Konfigurieren von RADIUS IPSec-Sicherheit für WLCs und Microsoft Windows 2003 IAS Server

Inhalt

Einleitung

Dieses Handbuch beschreibt die Konfiguration der von WCS unterstützten RADIUS IPSec-Funktion und der folgenden WLAN-Controller:

- Serie 4400
- WiSM
- 3750 G

Die Funktion RADIUS IPSec für den Controller befindet sich in der grafischen Benutzeroberfläche des Controllers im Abschnitt **Sicherheit > AAA > RADIUS-Authentifizierungsserver**. Mit dieser Funktion können Sie die gesamte RADIUS-Kommunikation zwischen Controllern und RADIUS-Servern (IAS) mit IPSec verschlüsseln.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Kenntnisse zu LWAPP
- Kenntnisse über RADIUS-Authentifizierung und IPSec
- Kenntnisse zum Konfigurieren von Diensten unter dem Betriebssystem Windows 2003 Server

Verwendete Komponenten

Diese Netzwerk- und Softwarekomponenten müssen installiert und konfiguriert werden, damit die RADIUS IPSec-Funktion des Controllers bereitgestellt werden kann:

- Controller WLC 4400, WiSM oder 3750G In diesem Beispiel wird der WLC 4400 mit der Softwareversion 5.2.178.0 verwendet.
- Lightweight Access Points (LAP) In diesem Beispiel wird die LAP der Serie 1231 verwendet.
- Switch mit DHCP
- Microsoft 2003 Server, der als Domänencontroller konfiguriert und mit Microsoft Certificate Authority und Microsoft Internet Authentication Service (IAS) installiert ist.
- Microsoft-Domänensicherheit
- Cisco 802.11 a/b/g Wireless Client Adapter mit ADU Version 3.6, konfiguriert mit WPA2/PEAP

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

IPSec-RADIUS-Konfiguration

Diese Konfigurationsanleitung behandelt nicht die Installation oder Konfiguration von Microsoft WinServer, Certificate Authority, Active Directory oder WLAN 802.1x-Client. Diese Komponenten müssen vor der Bereitstellung der Controller-IPSec-RADIUS-Funktion installiert und konfiguriert werden. Im verbleibenden Teil dieses Leitfadens wird die Konfiguration von IPSec RADIUS für die folgenden Komponenten beschrieben:

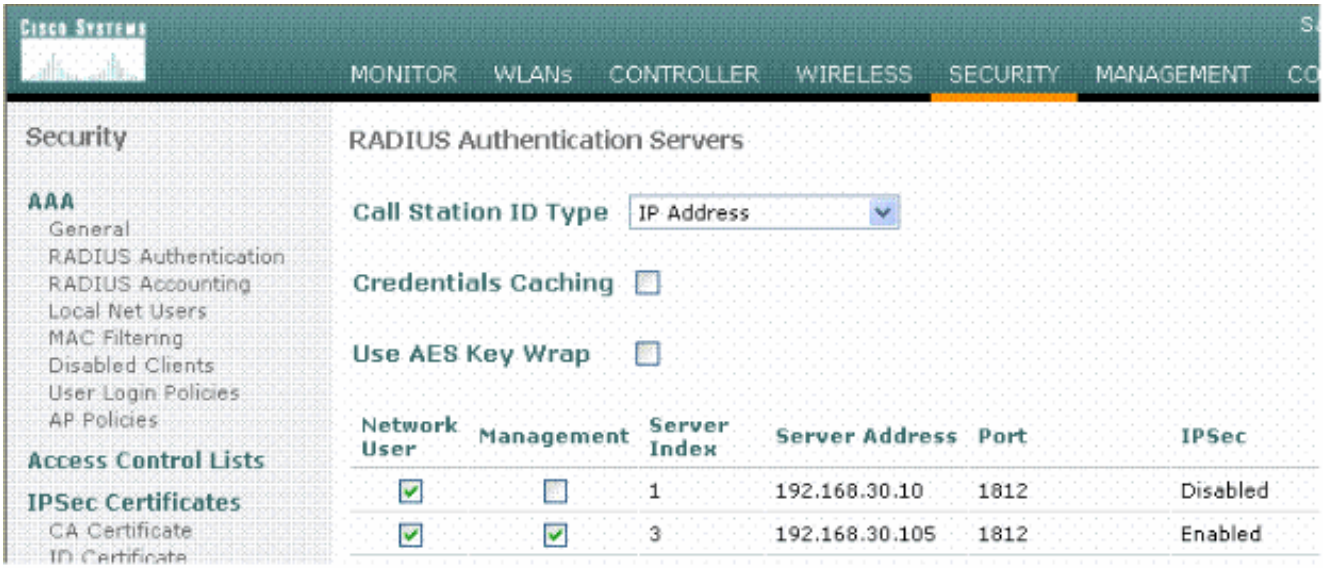
1. Cisco WLAN Controller
2. IAS Windows 2003
3. Microsoft Windows-Domänensicherheitseinstellungen

Konfigurieren des WLC

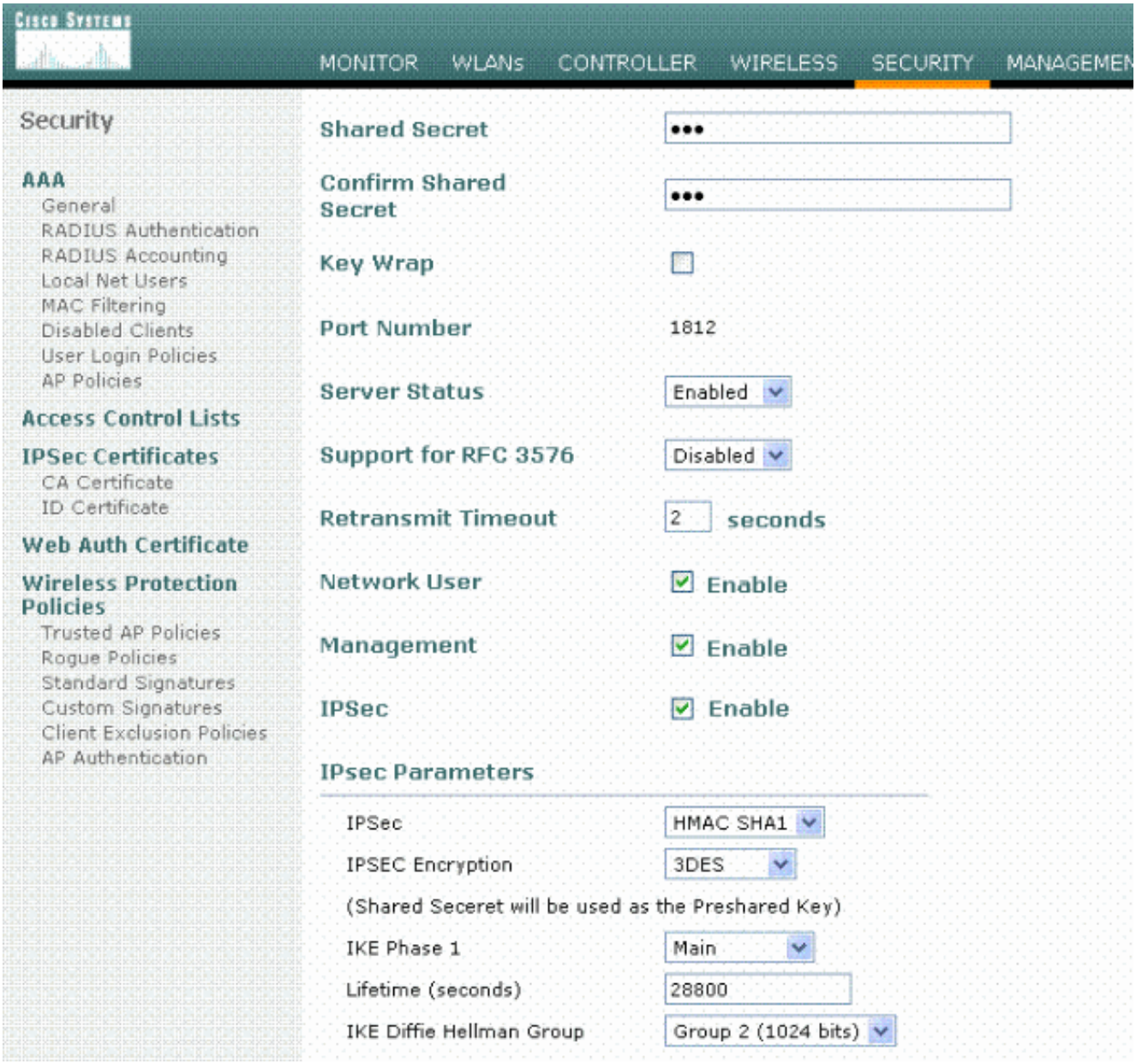
In diesem Abschnitt wird erläutert, wie Sie IPSec auf dem WLC über die Benutzeroberfläche konfigurieren.

Führen Sie in der Controller-GUI die folgenden Schritte aus.

1. Navigieren Sie zur Registerkarte **Security > AAA > RADIUS Authentication** (Sicherheit > AAA > RADIUS-Authentifizierung) in der Controller-GUI, und fügen Sie einen neuen RADIUS-Server
   hinzu.



