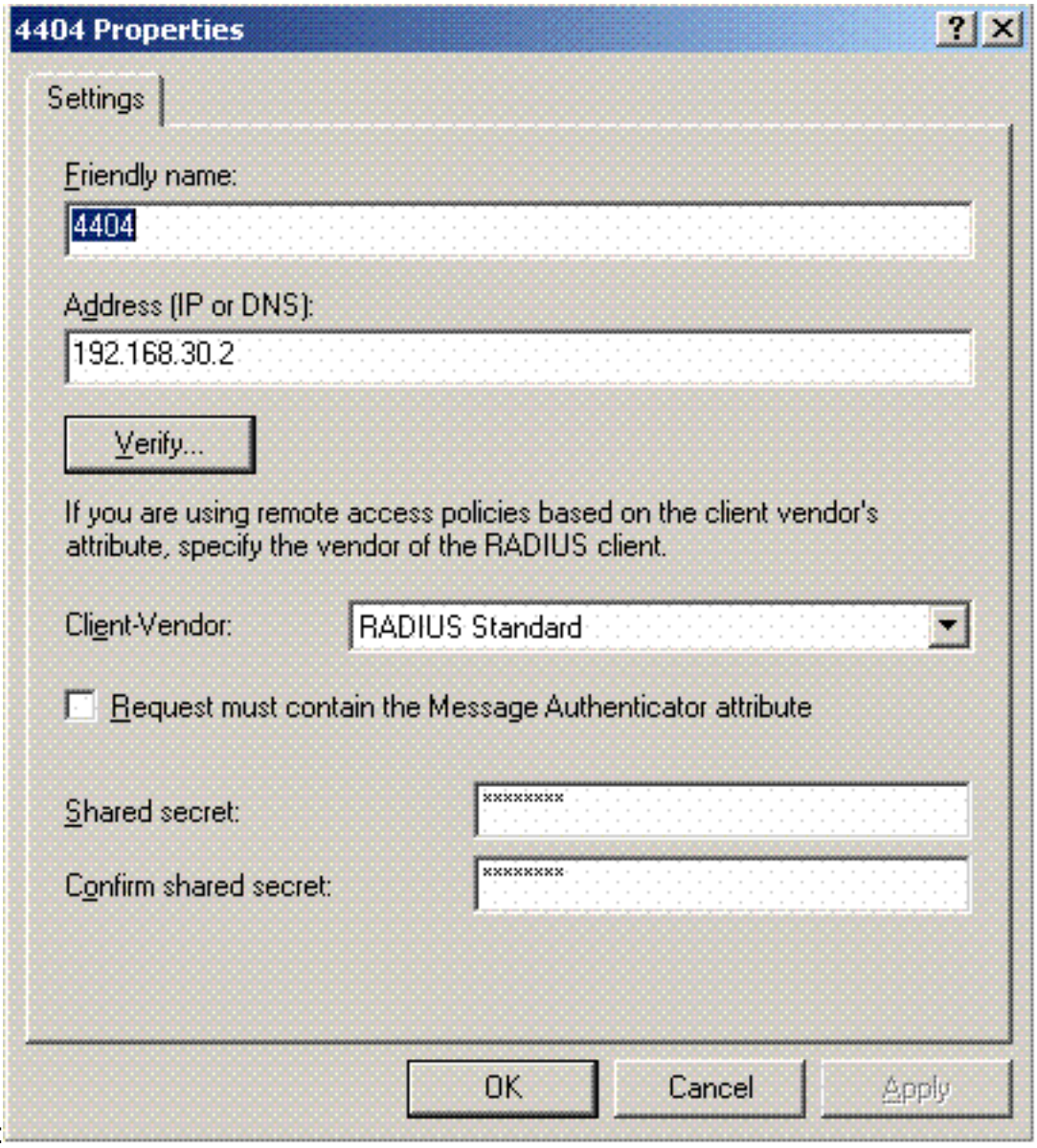
De IAS configureren

Voltooi de volgende stappen in de IAS:

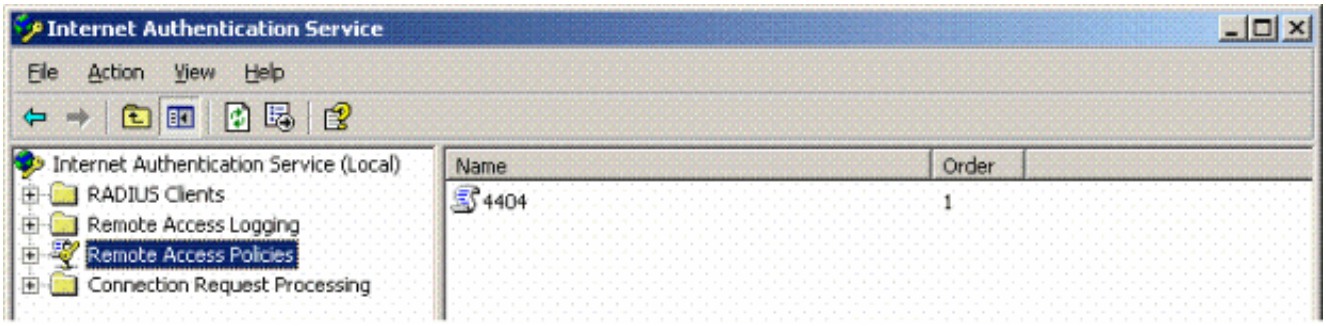
1. Navigeer naar de IAS-beheerder in Win2003 en voeg een nieuwe RADIUS-client toe.



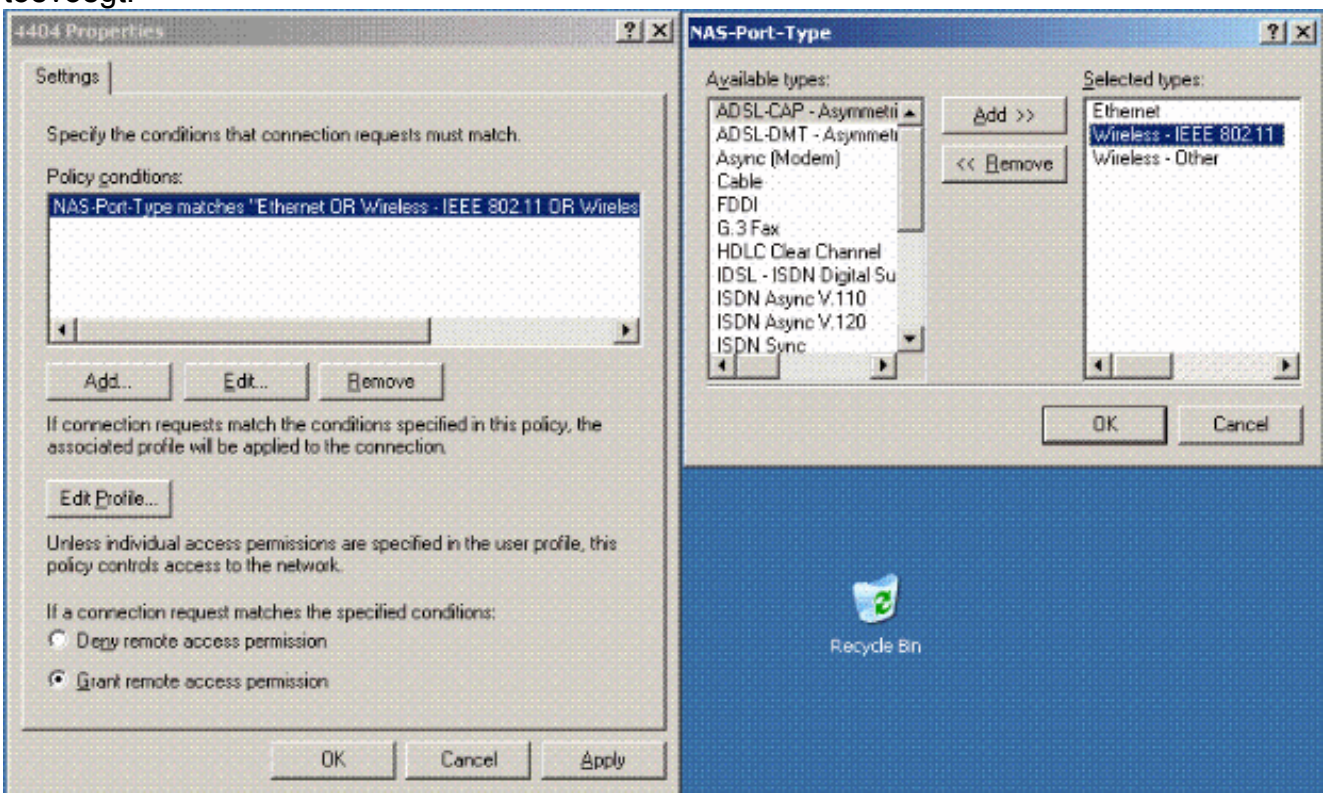
2. Configureer de RADIUS-clienteigenschappen met het IP-adres en het gedeelde geheim dat op de controller is geconfigureerd:



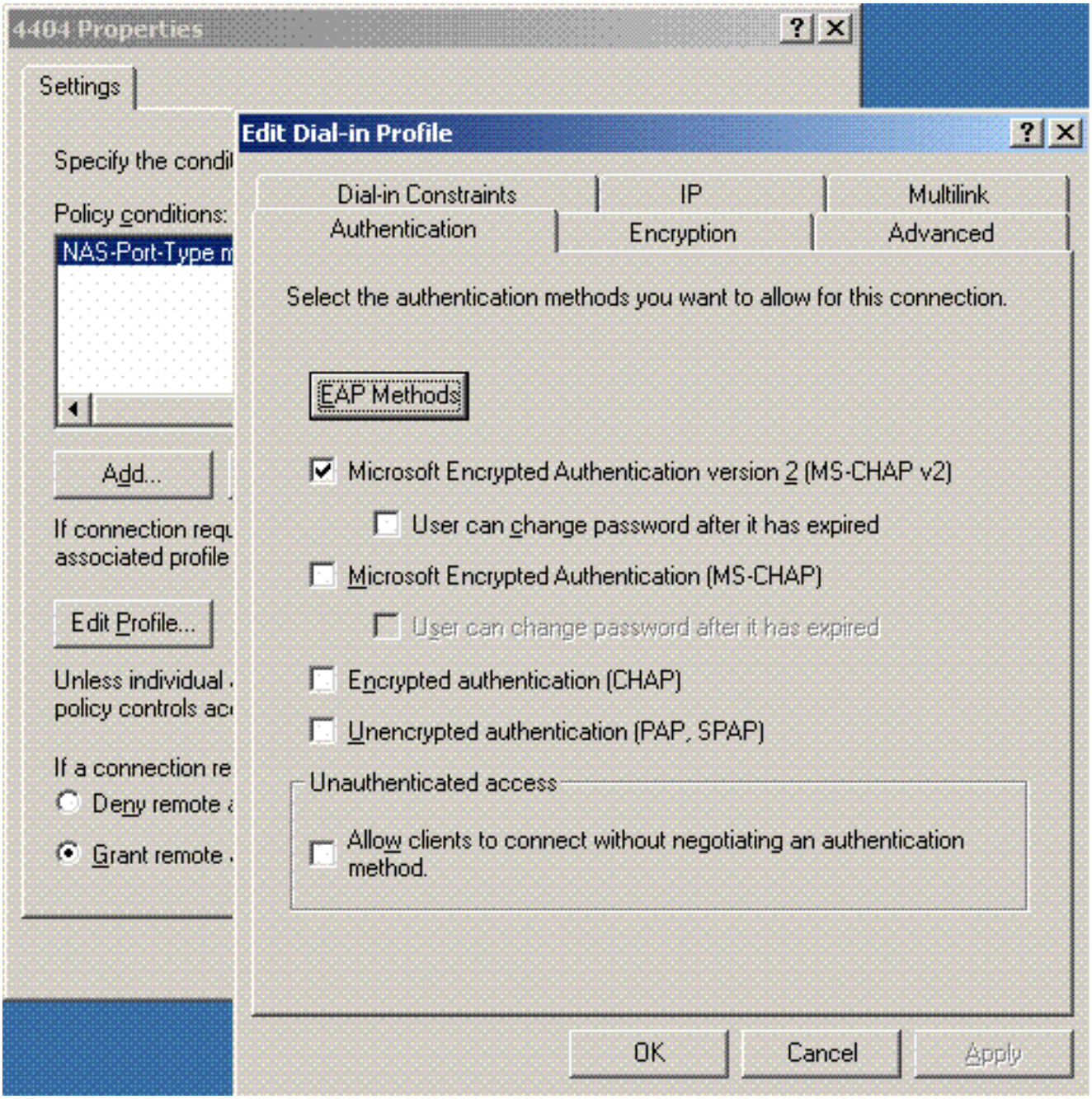
3. Configureer een nieuw beleid voor externe toegang voor de controller:



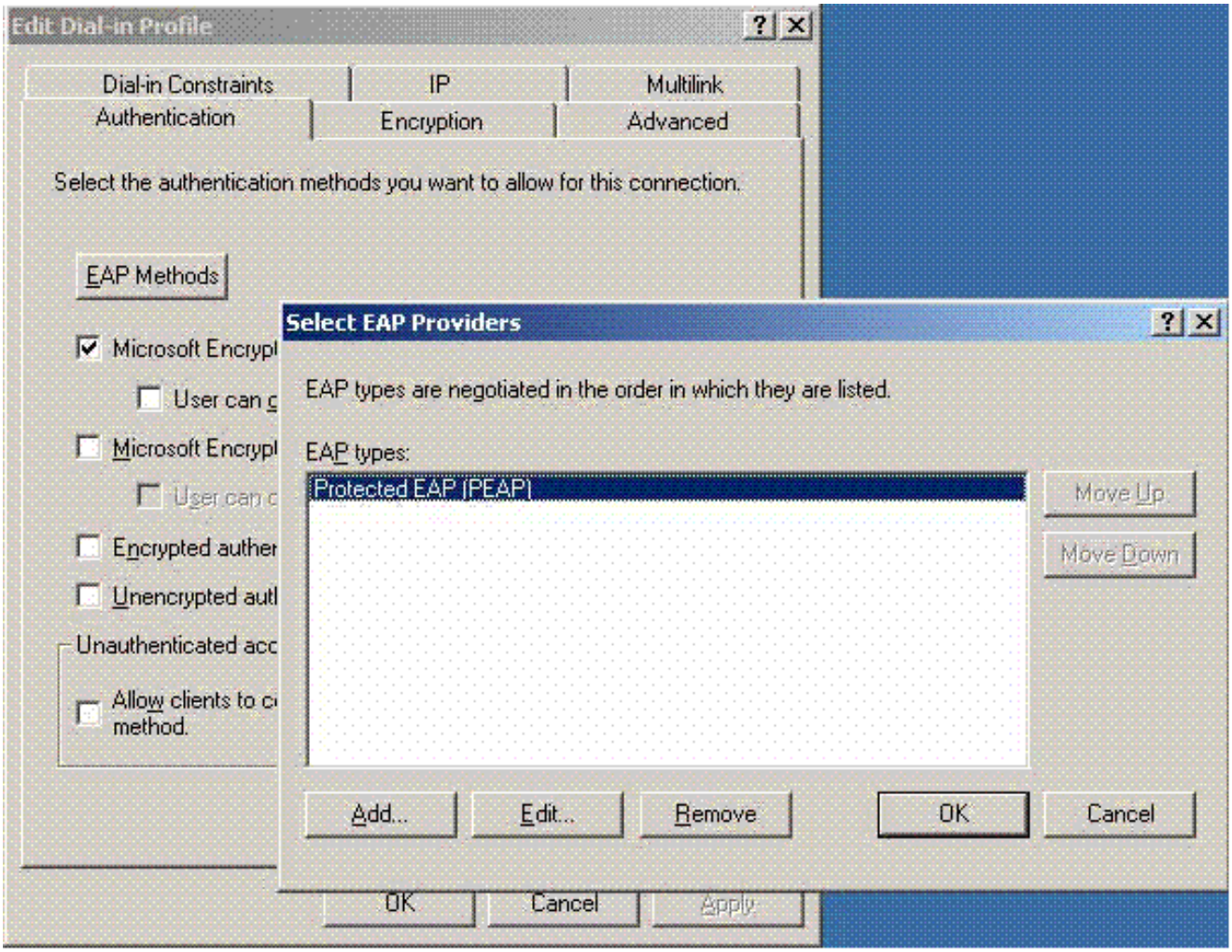
4. Bewerk de eigenschappen van het Controller Remote Access Policy. Zorg ervoor dat u het NAS-poorttype - Draadloos - IEEE 802.11 toevoegt:



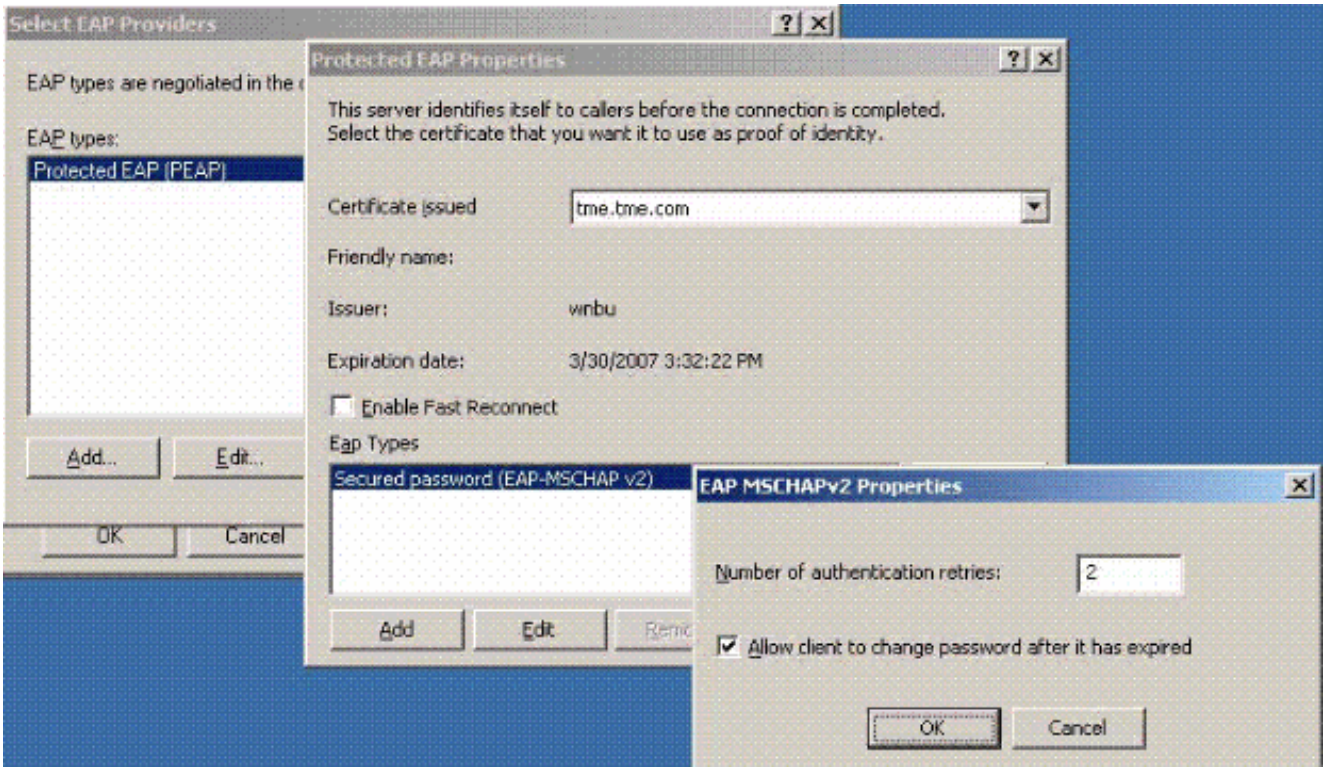
5. Klik op **Profiel bewerken**, klik op het tabblad **Verificatie** en controleer MS-CHAP v2 op Verificatie:



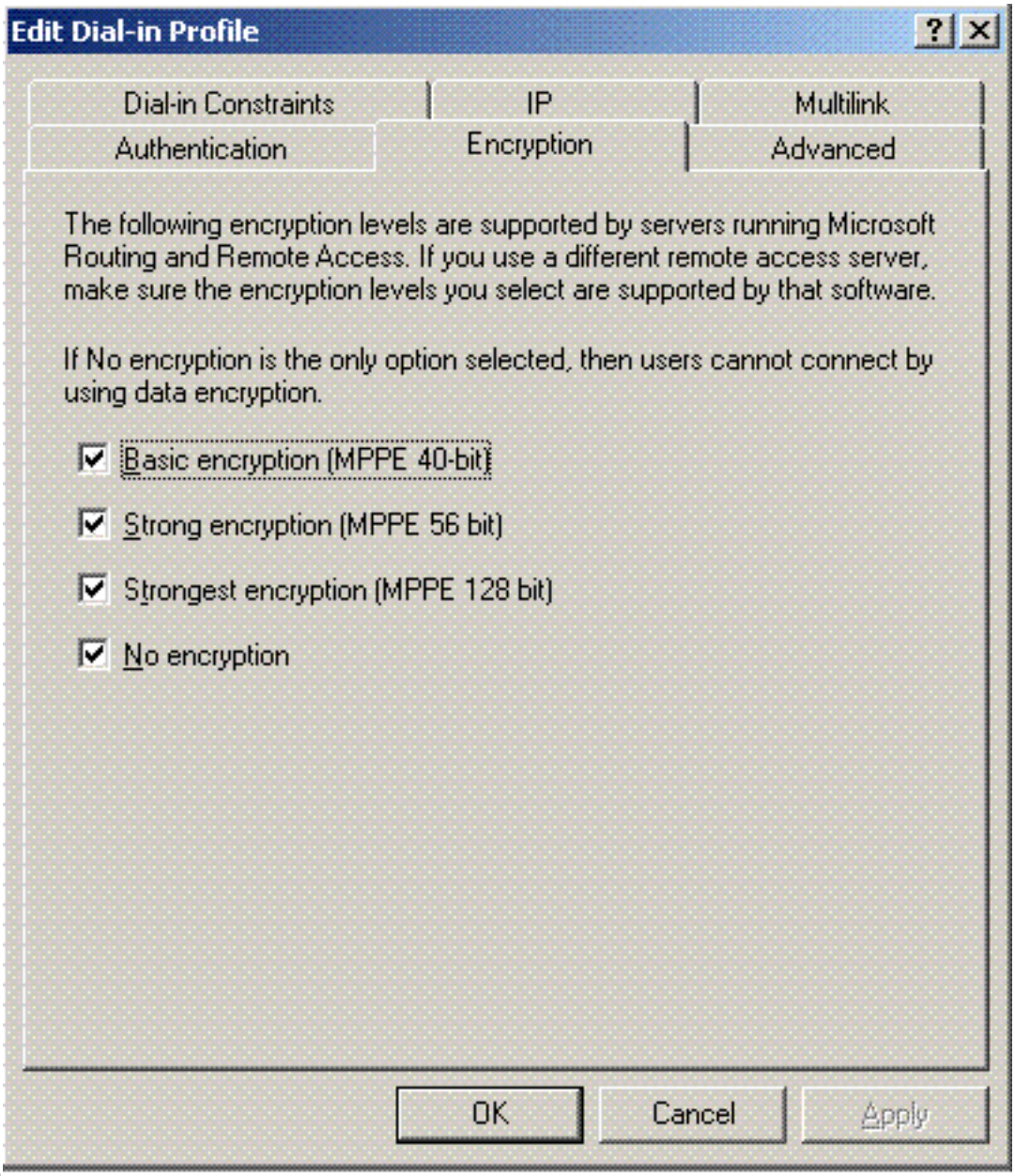
6. Klik op **EAP Methods**, selecteer EAP Providers en voeg PEAP toe als een EAP-type:



7. Klik op **Bewerken** op Selecteer EAP Providers en kies in het keuzemenu de server die is gekoppeld aan uw Active Directory-gebruikersaccounts en CA (bijvoorbeeld tme.tme.com). Voeg het EAP-type MSCHAP v2
toe:

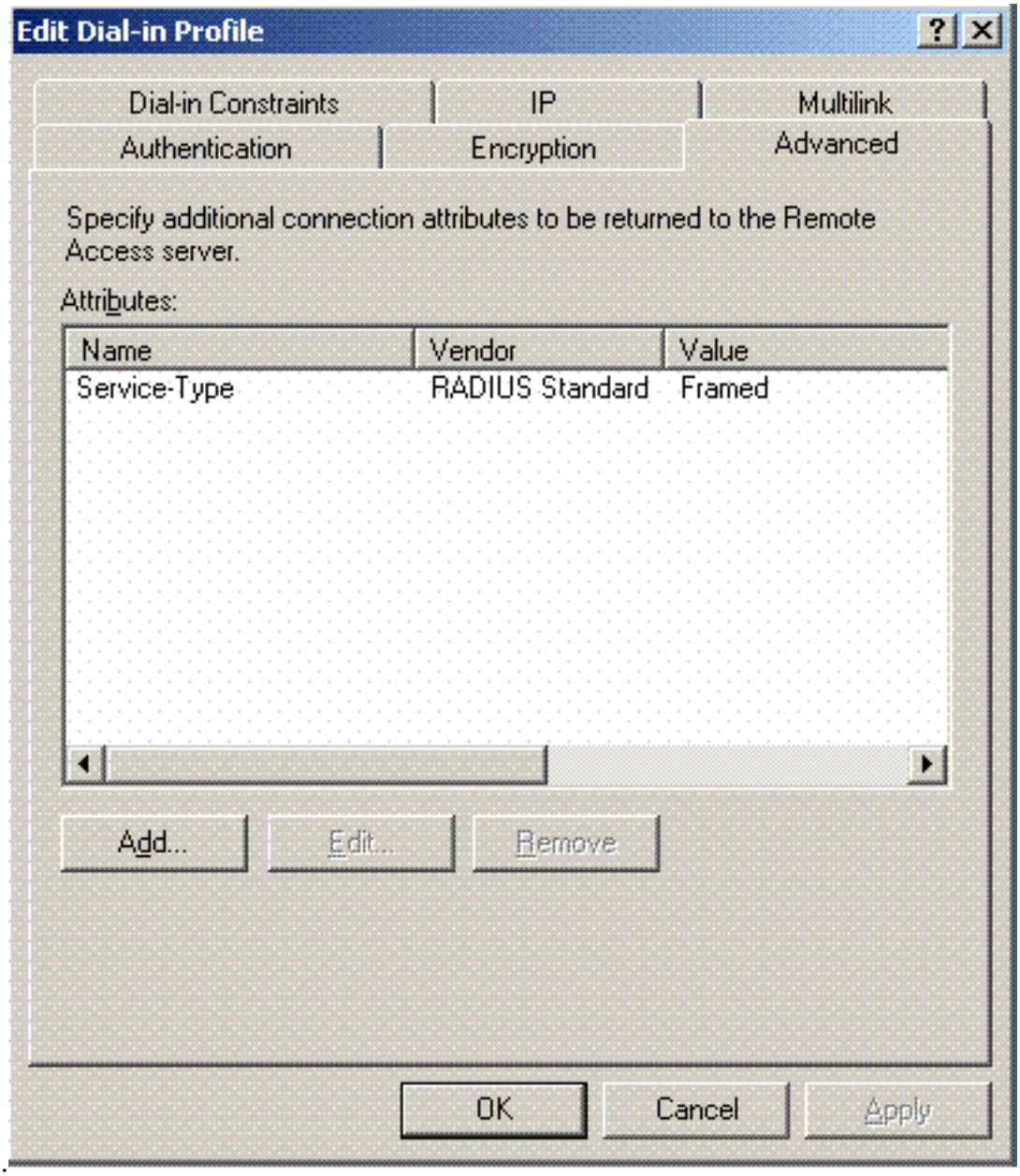


8. Klik op het tabblad **Encryptie** en controleer alle coderingstypen voor externe



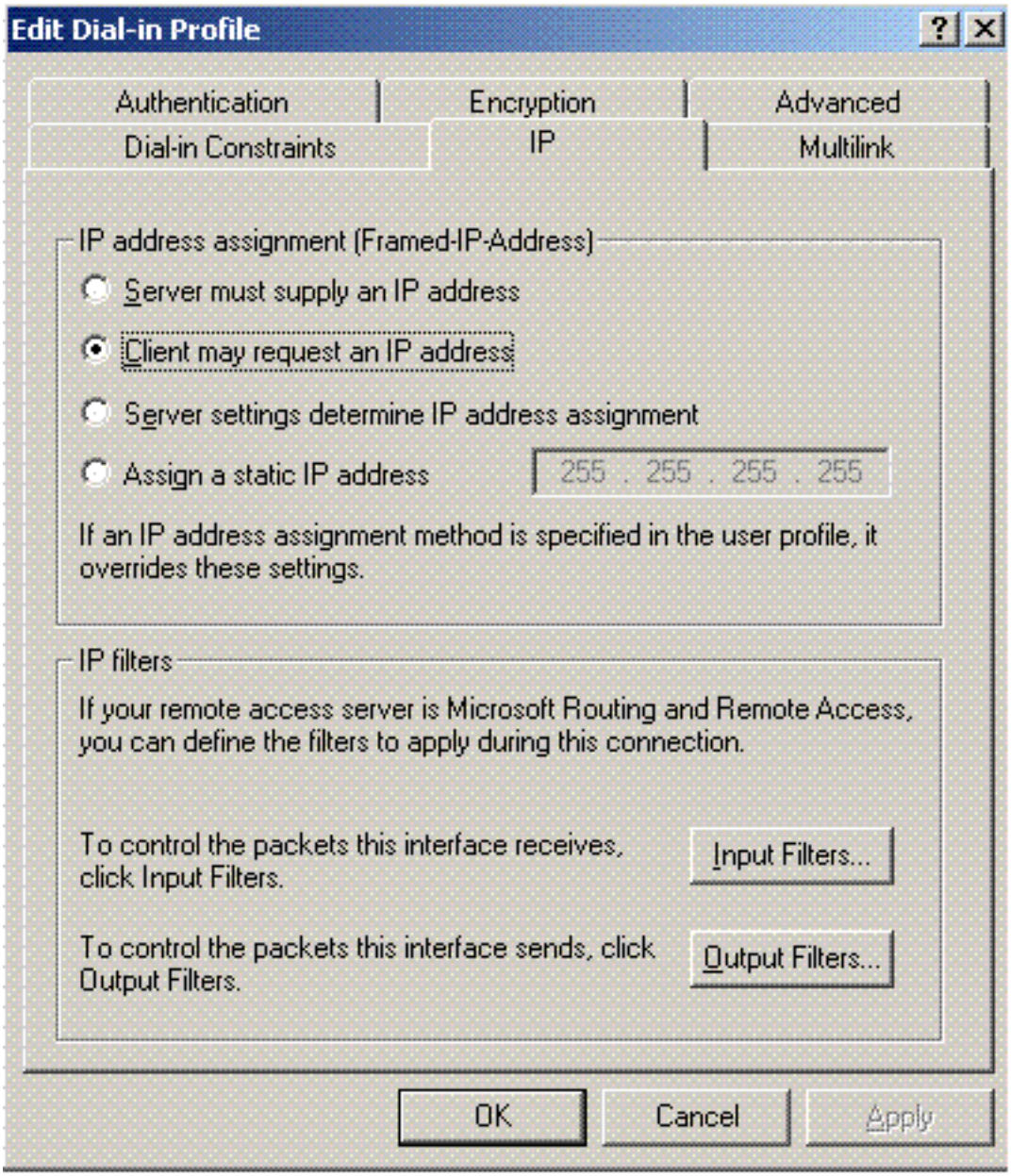
toegang:

9. Klik op het tabblad **Geavanceerd** en voeg RADIUS-standaard/framed toe als het



servicetype:

10. Klik op het tabblad **IP** en controleer of **de client een IP-adres kan aanvragen**. Dit veronderstelt dat DHCP is ingeschakeld op een switch of

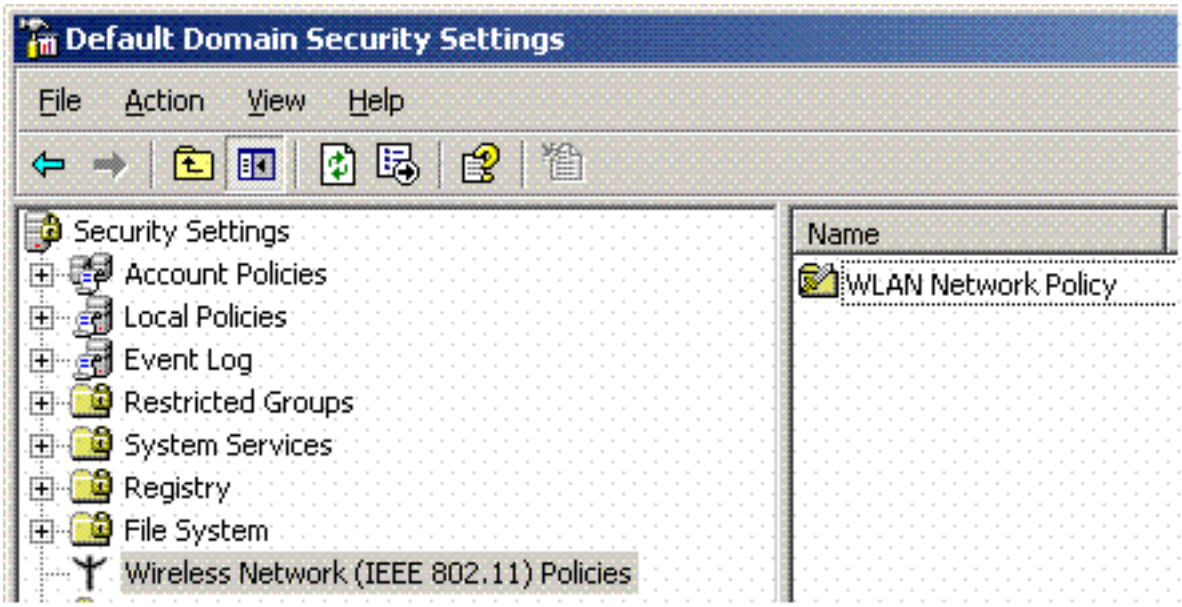


WinServer.

Microsoft Windows 2003 domeinbeveiligingsinstellingen

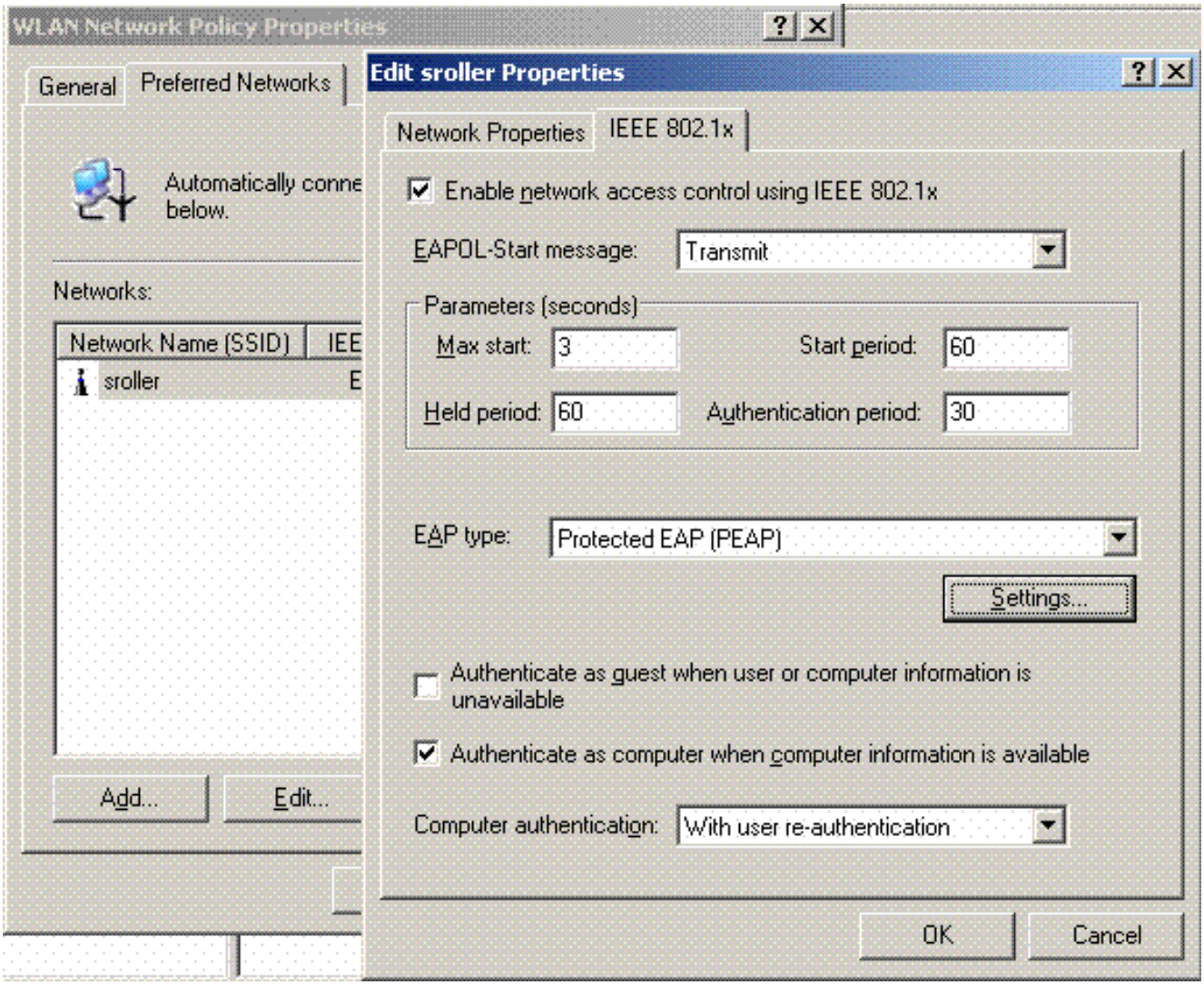
Voltooi de volgende stappen om de beveiligingsinstellingen voor het domein van Windows 2003 te configureren:

1. Start Default Domain Security Settings Manager en maak een nieuw beveiligingsbeleid voor het beleid voor draadloze netwerken (IEEE

