Настройте безопасность IPsec RADIUS для WLC и сервера IAS Microsoft Windows 2003 года

Содержание

Введение

Эти документы руководства, как настроить функцию IPSec RADIUS, поддерживавшую WCS и этими Контроллерами беспроводной локальной сети:

- Серии 4400
- WiSM
- 3750G

Функция IPSec RADIUS Контроллера расположена на Графическом интерфейсе контроллера под **Безопасностью> AAA>** раздел **Серверов проверки подлинности RADIUS**. Функция предоставляет метод для вас для шифрования всей связи RADIUS между Контроллерами и серверами RADIUS (IAS) с IPSec.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Знание о LWAPP
- Знание о проверке подлинности RADIUS и IPSec

- Знание о том, как настроить сервисы на Операционной системе Windows 2003 Server

Используемые компоненты

Они передают, и программные компоненты должны быть установлены и настроены для развертывания функции IPSec RADIUS Контроллера:

- WLC 4400, WiSM, или 3750G Контроллеры. Данный пример использует WLC 4400, который работает под управлением ПО версии 5.2.178.0
- Облегченные точки доступа (LAP). Данный пример использует LAP серии 1231.
- Коммутатор с DHCP
- Сервер Microsoft 2003, настроенный как Контроллер домена, установленный с Microsoft Certificate Authority и с Microsoft Internet Authentication Service (IAS).
- Безопасность домена Microsoft
- Адаптер беспроводного клиента a/b/g 802.11 Cisco с версией ADU 3.6, настроенной с WPA2 / PEAP

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Конфигурация RADIUS IPSec

Это руководство по конфигурации не обращается к установке или конфигурации Microsoft WinServer, Центра сертификации, Active Directory или клиента 802.1x WLAN. Эти компоненты должны быть установлены и настроены до развертываний функции RADIUS IPSec Контроллера. Остаток от этого руководства документирует, как настроить RADIUS IPSec на этих компонентах:

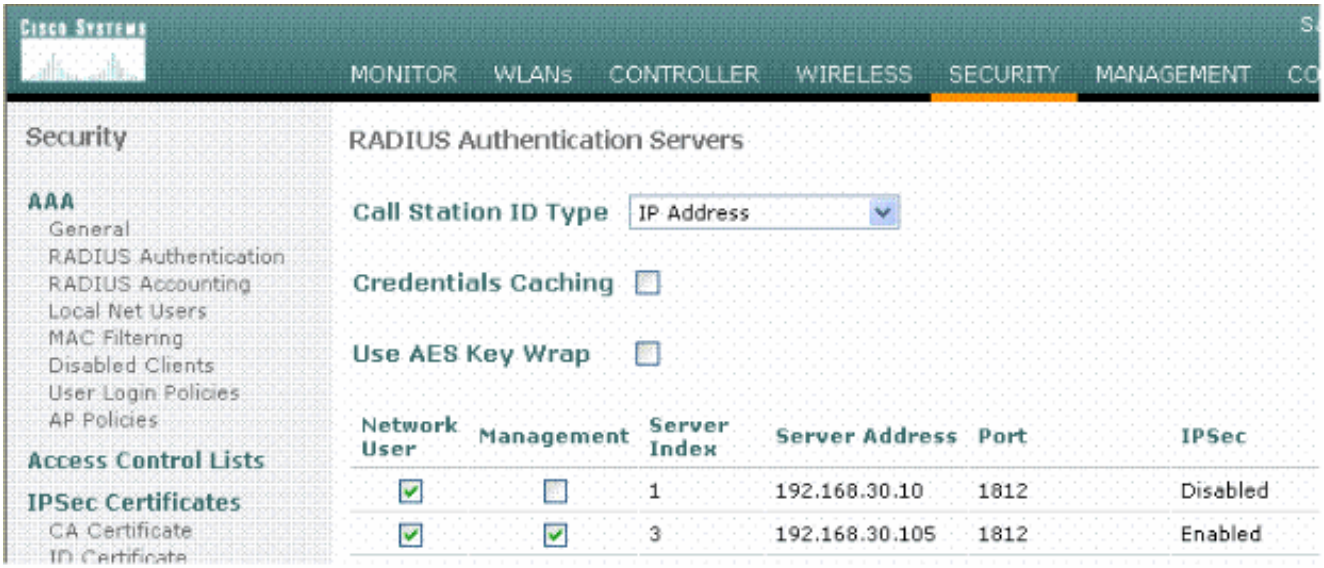
1. Контроллеры беспроводной локальной сети Cisco
2. Windows 2003 IAS
3. Параметры настройки безопасности домена Microsoft Windows

Настройте WLC

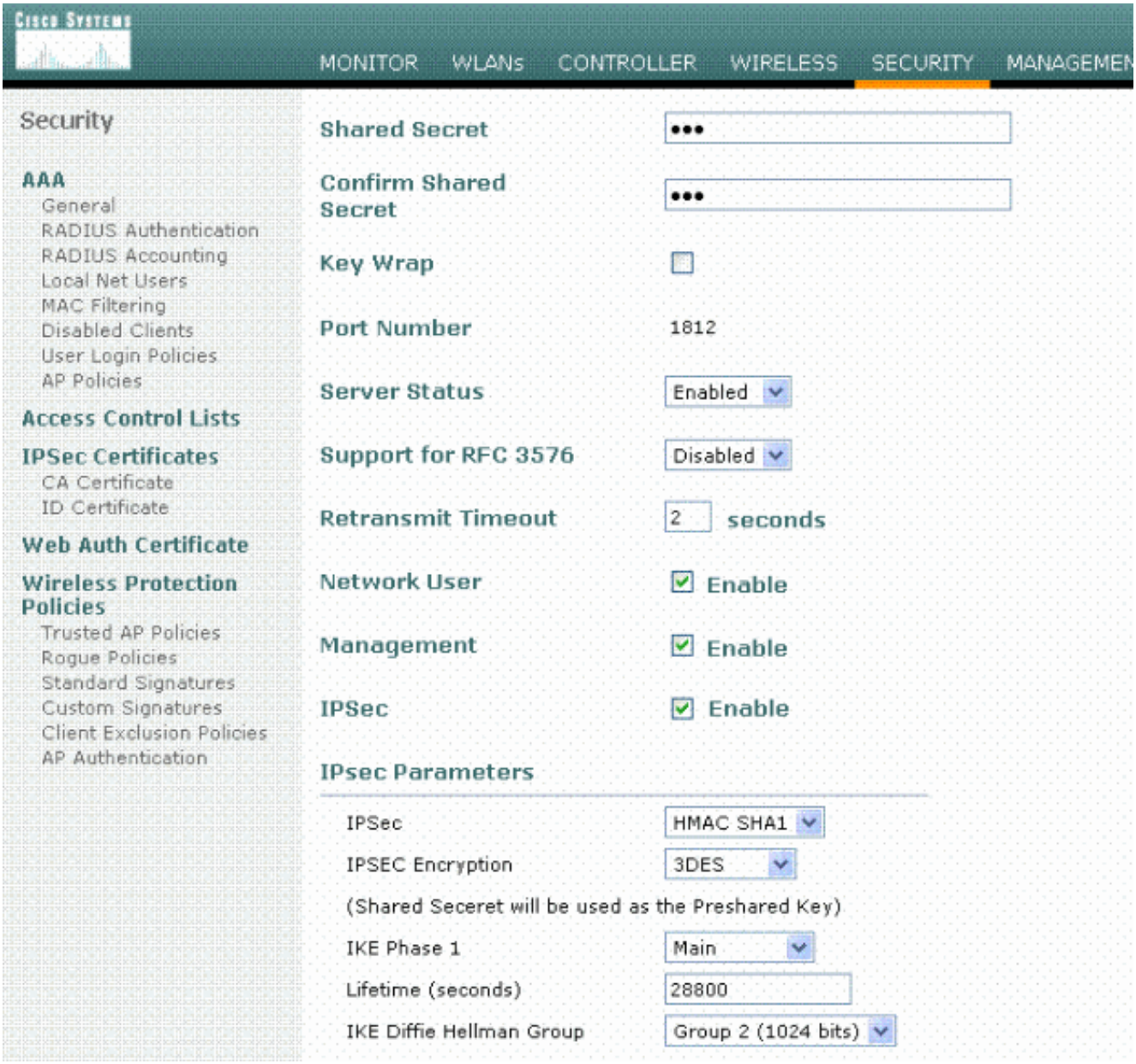
Этот раздел объясняет, как настроить IPSec на WLC через GUI.