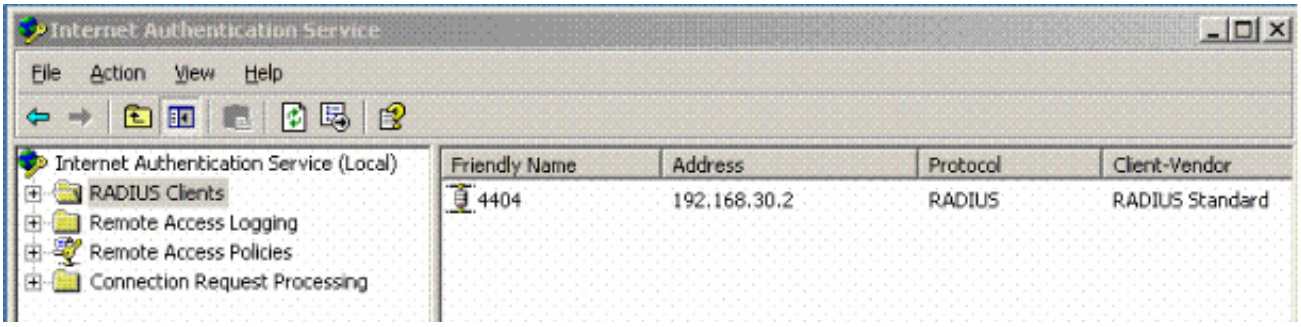
2. Konfigurieren Sie die IP-Adresse, Port 1812 und einen gemeinsamen geheimen Schlüssel des neuen RADIUS-Servers. Aktivieren Sie das Kontrollkästchen **IPSec-Aktivierung**, konfigurieren Sie diese IPSec-Parameter, und klicken Sie dann auf **Anwenden**.**Hinweis:** Der gemeinsame geheime Schlüssel wird sowohl zur Authentifizierung des RADIUS-Servers als auch als PSK für die IPSec-Authentifizierung
verwendet.



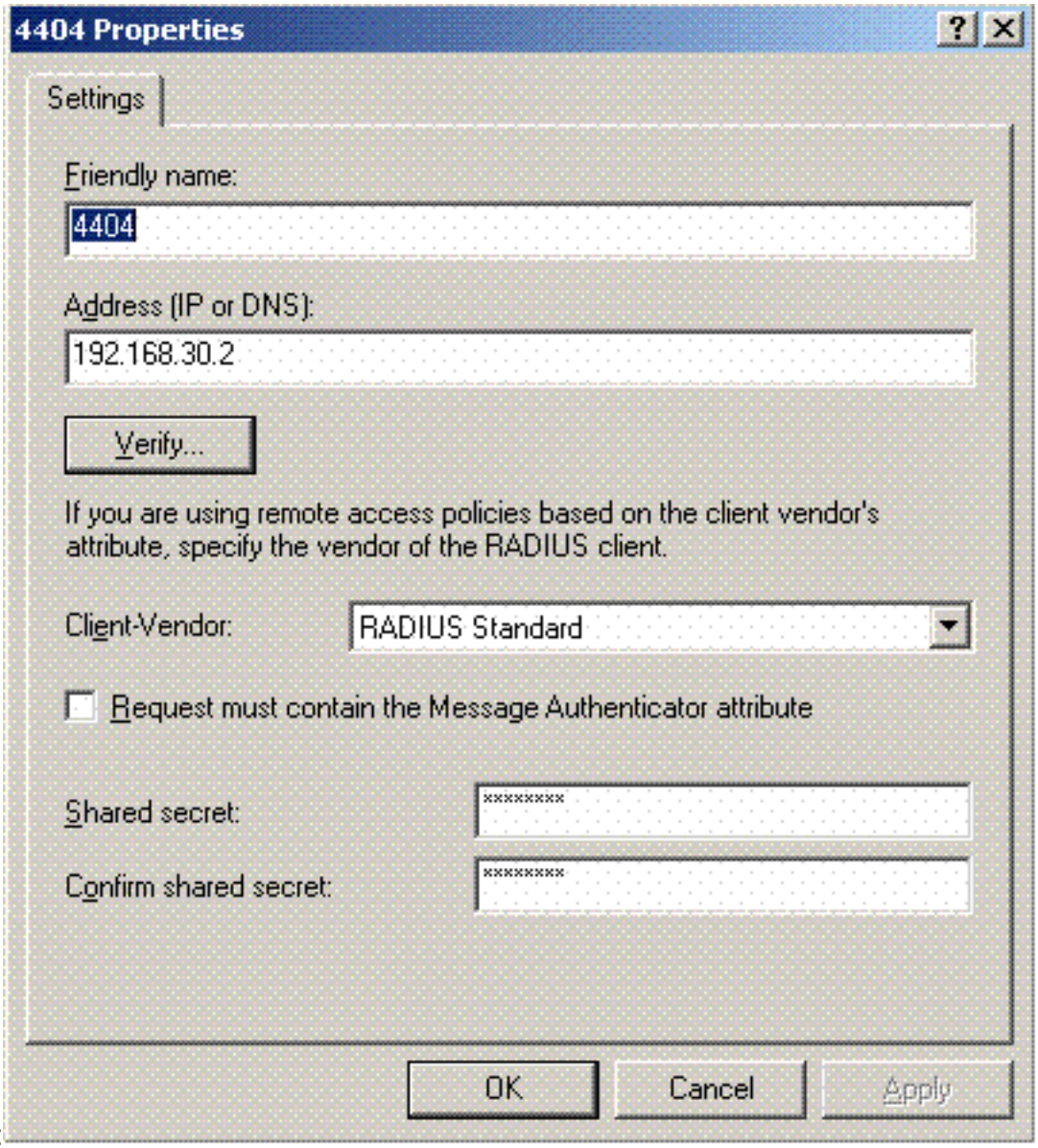
Konfigurieren des IAS

Gehen Sie wie folgt vor:

1. Navigieren Sie zum IAS-Manager in Win2003, und fügen Sie einen neuen RADIUS-Client hinzu.

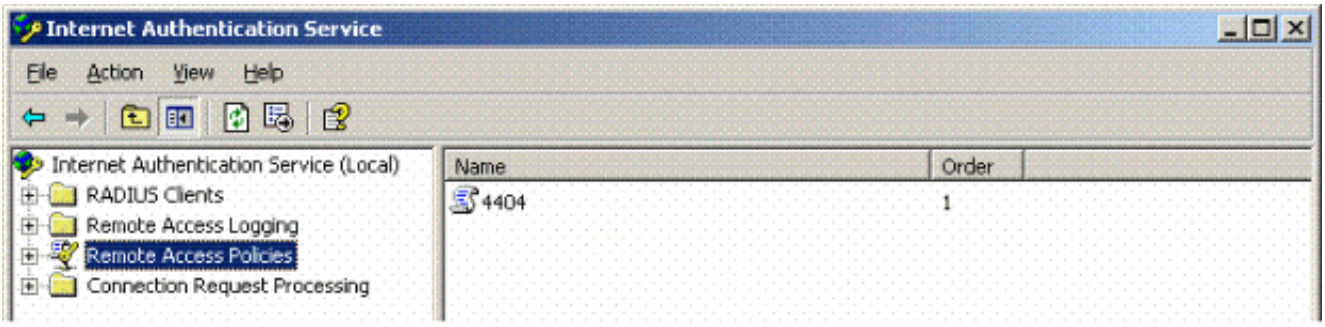


2. Konfigurieren Sie die RADIUS-Clienteigenschaften mit der IP-Adresse und dem auf dem Controller konfigurierten gemeinsamen geheimen