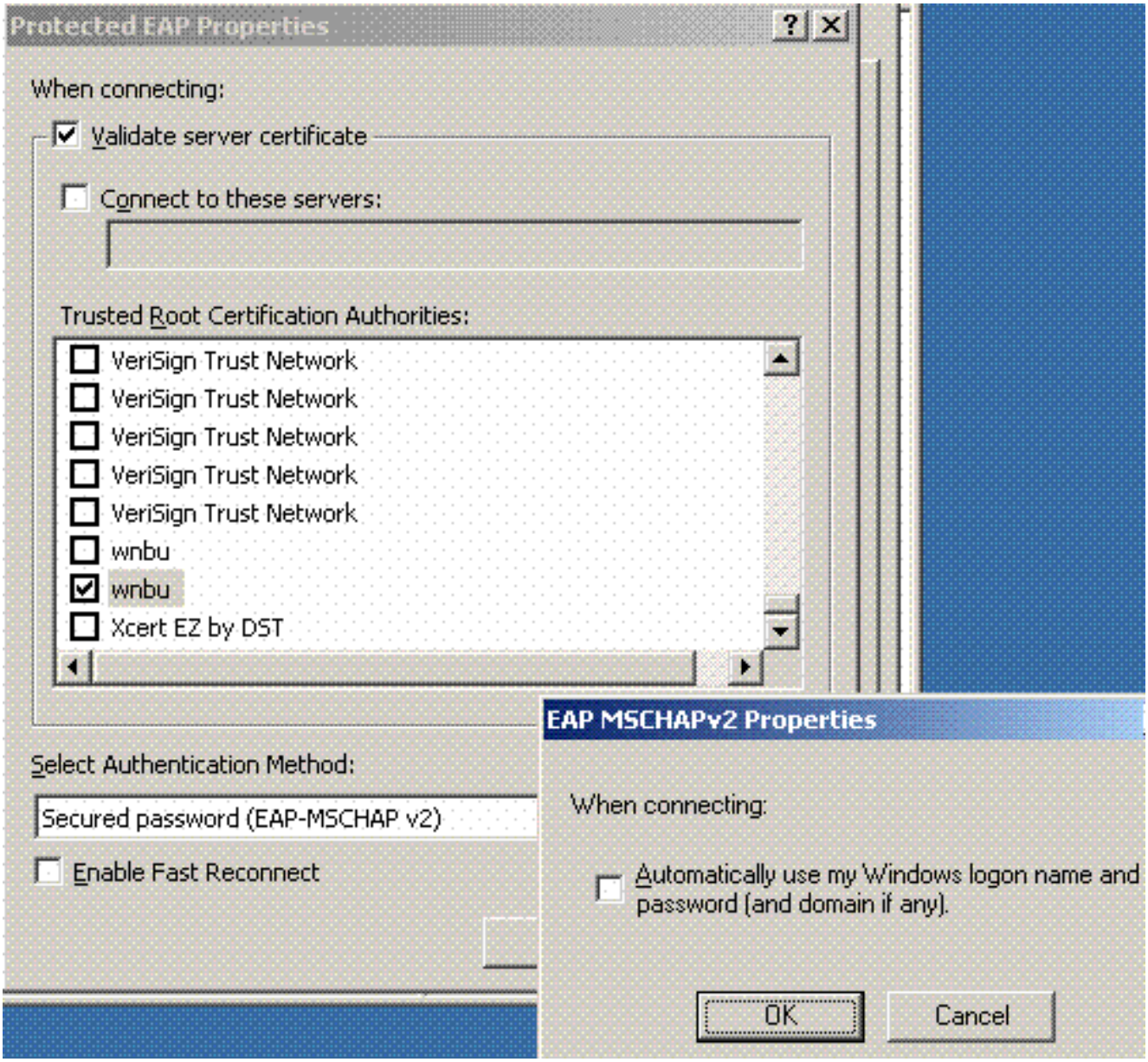


802.11).

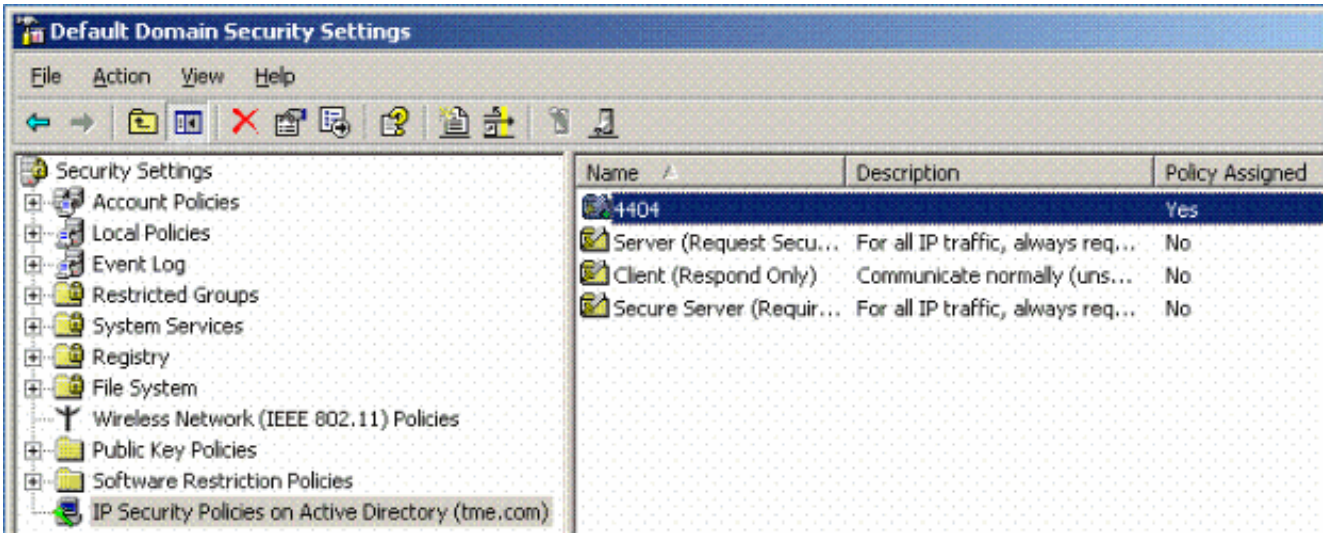
2. Open WLAN-netwerkbeleidseigenschappen en klik op **Voorkeursnetwerken**. Voeg een nieuw geprefereerd WLAN toe en typ de naam van uw WLAN-SSID, zoals `Wireless`. Dubbelklik op dat nieuwe voorkeursnetwerk en klik op het tabblad **IEEE 802.1x**. PEAP als EAP-type kiezen:



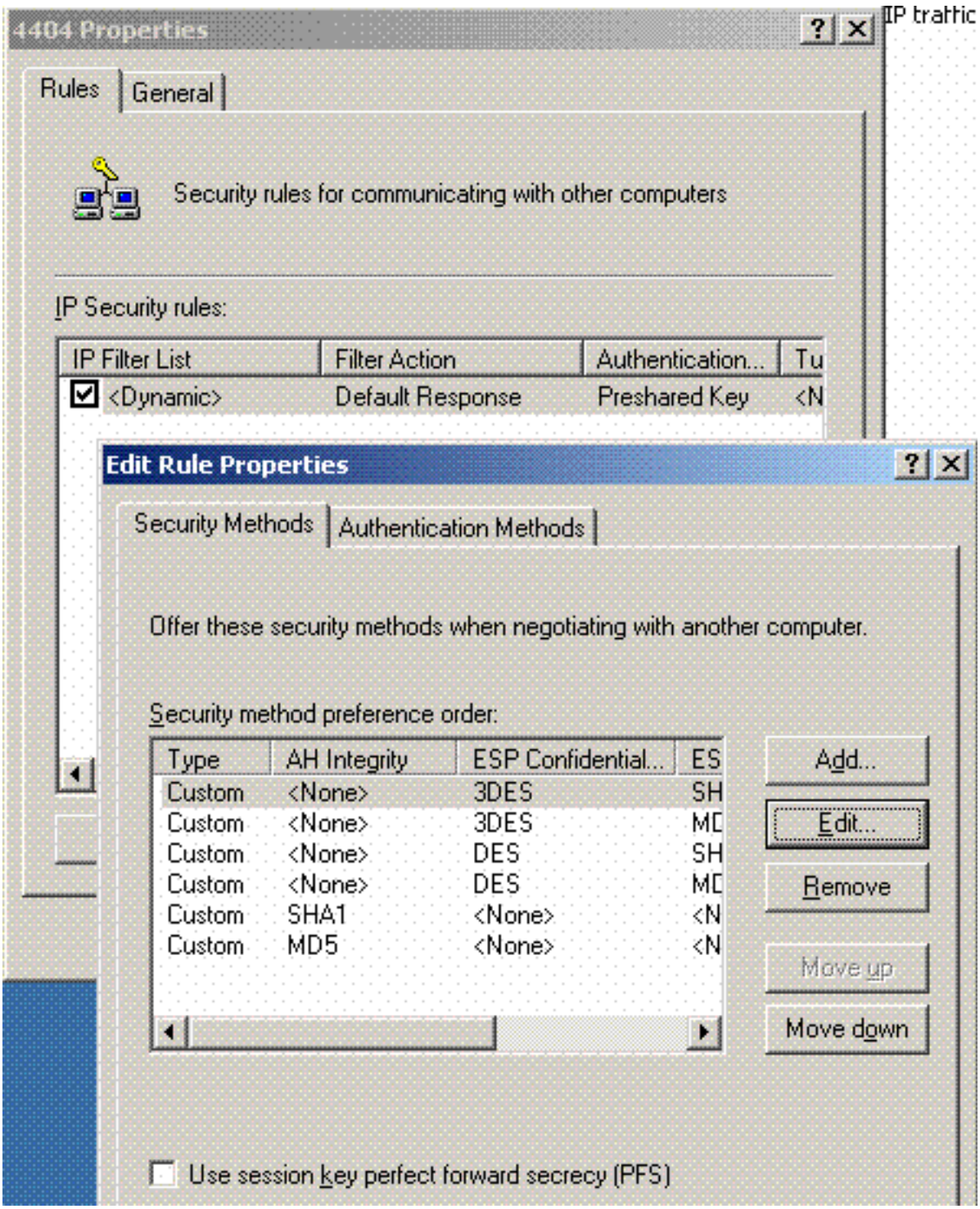
3. Klik op **PEAP-instellingen**, controleer het **servercertificaat valideren** en selecteer de Trusted Root Cert die is geïnstalleerd in de certificeringsinstantie. Voor testdoeleinden vinkt u het vakje MS CHAP v2 uit om automatisch mijn Windows-login en -wachtwoord te gebruiken.



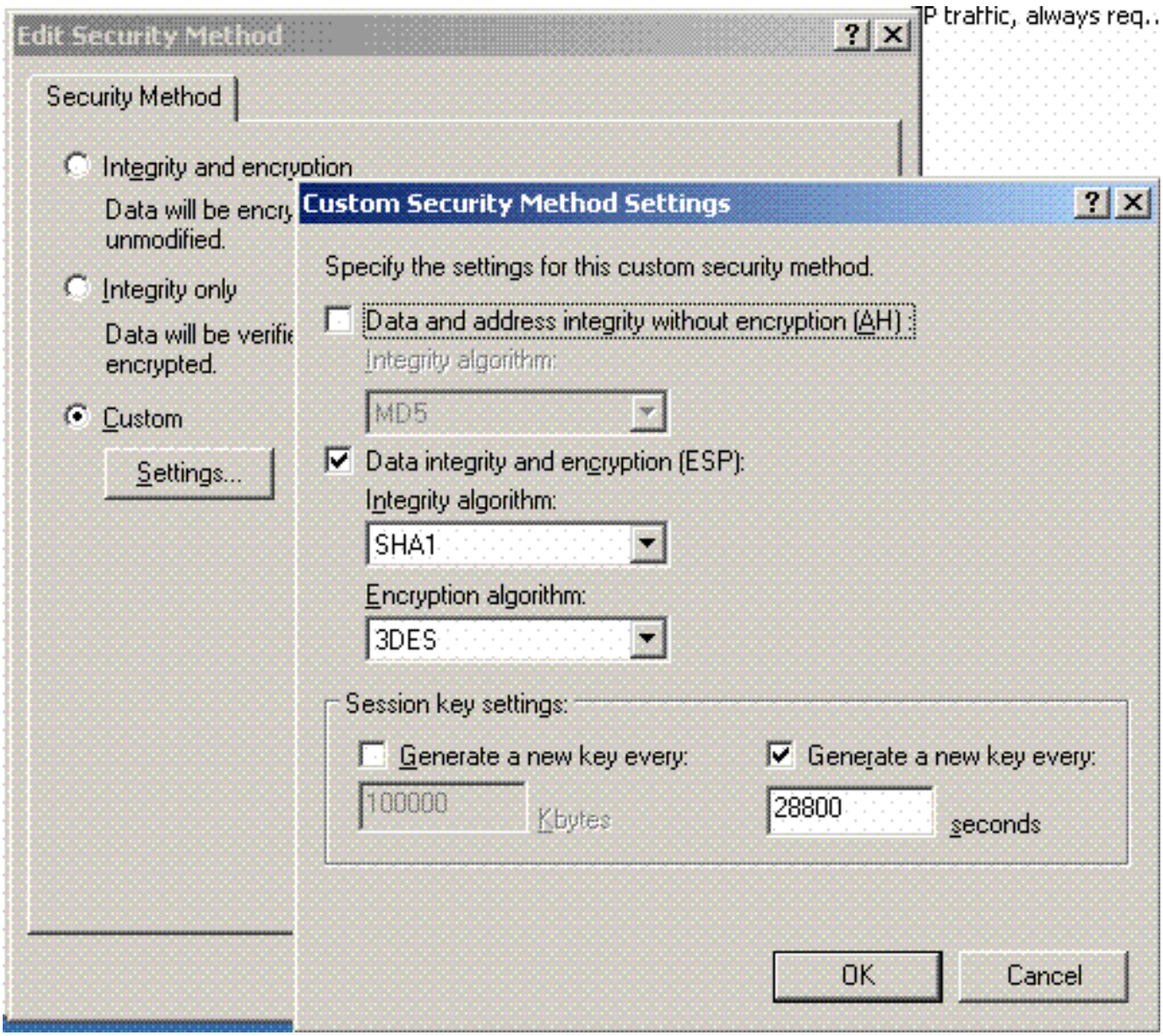
4. Maak in het venster van Windows 2003 Default Domain Security Settings een nieuw IP-beveiligingsbeleid voor het Active Directory-beleid, zoals **4404**.