От Графического интерфейса контроллера выполните эти шаги.

1. Перейдите к вкладке **Security> AAA> RADIUS Authentication** в Графическом интерфейсе контроллера и добавьте новый сервер RADIUS.



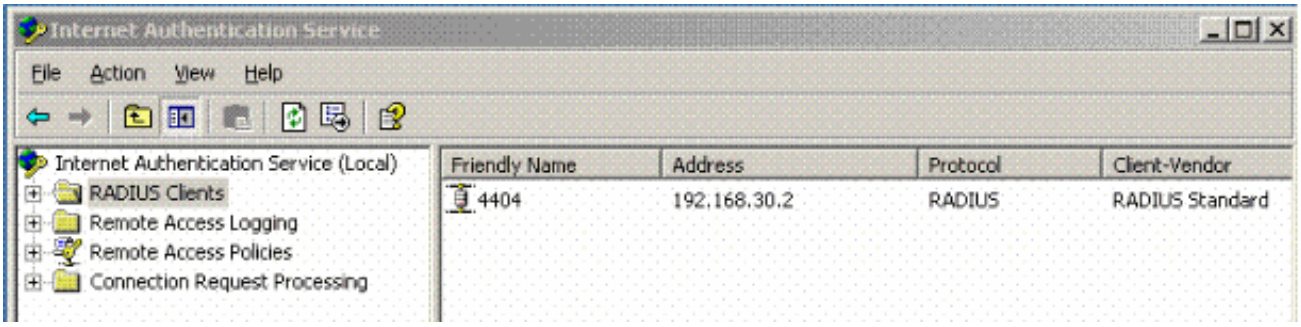
2. Настройте IP-адрес, порт 1812 и общий секретный ключ нового сервера RADIUS. Проверьте**, что IPSec Включает -** флажок, настраивает эти Параметры IPSec, и затем нажимает **Apply**.**Примечание:** Общий секретный ключ используется и для аутентификации сервера RADIUS и как Предварительного общего ключа (PSK) для Аутентификации
IPSec.



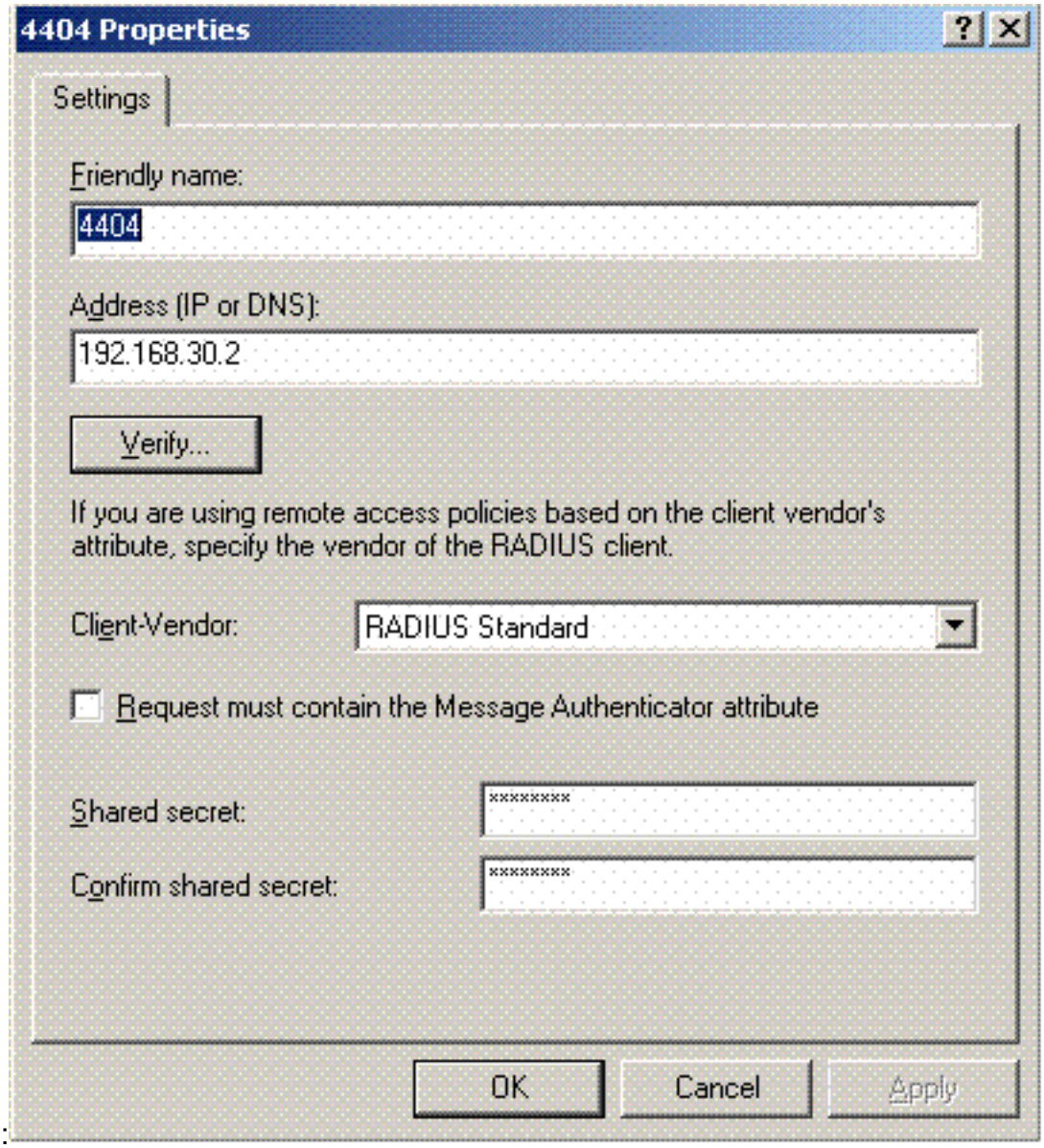
Настройте IAS

Выполните эти шаги на IAS:

1. Перейдите менеджеру IAS в Win2003 и добавьте нового КЛИЕНТА RADIUS.