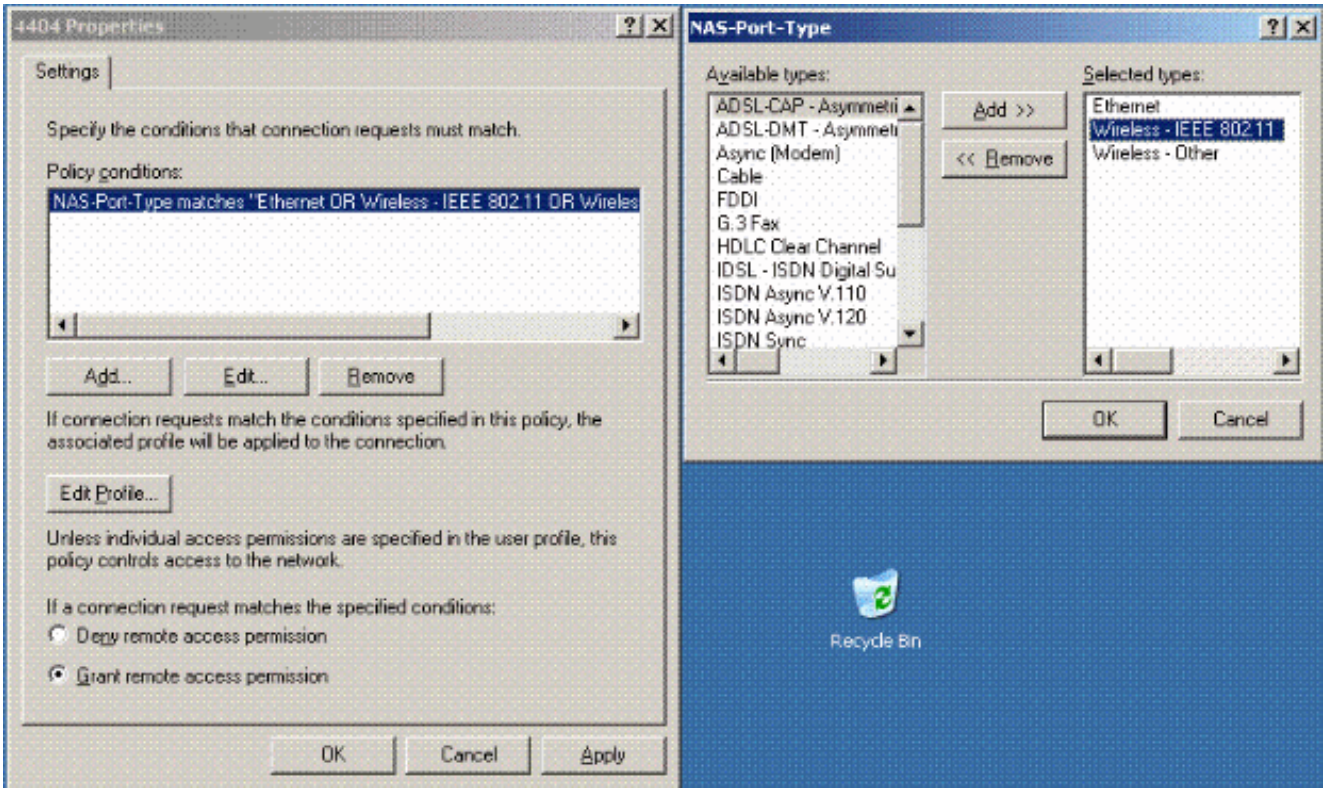


Schlüssel:

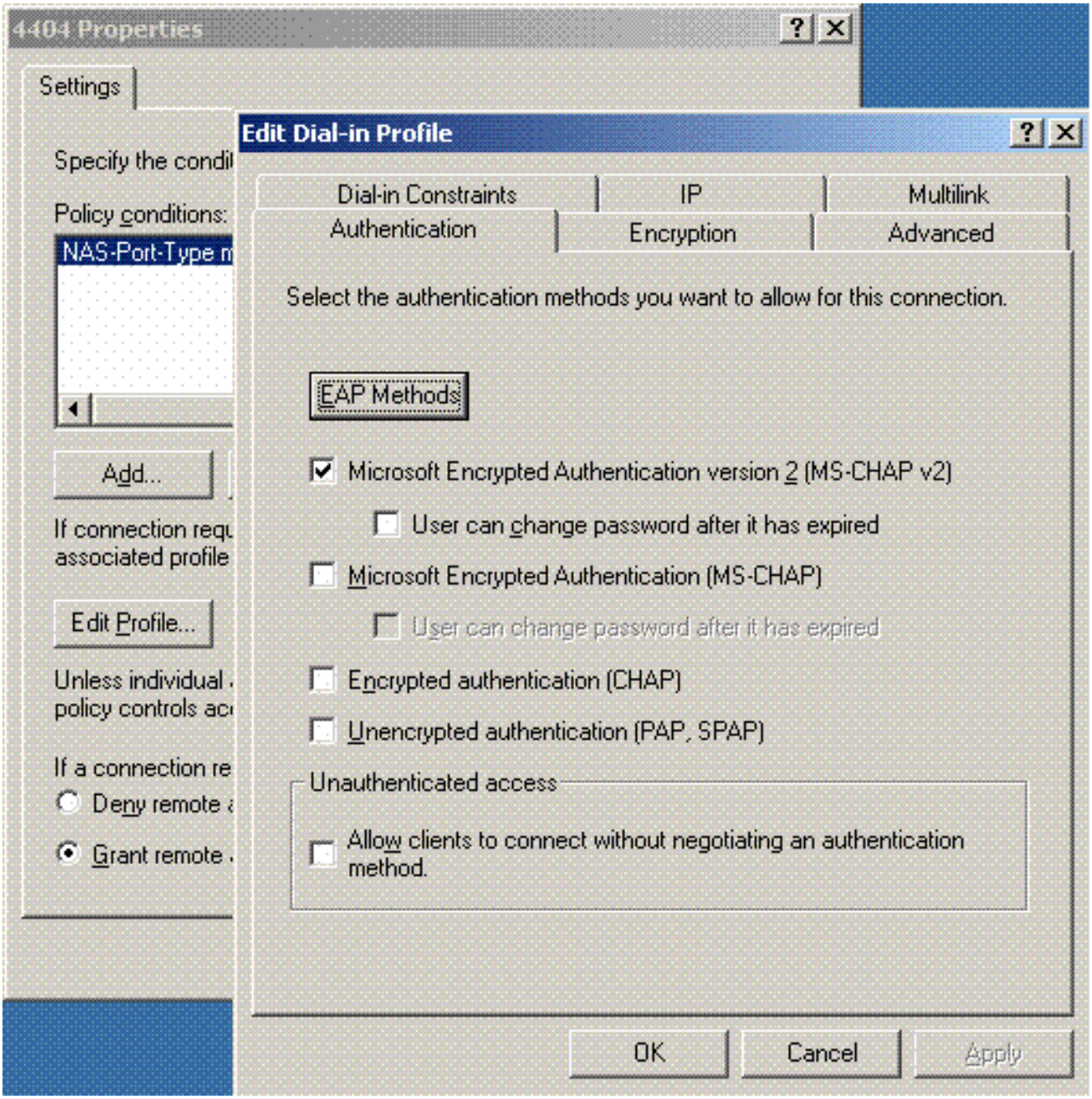
3. Konfigurieren Sie eine neue RAS-Richtlinie für den Controller:



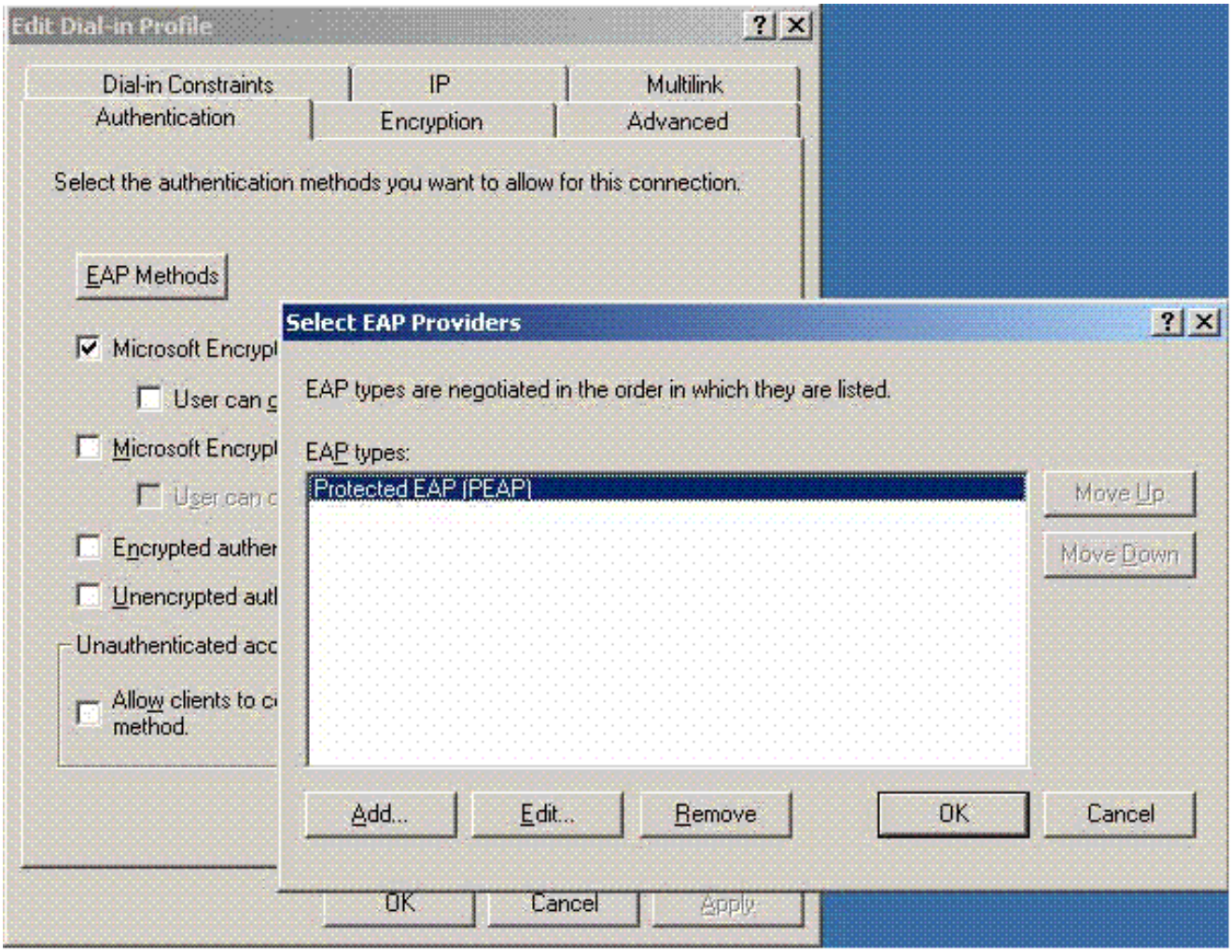
4. Bearbeiten Sie die Eigenschaften der Controller-RAS-Richtlinie. Stellen Sie sicher, dass der NAS-Port-Typ - Wireless - IEEE 802.11 hinzugefügt wird:



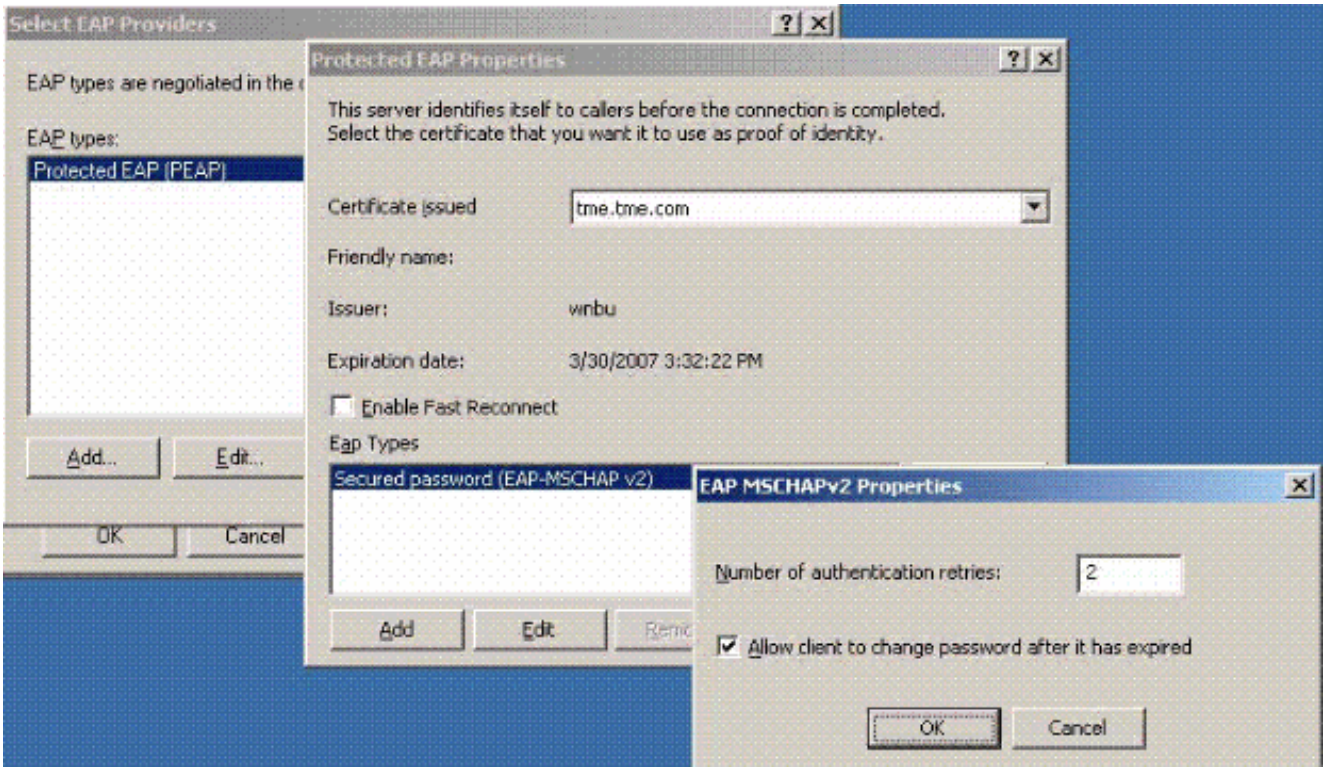
5. Klicken Sie auf **Profil bearbeiten**, klicken Sie auf die Registerkarte **Authentifizierung**, und aktivieren Sie MS-CHAP v2 für Authentifizierung:



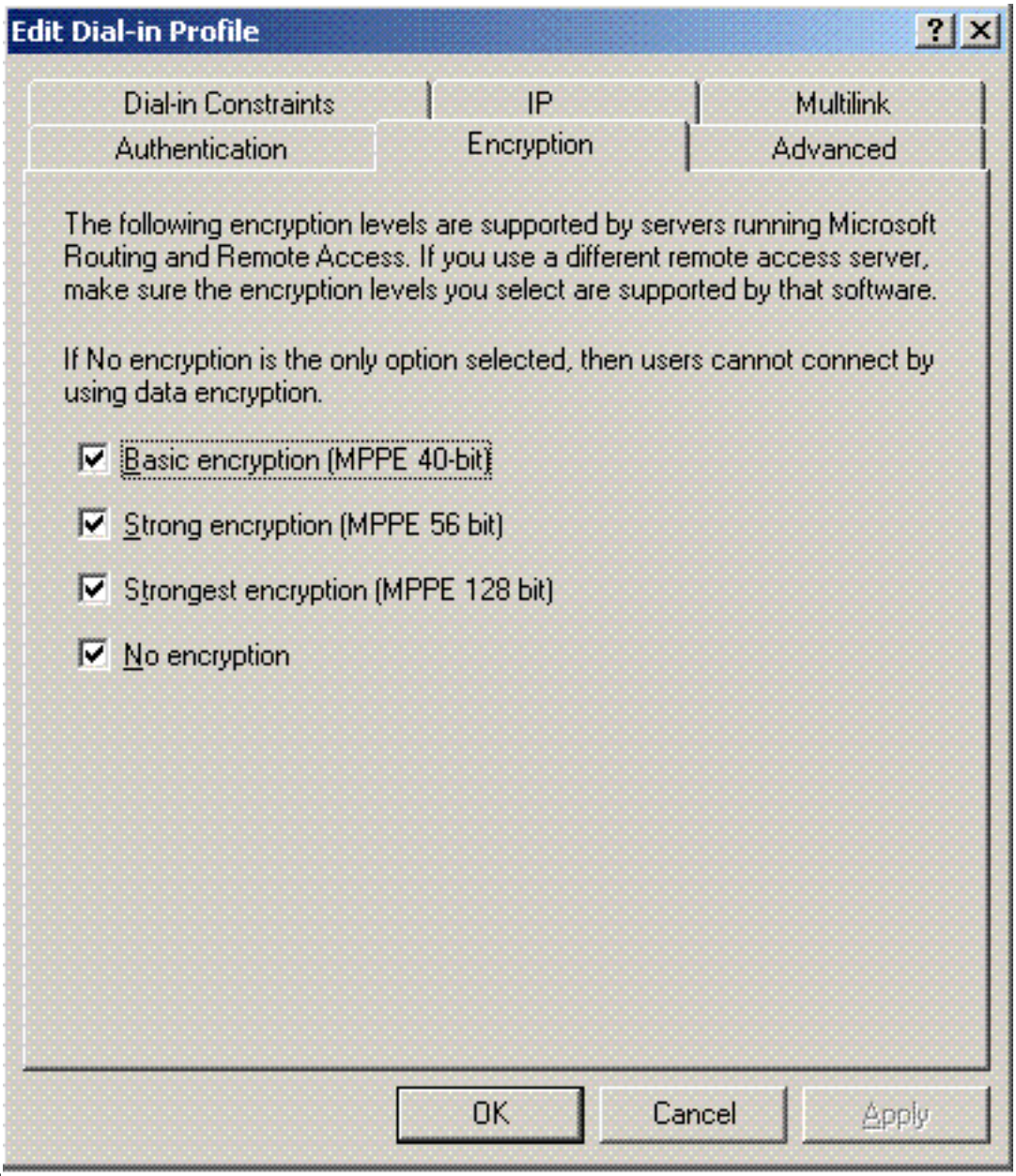
6. Klicken Sie auf **EAP Methods**, wählen Sie EAP Providers aus, und fügen Sie PEAP als EAP-Typ
hinzu:



7. Klicken Sie auf Select EAP Providers (EAP-Anbieter auswählen) und wählen Sie aus dem Dropdown-Menü den Server aus, der Ihren Active Directory-Benutzerkonten und -CA zugeordnet ist (z. B. tme.tme.com). Fügen Sie den EAP-Typ MSCHAP v2 hinzu:

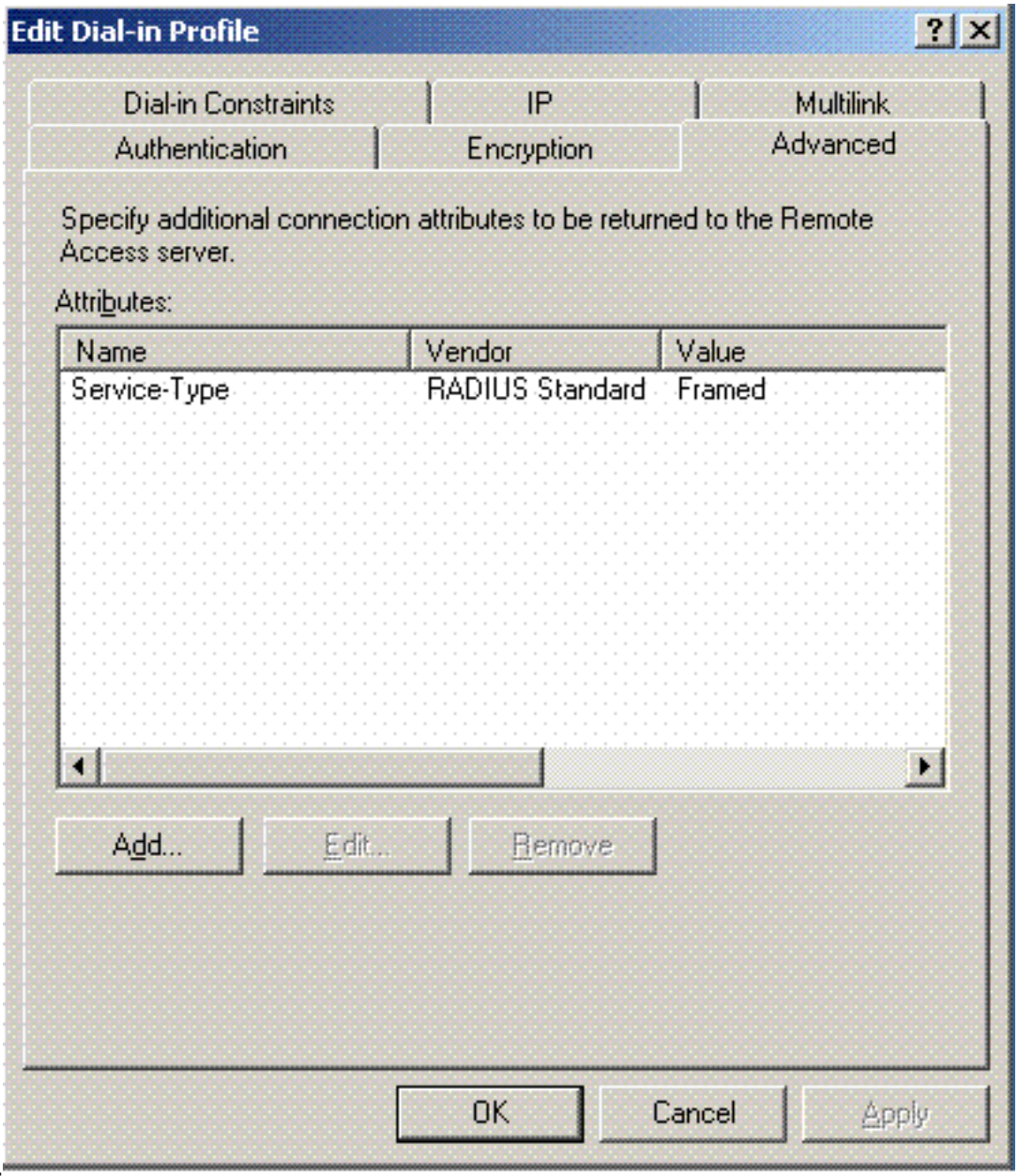


8. Klicken Sie auf die Registerkarte **Verschlüsselung**, und überprüfen Sie alle Verschlüsselungstypen für den



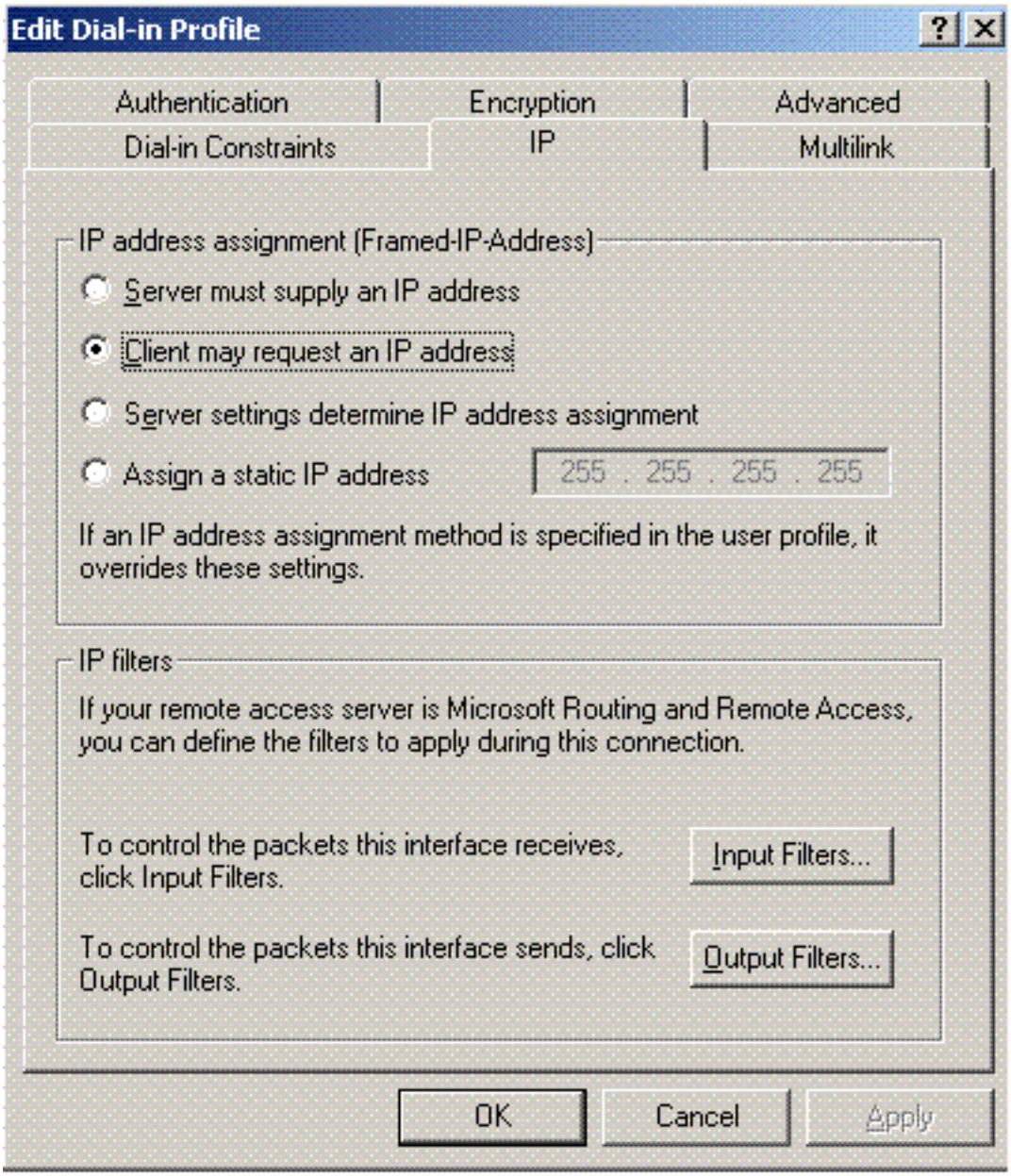
Remotezugriff:

9. Klicken Sie auf die Registerkarte **Advanced** (Erweitert), und fügen Sie RADIUS Standard/Framed als Servicetyp



hinzu:

10. Klicken Sie auf die Registerkarte **IP**, und aktivieren Sie das Kontrollkästchen **Client may request an IP address (Client kann eine IP-Adresse anfordern)**. Dies setzt voraus, dass DHCP auf einem Switch oder WinServer aktiviert

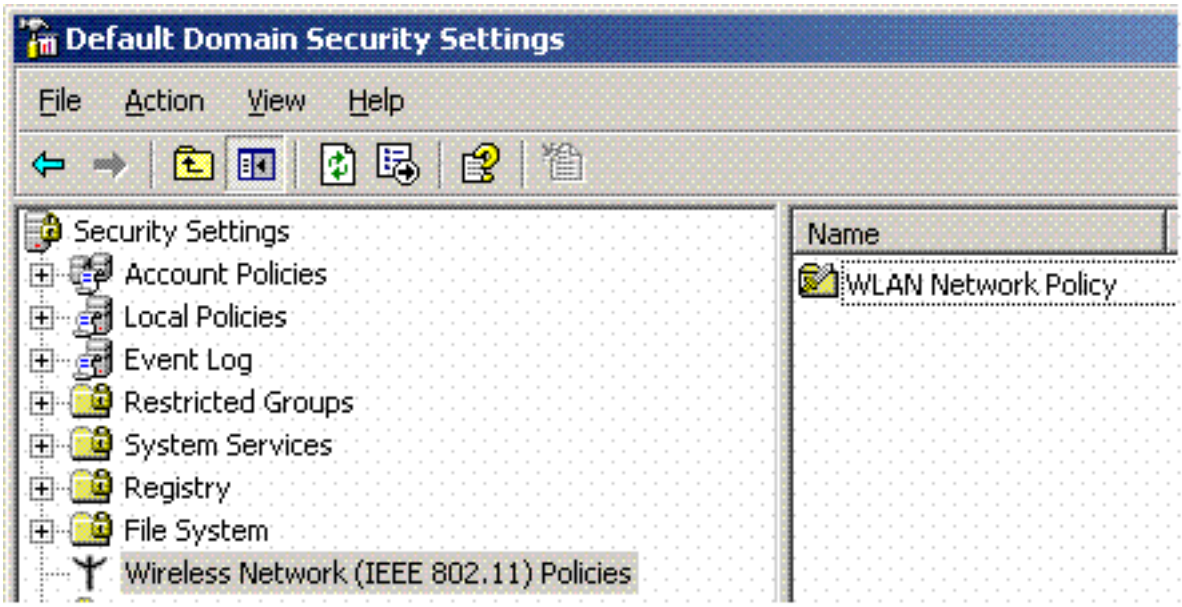


ist.