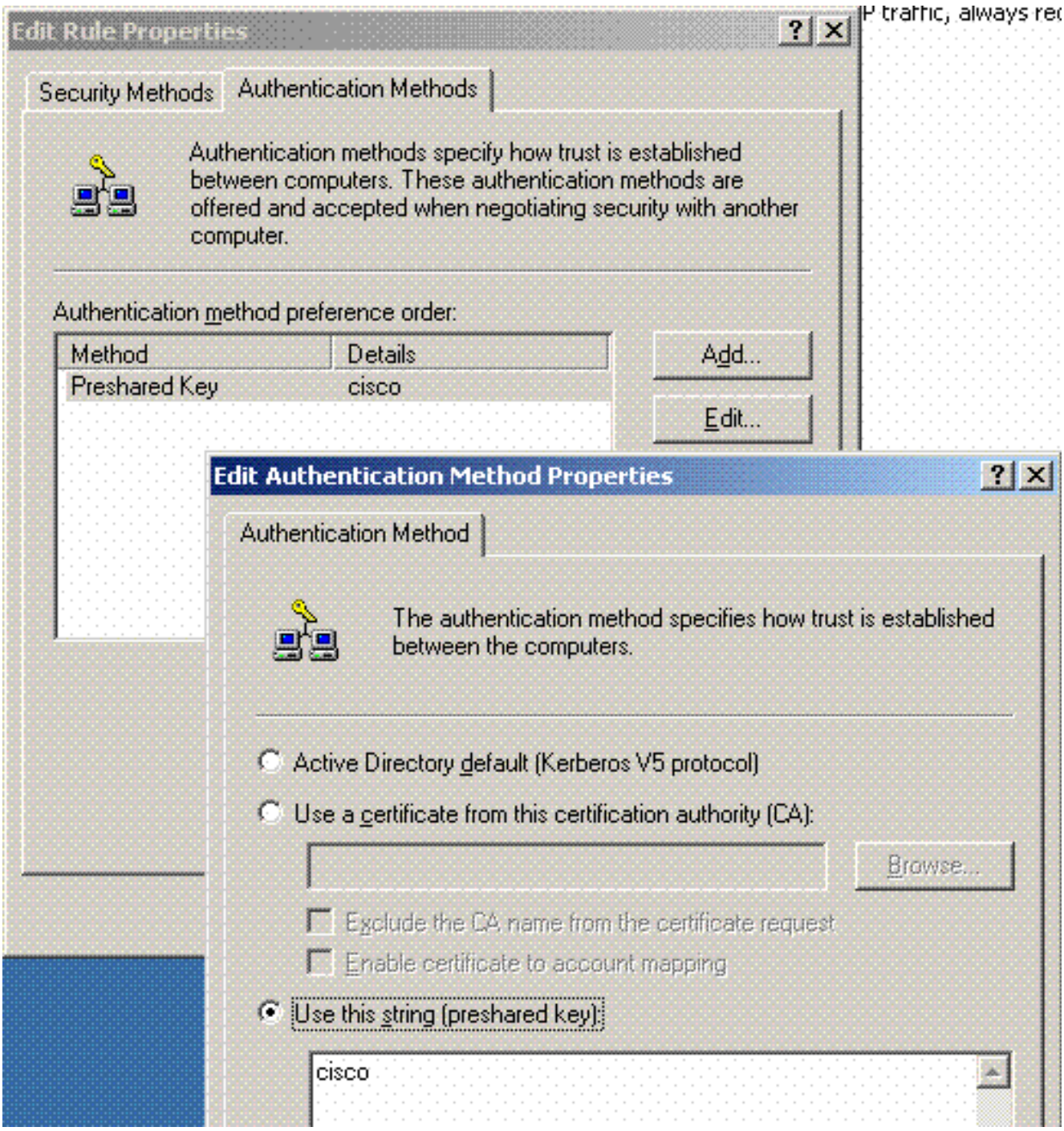
5. Bewerk de nieuwe 4404 beleidseigenschappen en klik op het tabblad **Regels**. Voeg een nieuwe filterregel toe - IP Filet List (Dynamisch); Filter Actie (Default Response); Verificatie (PSK); Tunnel (Geen). Dubbelklik op de nieuwe filterregel en selecteer Beveiligingsmethoden:



6. Klik op **Security Method bewerken** en klik op de knop **Aangepaste** instellingen. Kies deze instellingen.**Opmerking:** deze instellingen moeten overeenkomen met de beveiligingsinstellingen van de controllerRADIUS
IPSec.



7. Klik op het tabblad **Verificatiemethode** onder de Eigenschappen regel bewerken. Voer hetzelfde gedeelde geheim in dat u eerder hebt ingevoerd in de controller-RADIUS-configuratie.



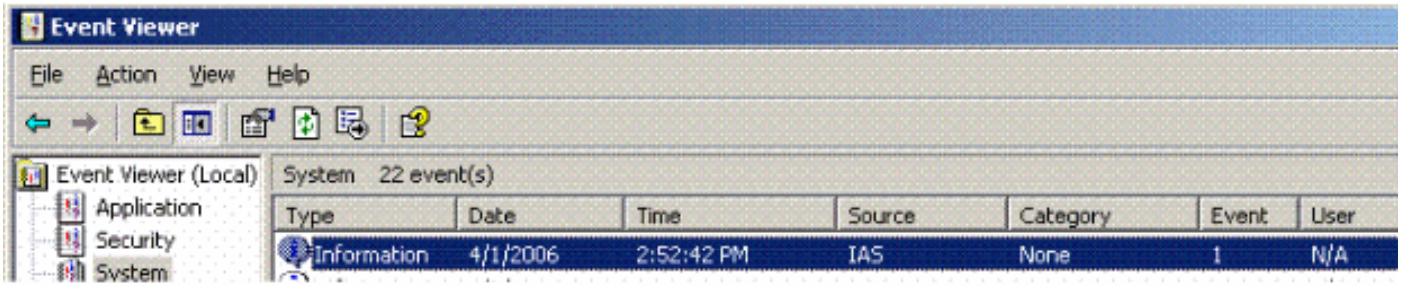
Op dit punt zijn alle configuraties voor de Controller, IAS en Domain Security Settings voltooid. Sla alle configuraties op zowel de controller als WinServer op en herstart alle machines. Installeer op de WLAN-client die voor de test wordt gebruikt de basiskern en configureer deze voor WPA2/PEAP. Nadat de root cert is geïnstalleerd op de client, herstart de client machine. Nadat alle machines opnieuw zijn opgestart, sluit u de client aan op het WLAN en neemt u deze loggebeurtenissen op.

Opmerking: een clientverbinding is vereist om de IPSec-verbinding tussen de controller en WinServer RADIUS in te stellen.

Windows 2003-systeemloggebeurtenissen

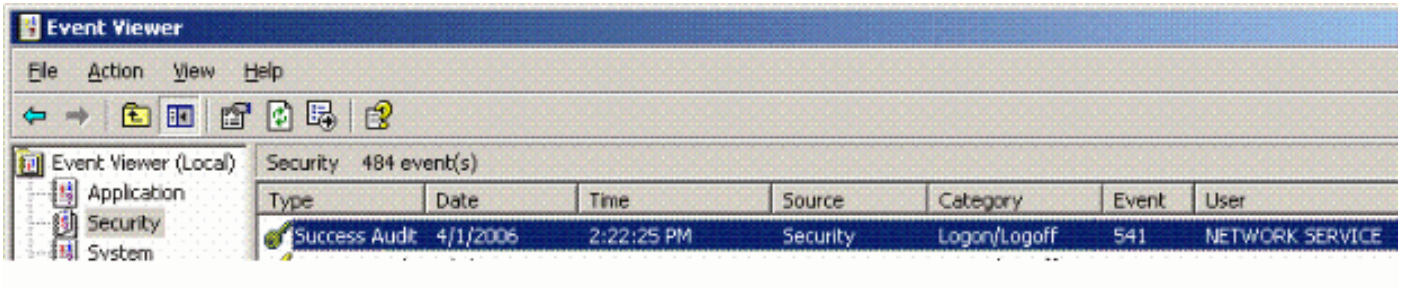
Een succesvolle WLAN-clientverbinding die voor WPA2/PEAP met IPSec RADIUS is geconfigureerd, genereert deze systeemgebeurtenis op de WinServer:

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)
```

Een succesvolle controller <> RADIUS IPSec-verbinding genereert deze security gebeurtenis op de WinServer-logbestanden:




```
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
```

Draadloze LAN-controller voor RADIUS en IPSec-succes bij debugvoorbeeld

U kunt de debug opdracht gebruiken **debug debug pm ikemsg inschakelen** op de controller om deze configuratie te verifiëren. Hierna volgt een voorbeeld.

```
(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
```

Ethreal Capture

Hier is een voorbeeld van Ethreal Capture.

```
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
```

Gerelateerde informatie

- Configuratiehandleiding voor Cisco draadloze LAN-controllers, release 5.2
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.