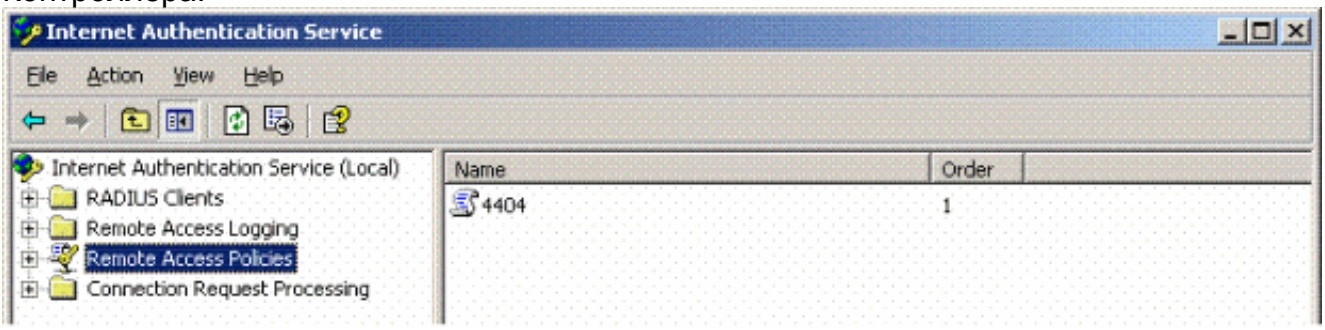


2. Настройте свойства Клиента RADIUS с IP-адресом и общим секретным ключом, настроенным на

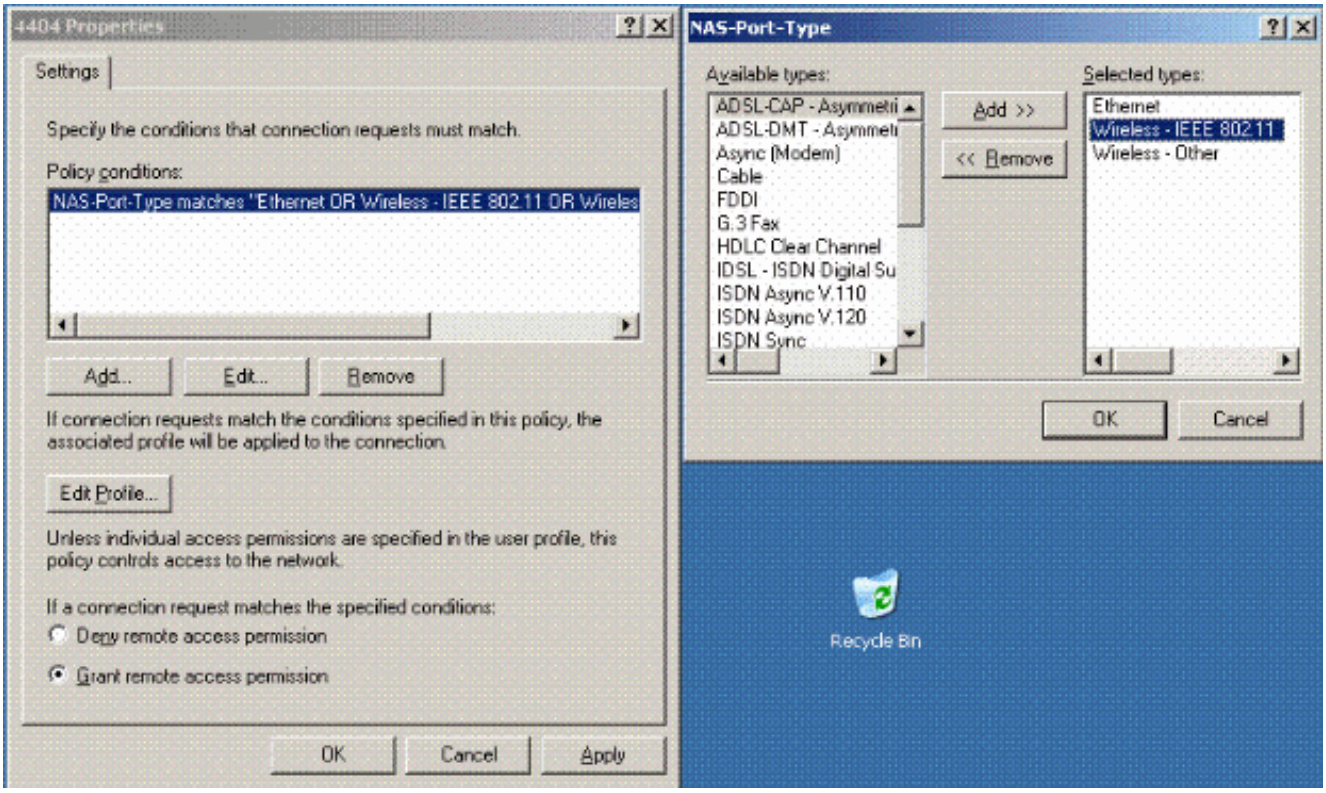


Контроллере:

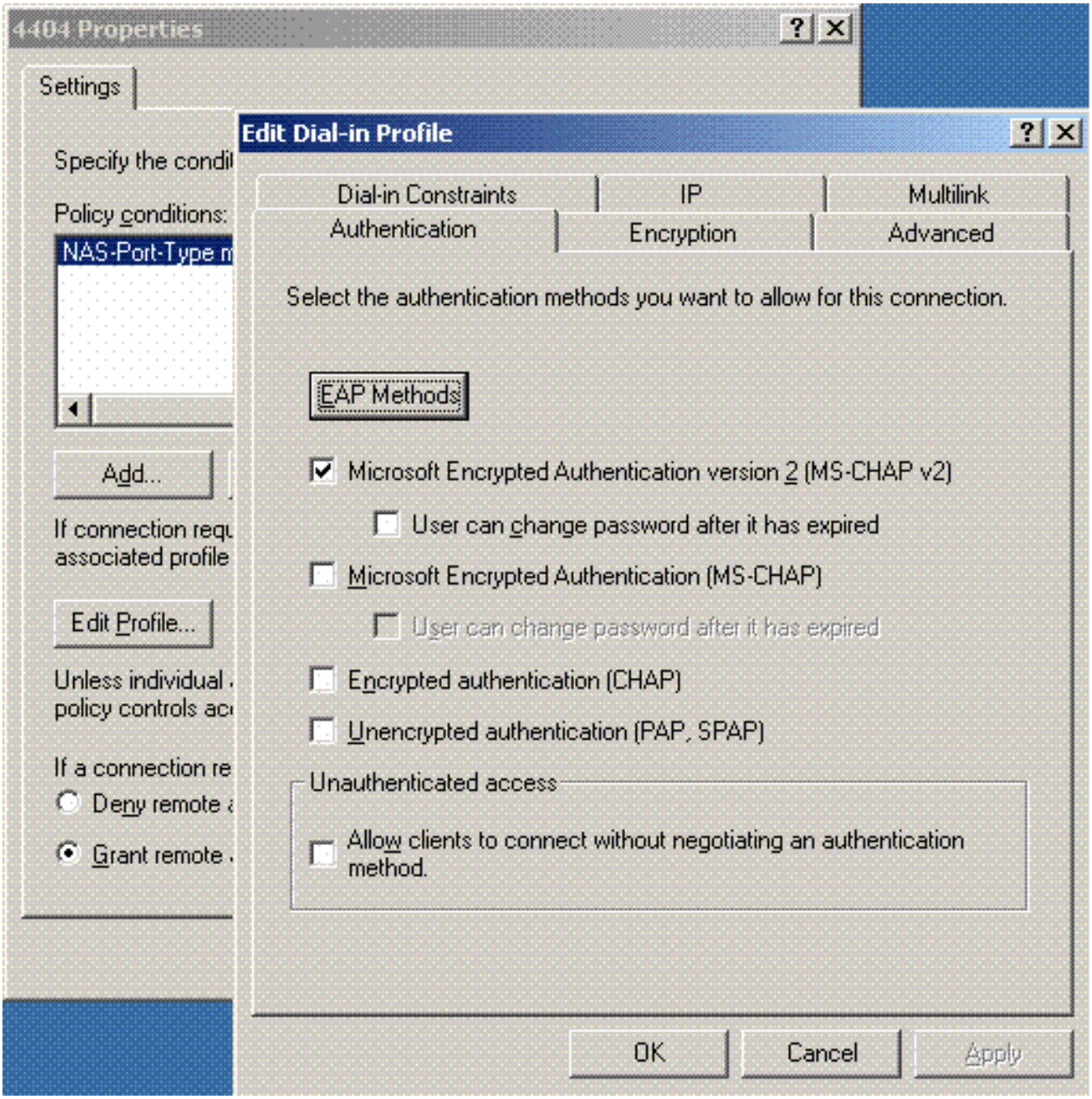
3. Настройте новую Политику Удаленного доступа для Контроллера:



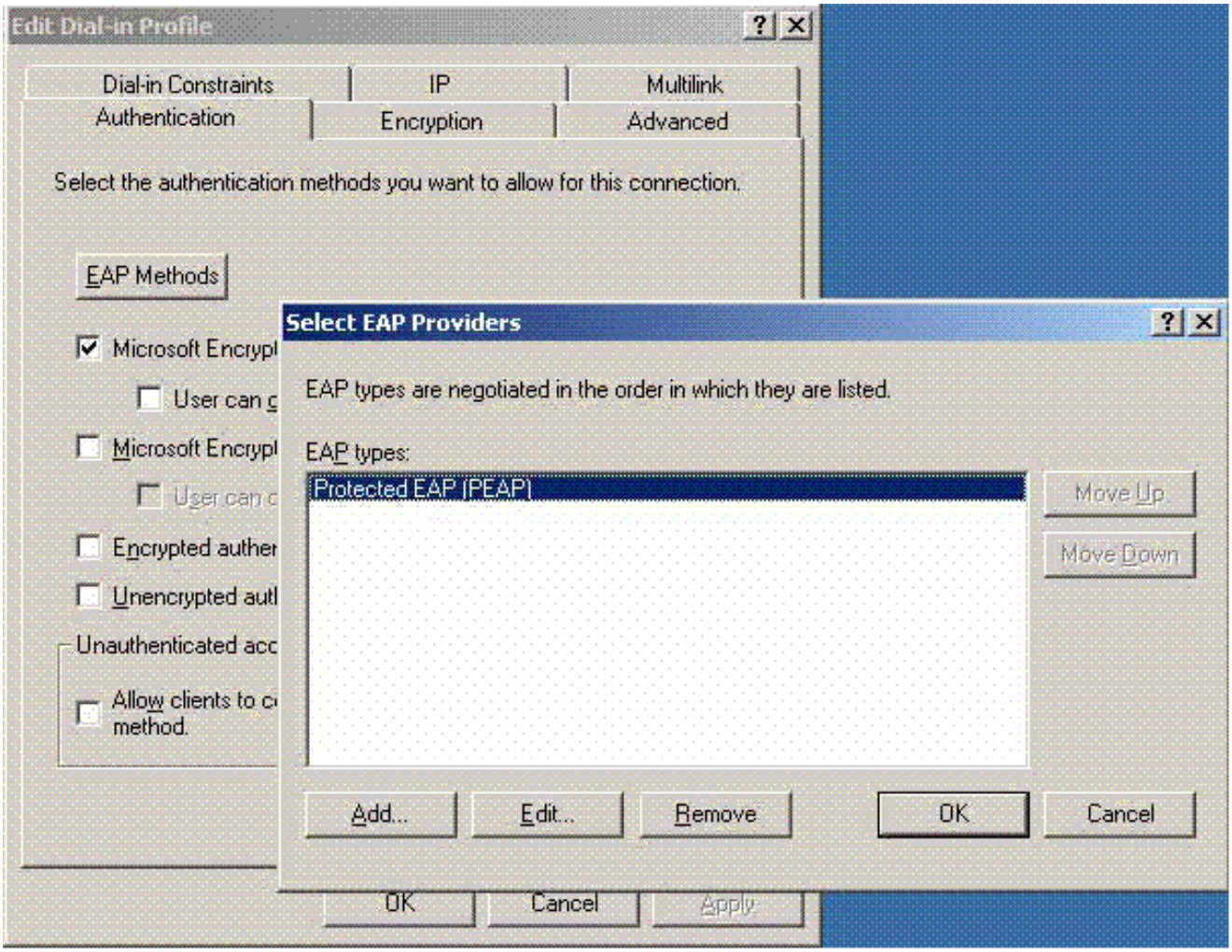
4. Отредактируйте свойства Политики Удаленного доступа Контроллера. Удостоверьтесь, что добавили Тип порта NAS - беспроводные сети – IEEE 802.11:



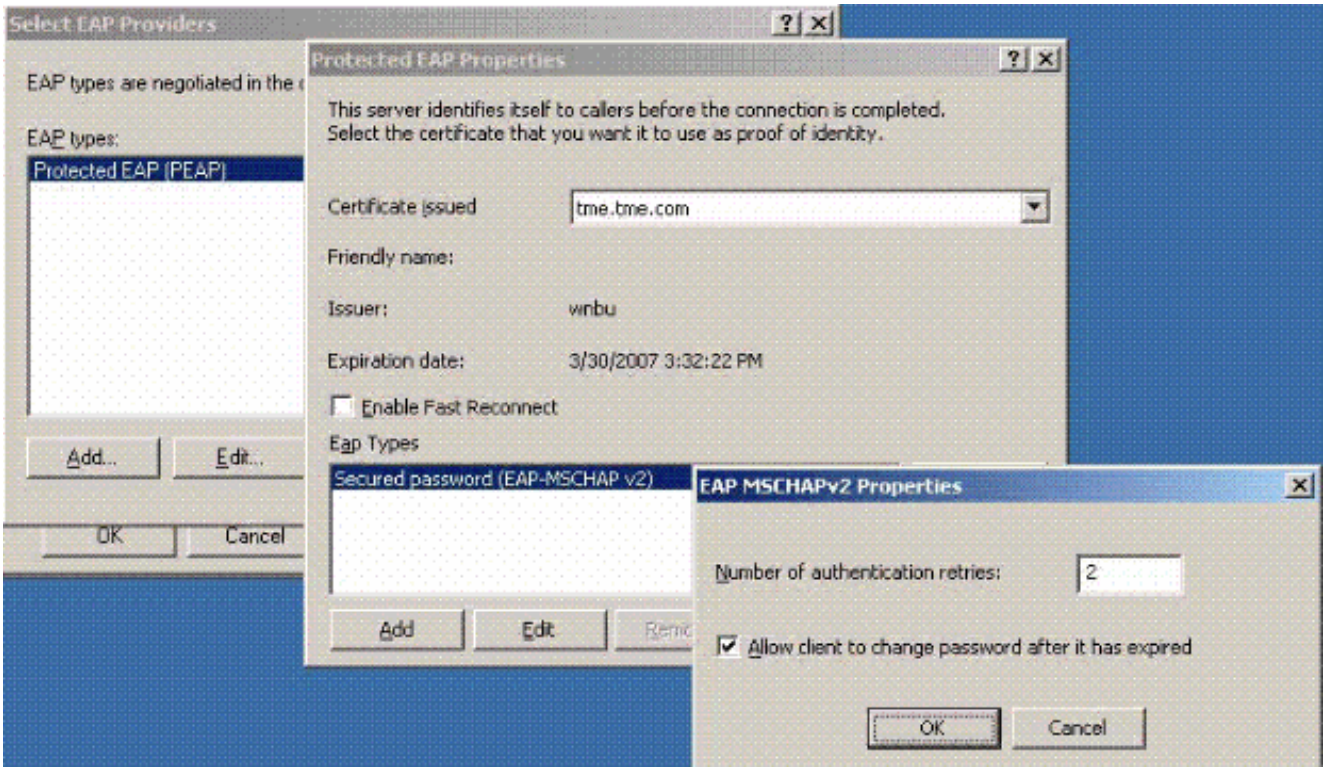
5. Нажмите **Edit Profile**, нажмите **вкладку Authentication** и проверьте MS-CHAP v2 для Аутентификации:



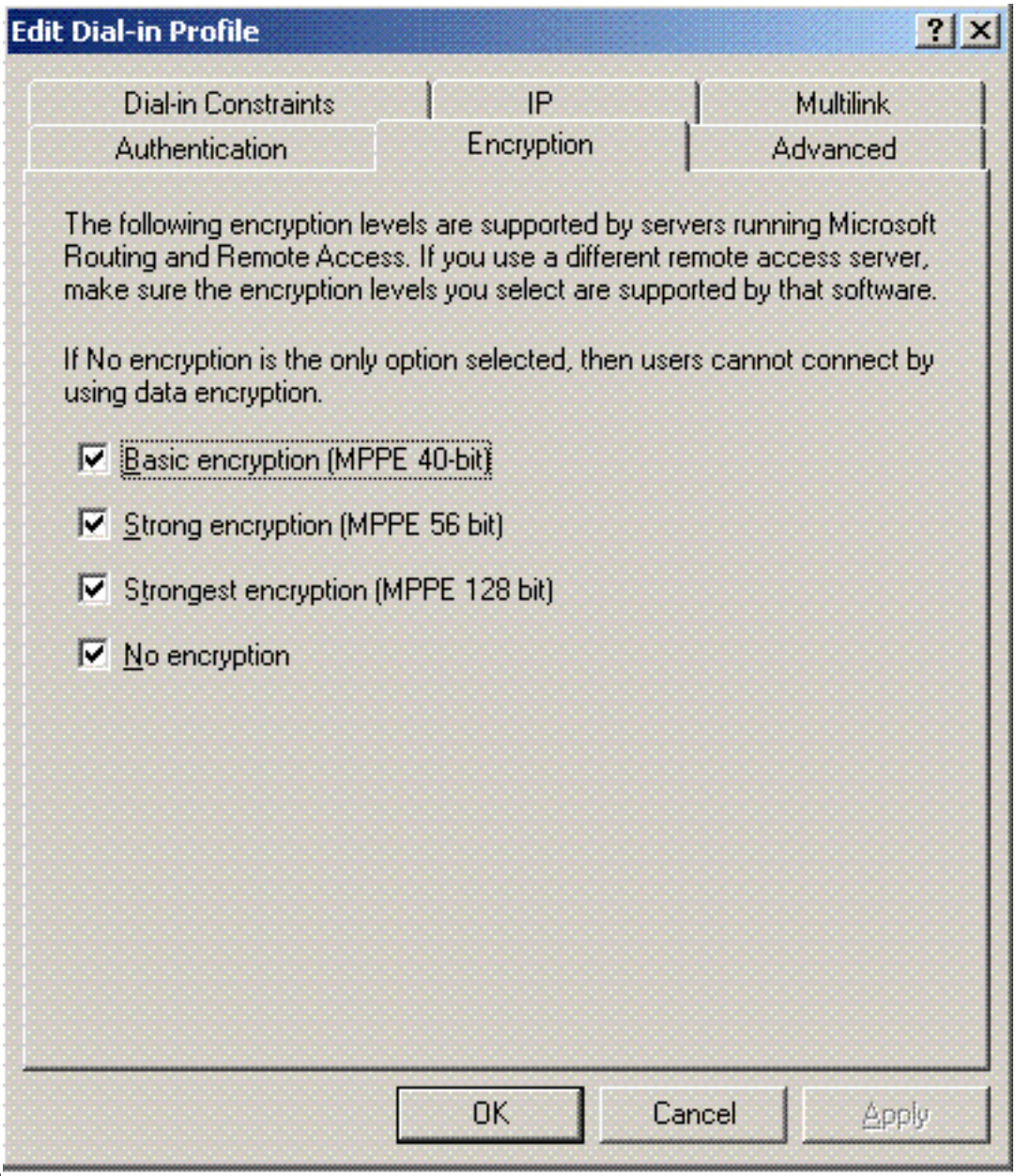
6. Нажмите **EAP Methods**, выберите EAP Providers и добавьте PEAP как тип EAP:



7. Нажмите **Edit on Select EAP Providers** и выберите из выпадающее меню сервер, привязанный к вашим учетным записям Пользователя Active Directory и CA (например, tme.tme.com). Добавьте MSCHAP v2 типа
EAP:

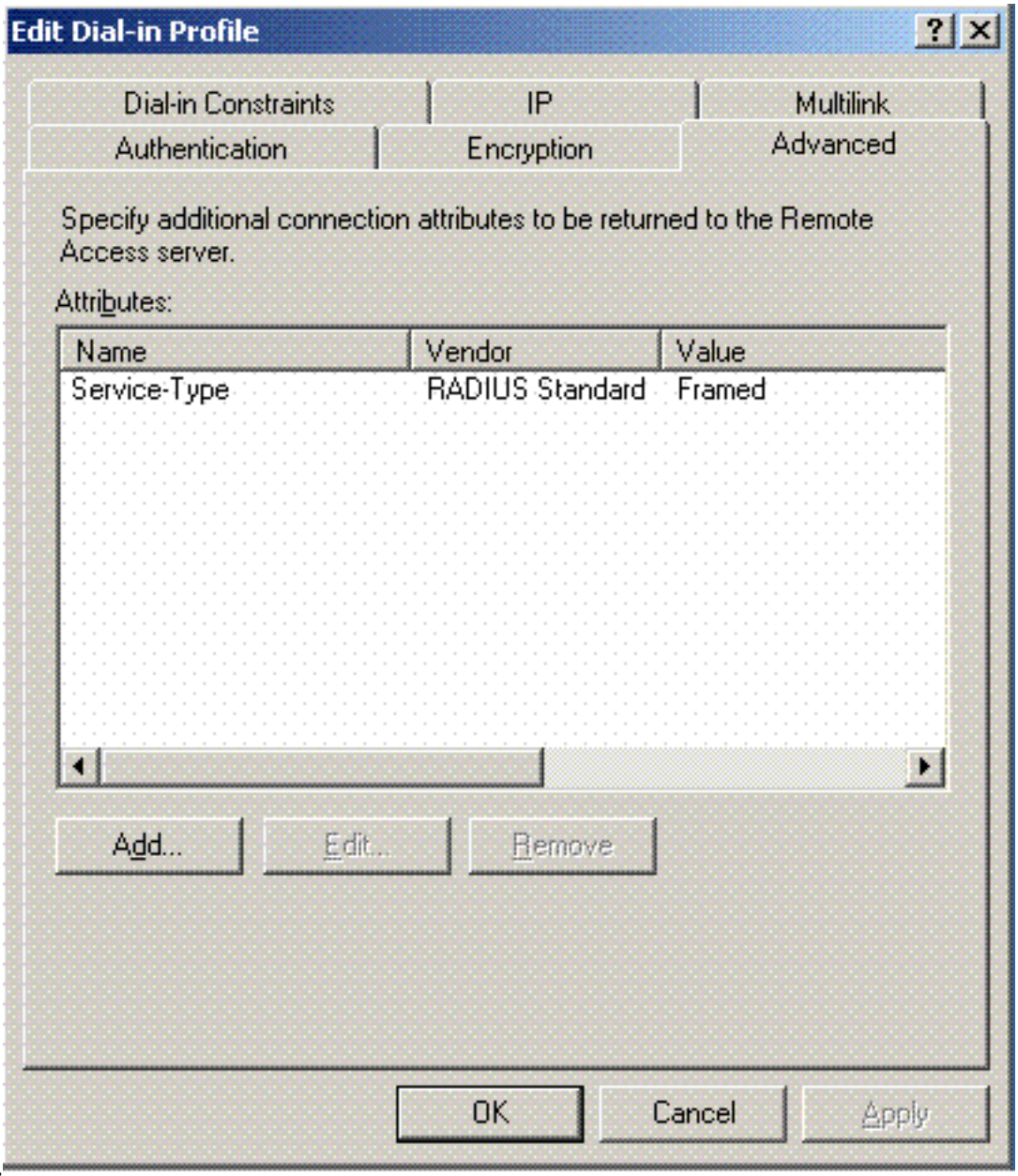


8. Нажмите **вкладку Encryption** и проверьте все типы шифрования для удаленного



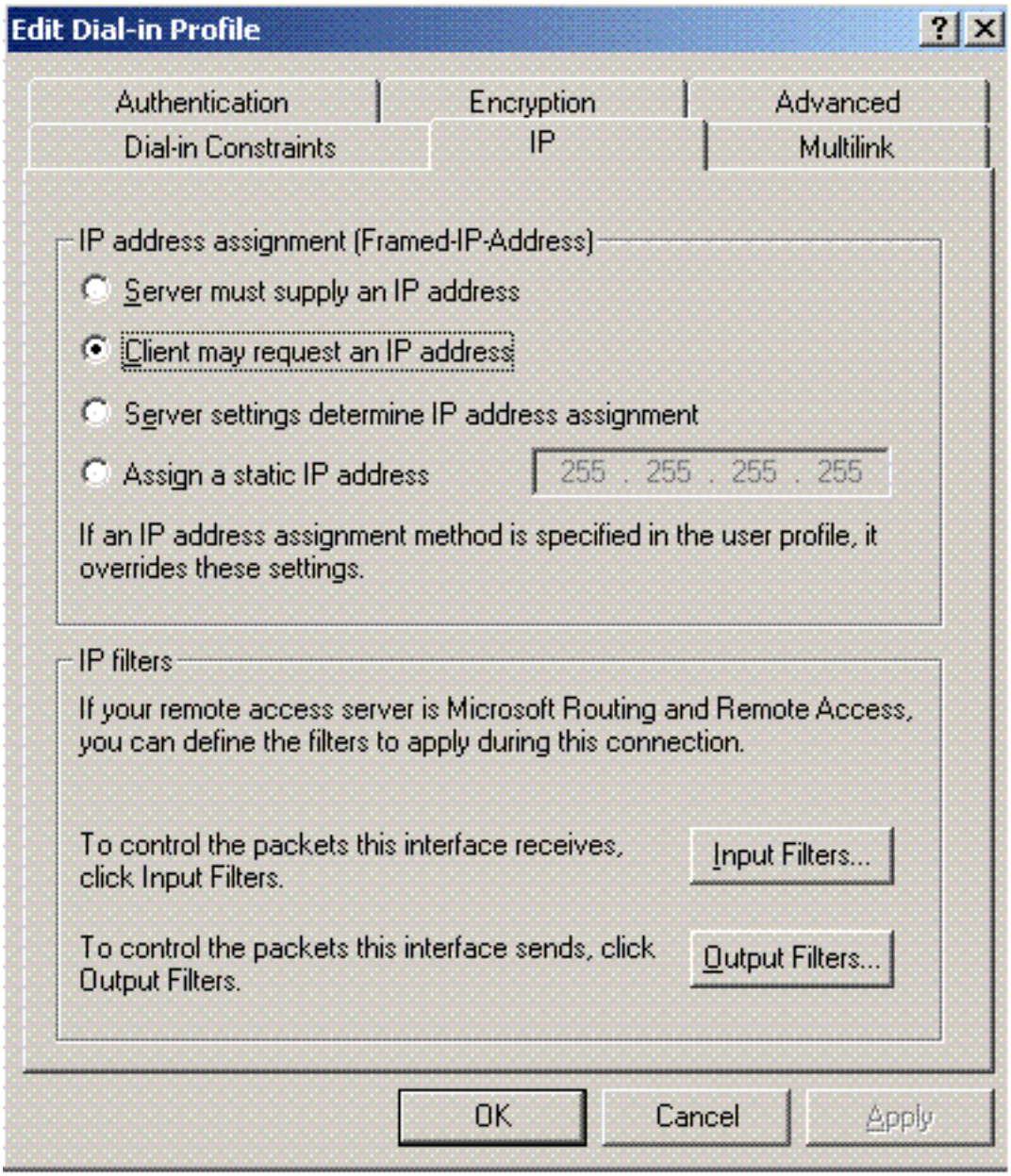
доступа:

9. Нажмите **Вкладку Дополнительно** и добавьте Стандарт RADIUS / Обрамленный как



Service-Type:

10. Нажмите вкладку **IP** и проверьте**, что Клиент может запросить IP-адрес**. Это предполагает, что вам включили DHCP на коммутаторе или

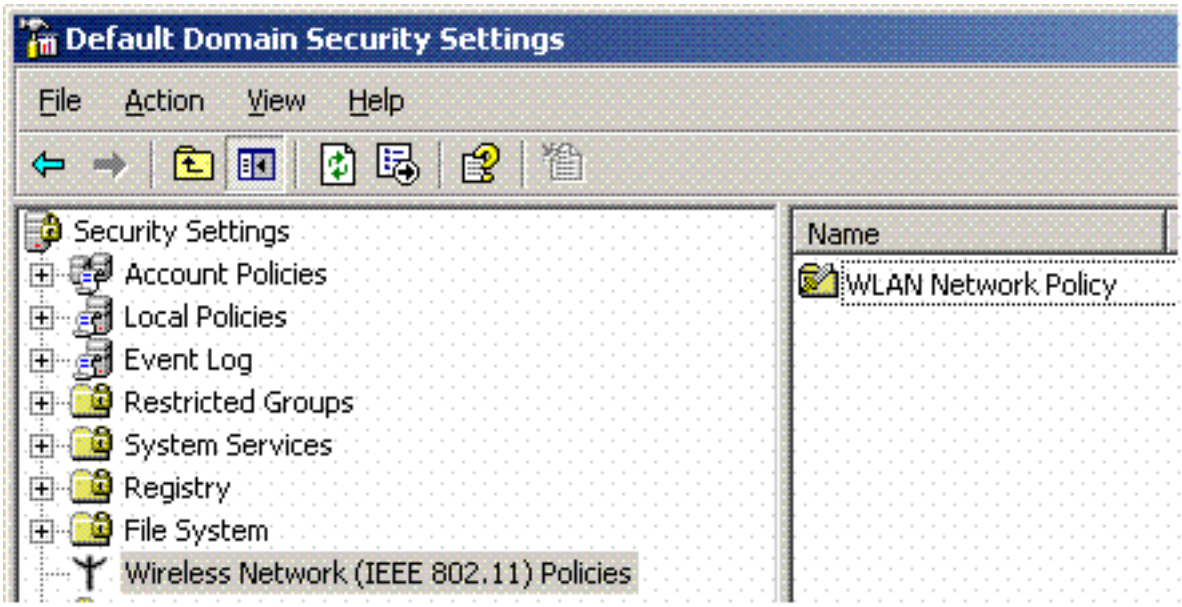


WinServer.

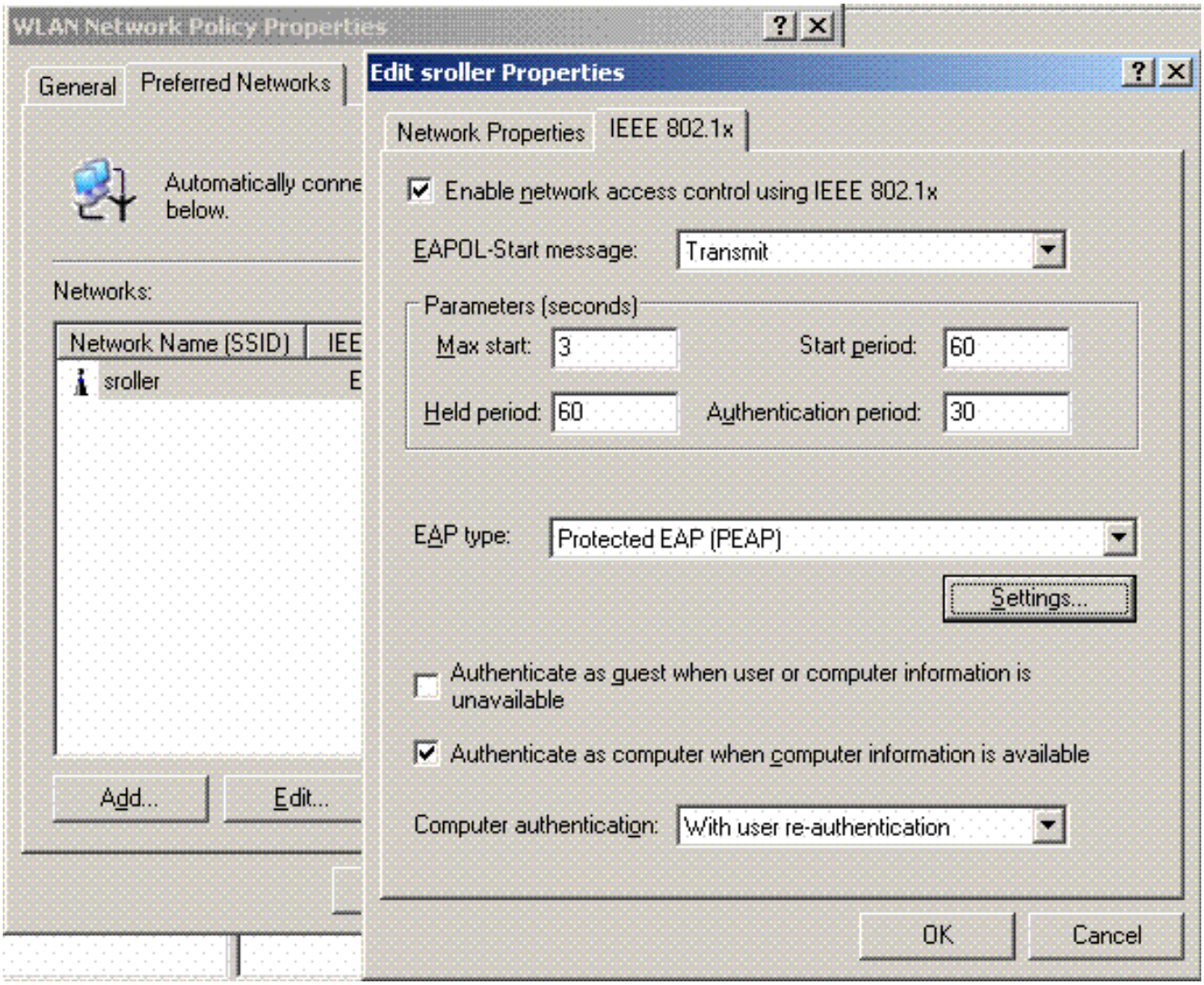
Параметры настройки безопасности домена Microsoft Windows 2003 года

Выполните эти шаги для настройки параметров настройки безопасности домена Windows 2003:

1. Запустите менеджера Параметров безопасности Домена по умолчанию и создайте новую политику безопасности для Беспроводной сети (IEEE 802.11) Политика.