Microsoft Windows 2003 - Domänensicherheitseinstellungen

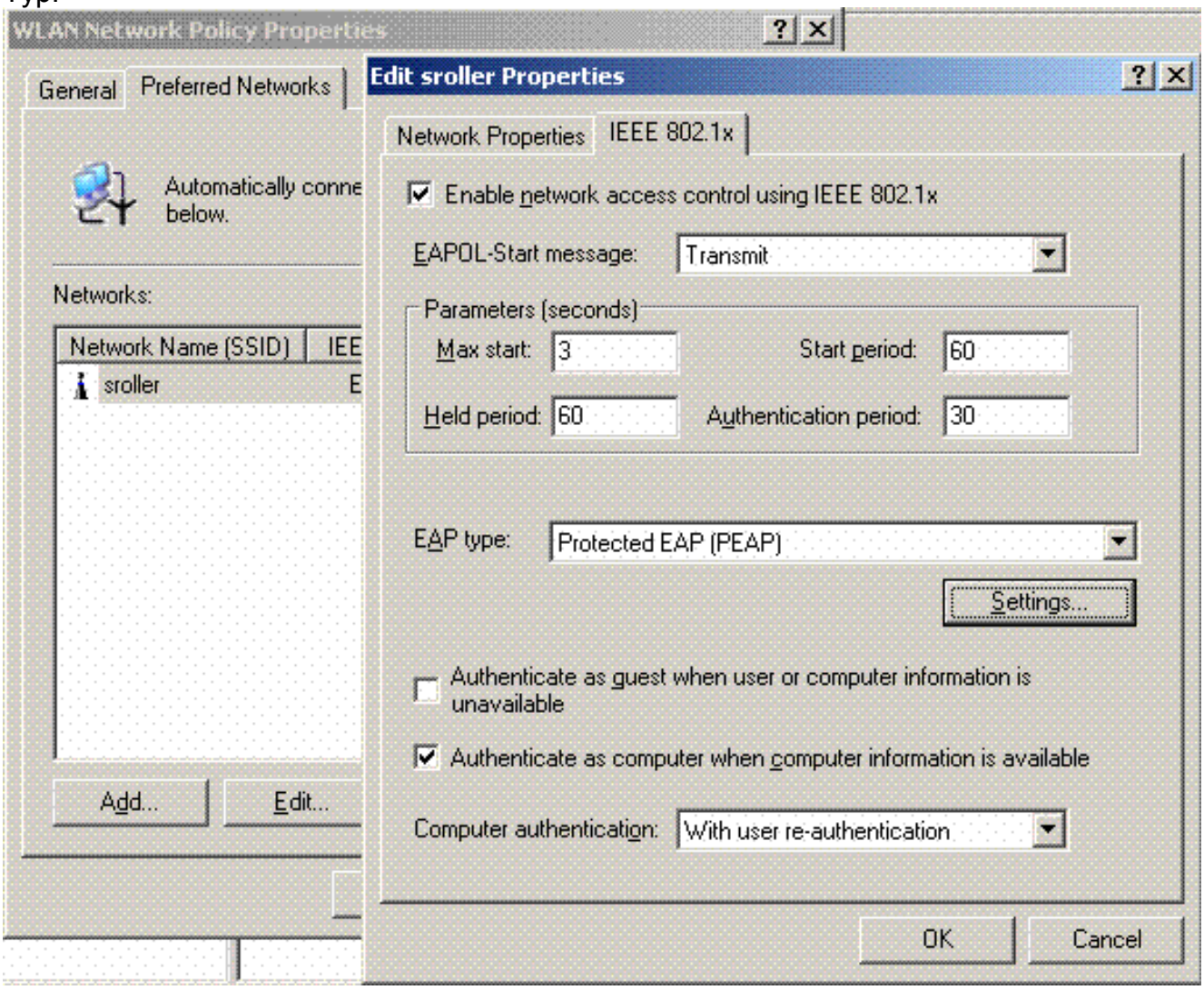
Führen Sie die folgenden Schritte aus, um die Windows 2003-Domänensicherheitseinstellungen zu konfigurieren:

1. Starten Sie den Manager für die Sicherheitseinstellungen der Standarddomäne, und erstellen Sie eine neue Sicherheitsrichtlinie für Richtlinien für Wireless-Netzwerke (IEEE



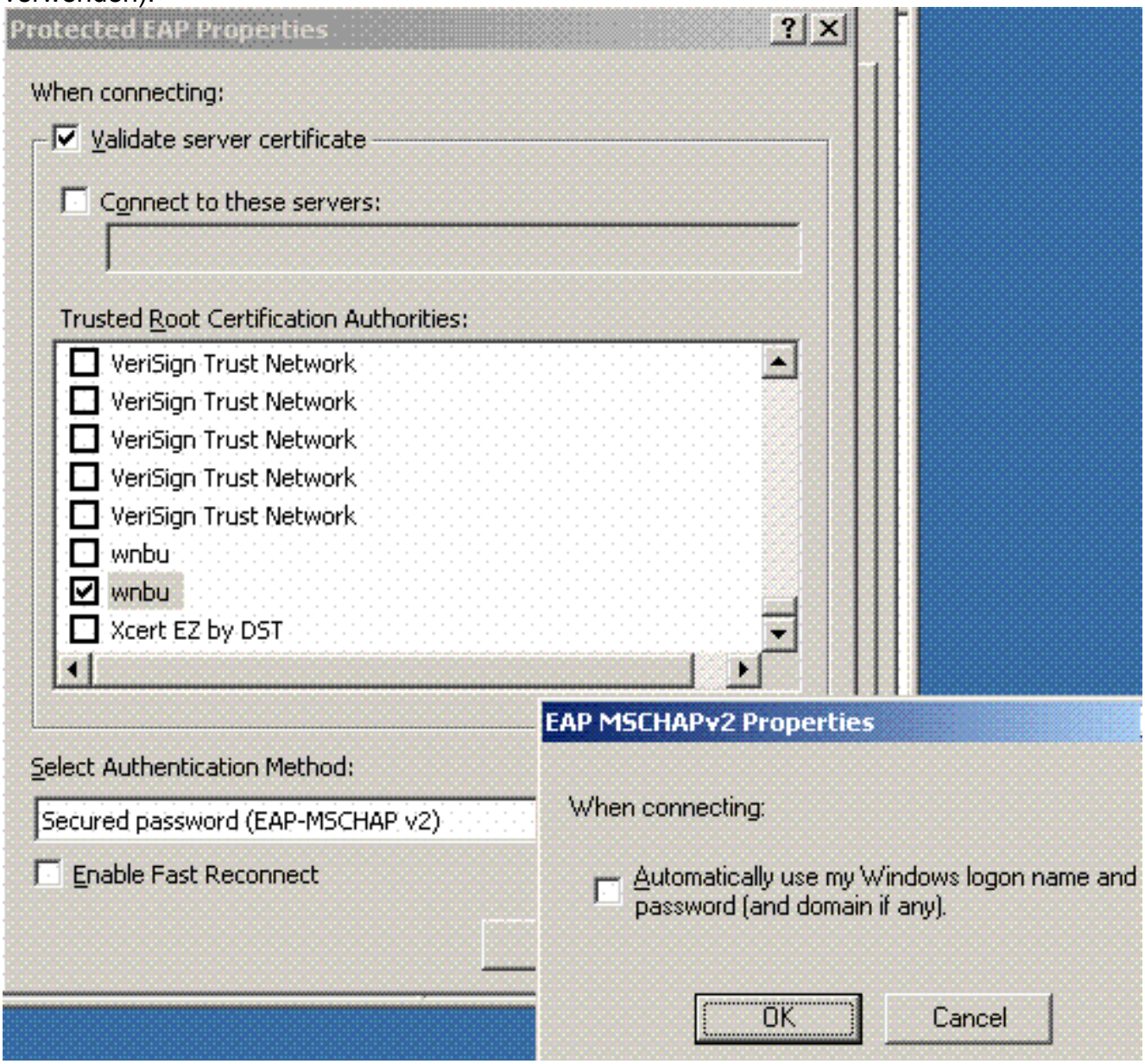
802.11).

2. Öffnen Sie Eigenschaften von WLAN-Netzwerkrichtlinie, und klicken Sie auf **Bevorzugte Netzwerke**. Fügen Sie ein neues bevorzugtes WLAN hinzu, und geben Sie den Namen Ihrer WLAN-SSID ein, z. B. `Wireless`. Doppelklicken Sie auf das neue bevorzugte Netzwerk und anschließend auf die Registerkarte **IEEE 802.1x**. Wählen Sie PEAP als EAP-Typ:

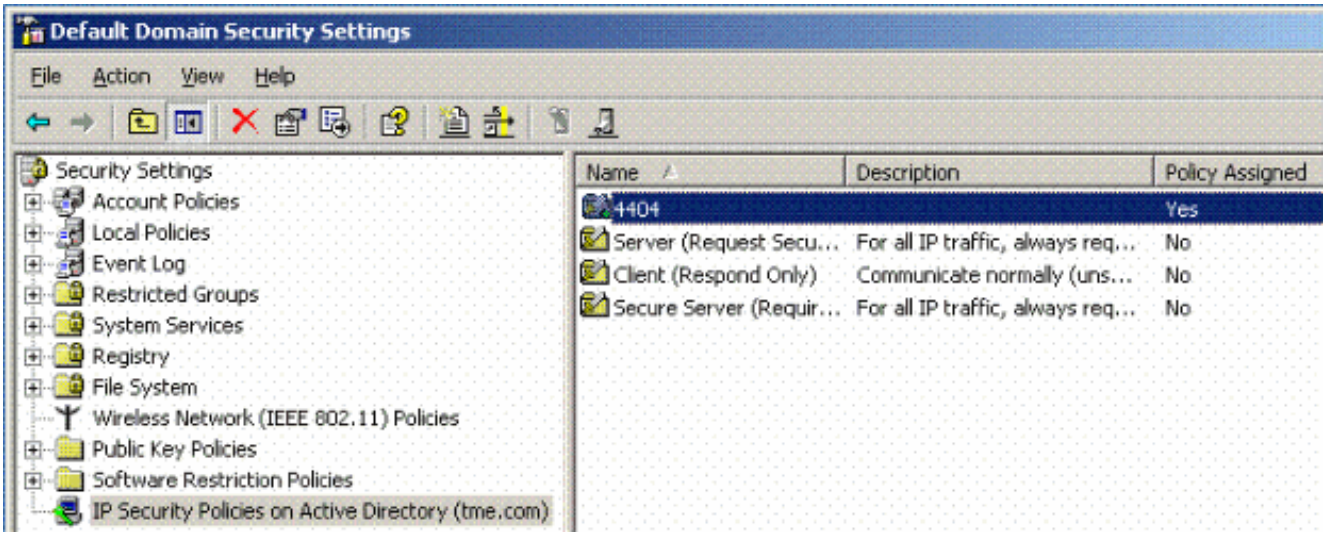


3. Klicken Sie auf **PEAP Settings**, aktivieren Sie **Validate server certificate (Serverzertifikat validieren)**, und wählen Sie das auf Certificate Authority installierte vertrauenswürdige Stammzertifikat aus. Deaktivieren Sie zu Testzwecken das Feld MS CHAP v2 für

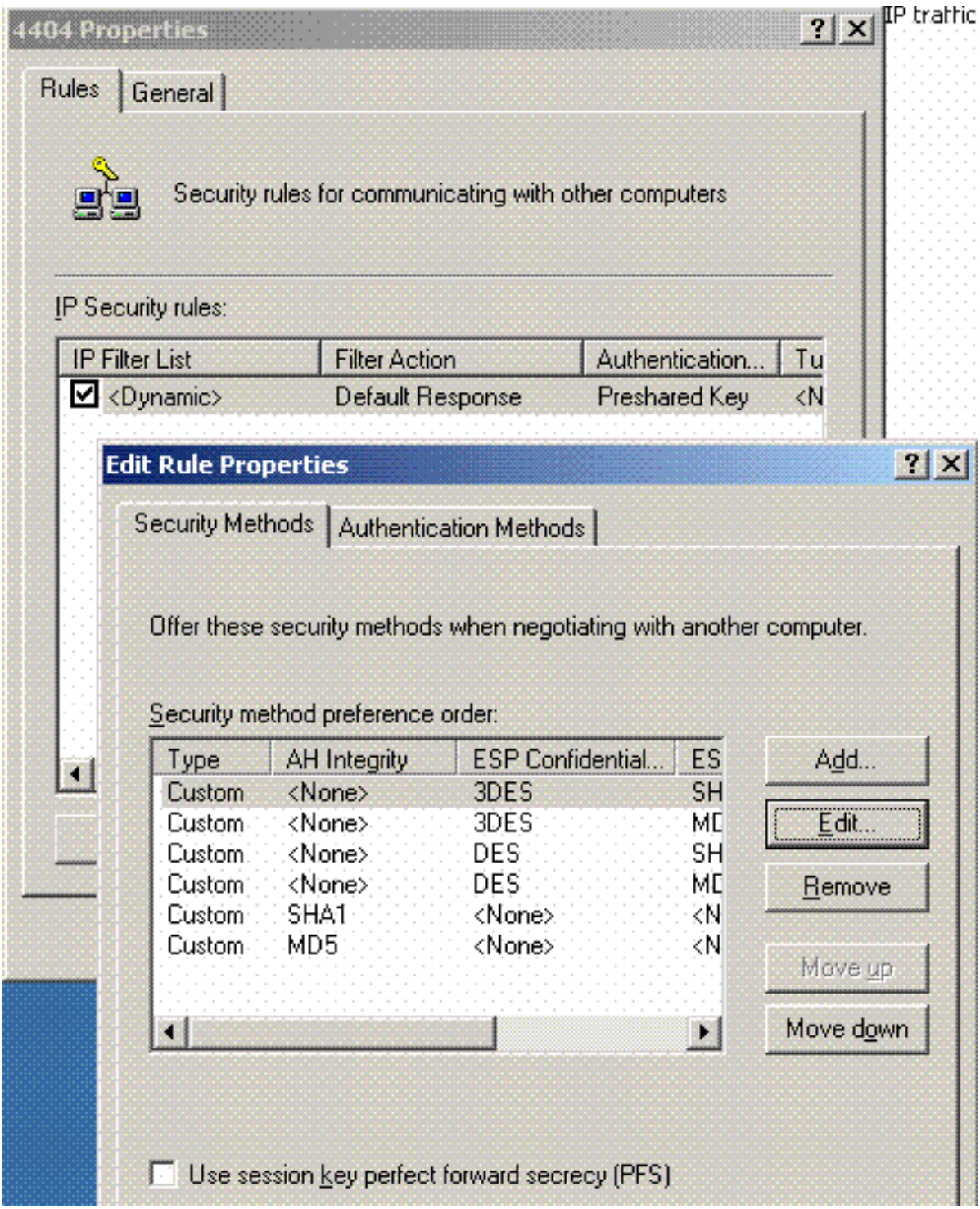
Automatically use my Windows login and password (Automatisch meinen Windows-Benutzernamen und mein Windows-Kennwort
verwenden).



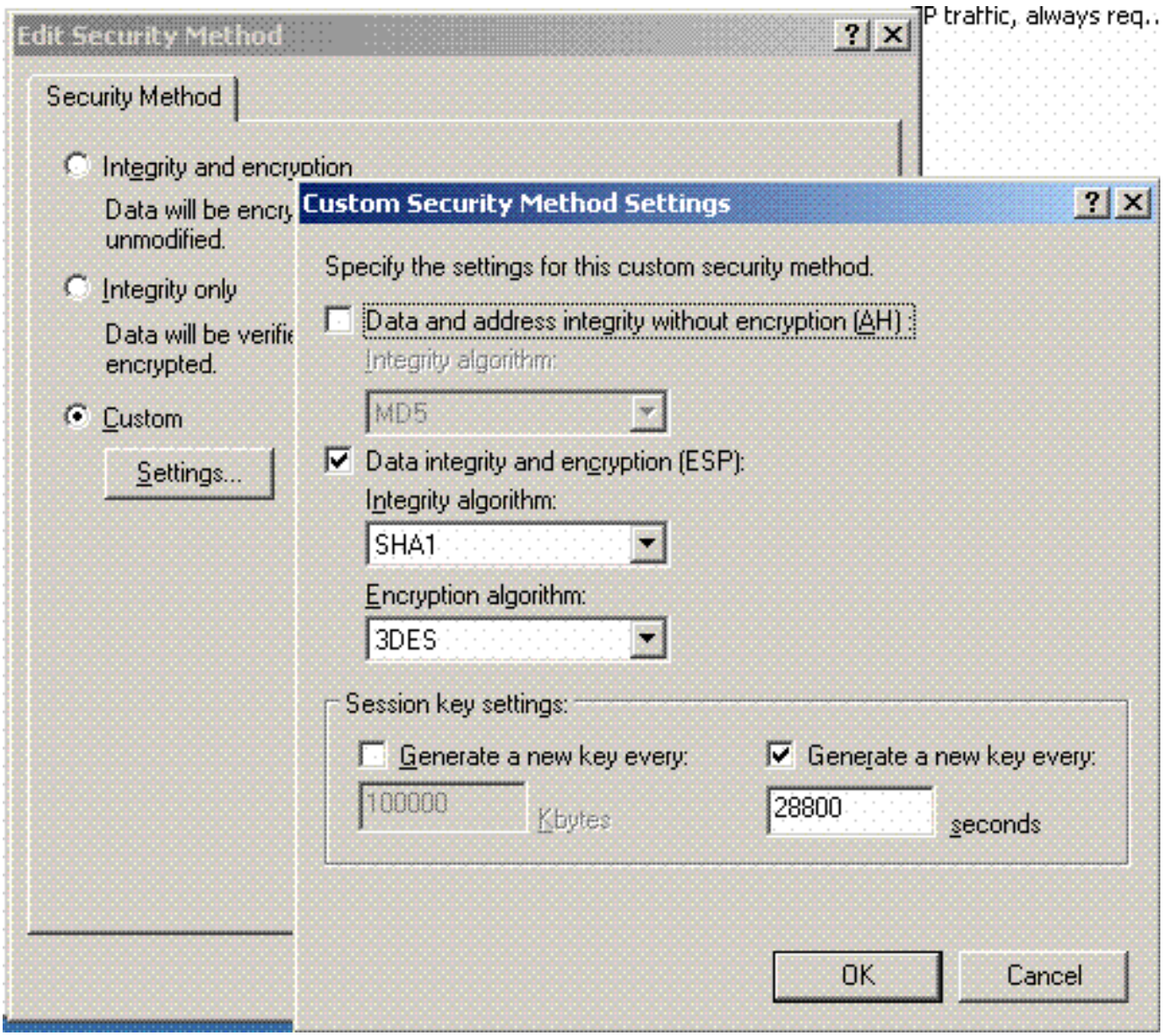
4. Erstellen Sie im Fenster Windows 2003 Default Domain Security Settings Manager (Manager für Standarddomänensicherheitseinstellungen) eine neue IP-Sicherheitsrichtlinie für die Active Directory-Richtlinie, z. B.
4404.



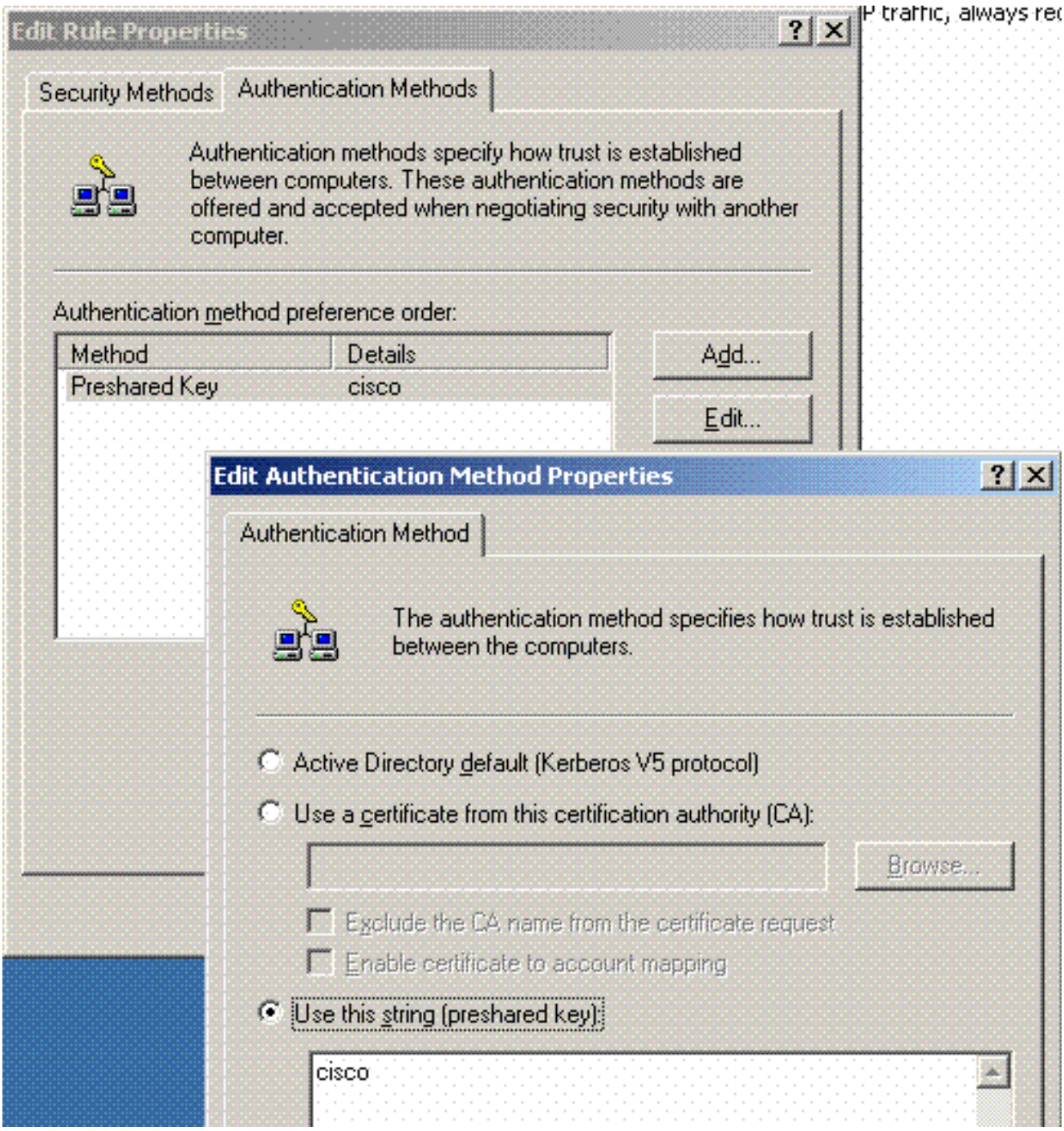
5. Bearbeiten Sie die neuen Eigenschaften der 4404-Richtlinie, und klicken Sie auf die Registerkarte **Regeln**. Fügen Sie eine neue Filterregel hinzu: IP-Verrundungsliste (dynamisch), Filteraktion (Standardantwort), Authentifizierung (PSK) und Tunnel (keine). Doppelklicken Sie auf die neu erstellte Filterregel, und wählen Sie Sicherheitsmethoden:



6. Klicken Sie auf **Sicherheitsmethode bearbeiten** und dann auf das Optionsfeld **Benutzerdefinierte** Einstellungen. Wählen Sie diese Einstellungen aus.**Hinweis:** Diese Einstellungen müssen den RADIUS IPSec-Sicherheitseinstellungen des Controllers entsprechen.



7. Klicken Sie unter "Regeleigenschaften bearbeiten" auf die Registerkarte **Authentifizierungsmethode**. Geben Sie den gleichen gemeinsamen geheimen Schlüssel ein, den Sie zuvor für die Controller-RADIUS-Konfiguration eingegeben haben.



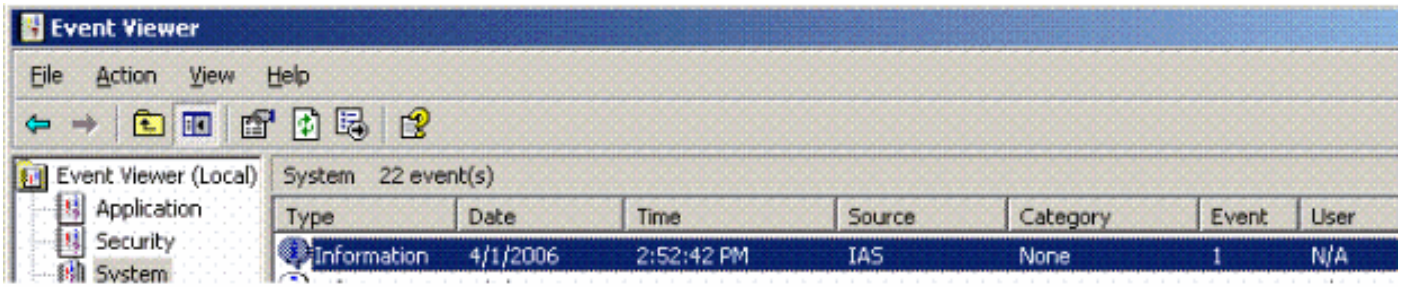
Zu diesem Zeitpunkt sind alle Konfigurationen für den Controller, die IAS und die Domänensicherheitseinstellungen abgeschlossen. Speichern Sie alle Konfigurationen auf dem Controller und auf WinServer, und starten Sie alle Computer neu. Installieren Sie auf dem WLAN-Client, der zum Testen verwendet wird, das Root-Zertifikat, und konfigurieren Sie es für WPA2/PEAP. Nachdem das Root-Zertifikat auf dem Client installiert wurde, starten Sie den Client-Computer neu. Nachdem alle Computer neu gestartet wurden, verbinden Sie den Client mit dem WLAN, und erfassen Sie diese Protokollereignisse.

Hinweis: Zum Einrichten der IPSec-Verbindung zwischen dem Controller und WinServer RADIUS ist eine Client-Verbindung erforderlich.

Windows 2003-Systemprotokollereignisse

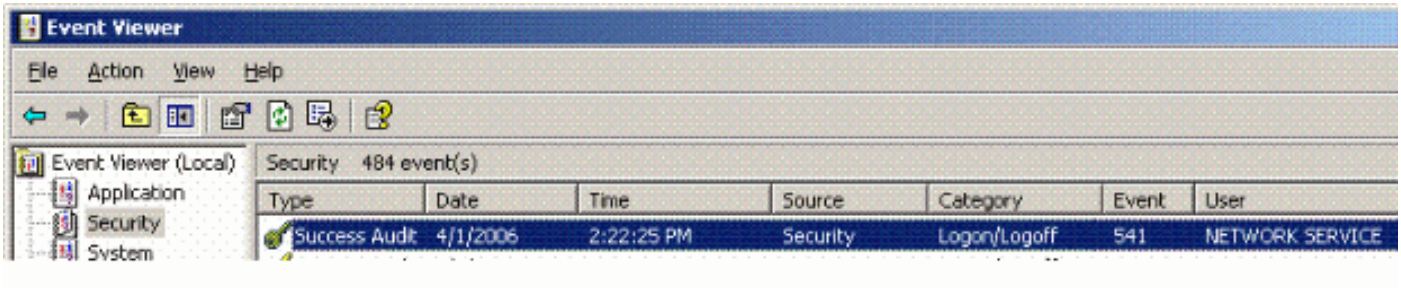
Eine erfolgreiche WLAN-Clientverbindung, die für WPA2/PEAP mit aktiviertem IPSec-RADIUS konfiguriert wurde, generiert dieses Systemereignis auf dem WinServer:

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)
```

Eine erfolgreiche RADIUS IPSec-Verbindung des Controllers <> generiert dieses Sicherheitsereignis in den WinServer-Protokollen:




```
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
```

Wireless LAN Controller RADIUS IPSec Success - Fehlerbeispiel

Sie können den Befehl debug **debug pm ikemsg enable** auf dem Controller verwenden, um diese Konfiguration zu überprüfen. Hier ein Beispiel.

```
(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-Erfassung

Hier ist ein Beispiel für eine Ethreal-Aufnahme.

```
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
```

Zugehörige Informationen

- Cisco Wireless LAN Controller Configuration Guide, Release 5.2
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.