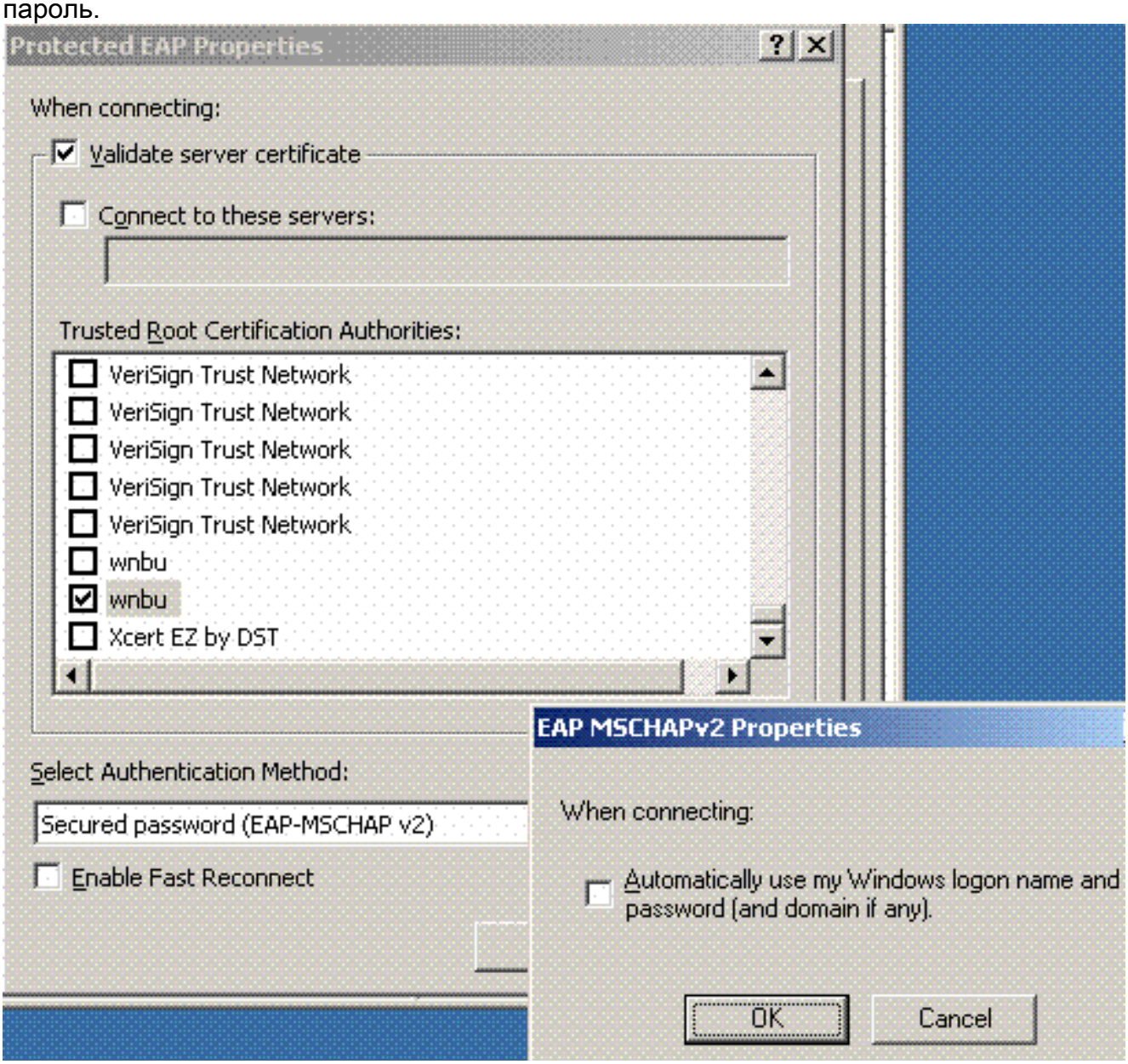


2. Открытые Свойства Policy Сети WLAN, и нажимают **Preferred Networks**. Добавьте новый предпочтительный WLAN и введите имя своего SSID WLAN, такого как `Wireless`. Двойной щелчок, что новая предпочтительная сеть и щелчок вкладка **IEEE 802.1x**. Выберите PEAP в качестве типа
EAP:

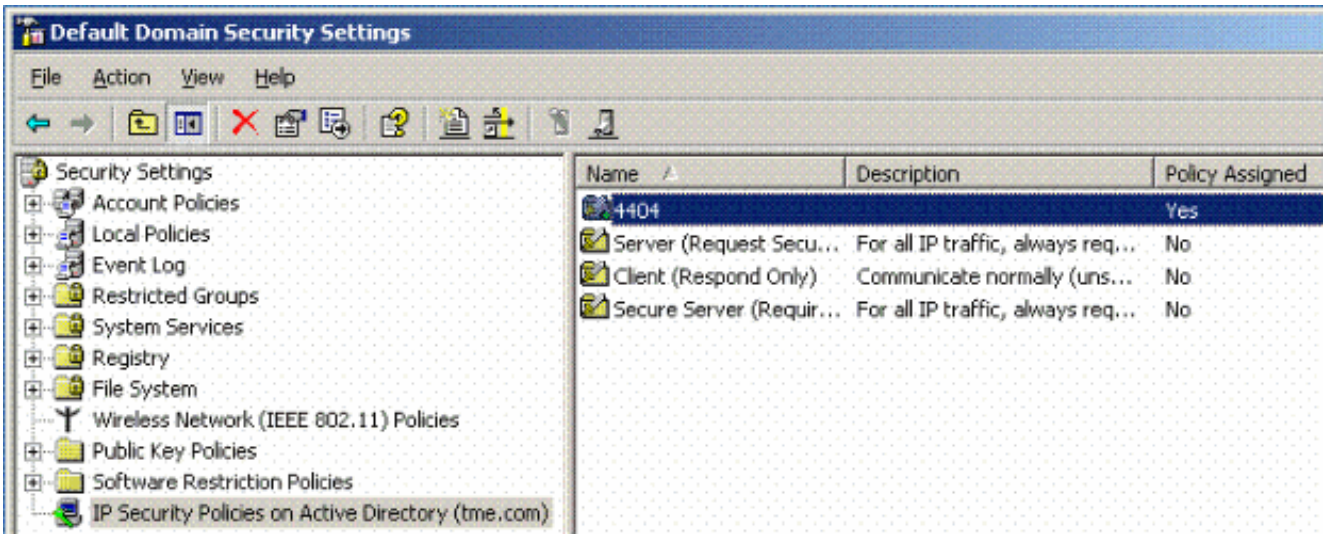


3. Нажмите **PEAP Settings**, проверка **Проверяют серверный сертификат** и выбирают Trusted Root Cert, установленный на Центре сертификации. Для тестирования снимите флажок с коробкой CHAP v2 MS для Автоматически использования мой вход в систему

Windows и
пароль.

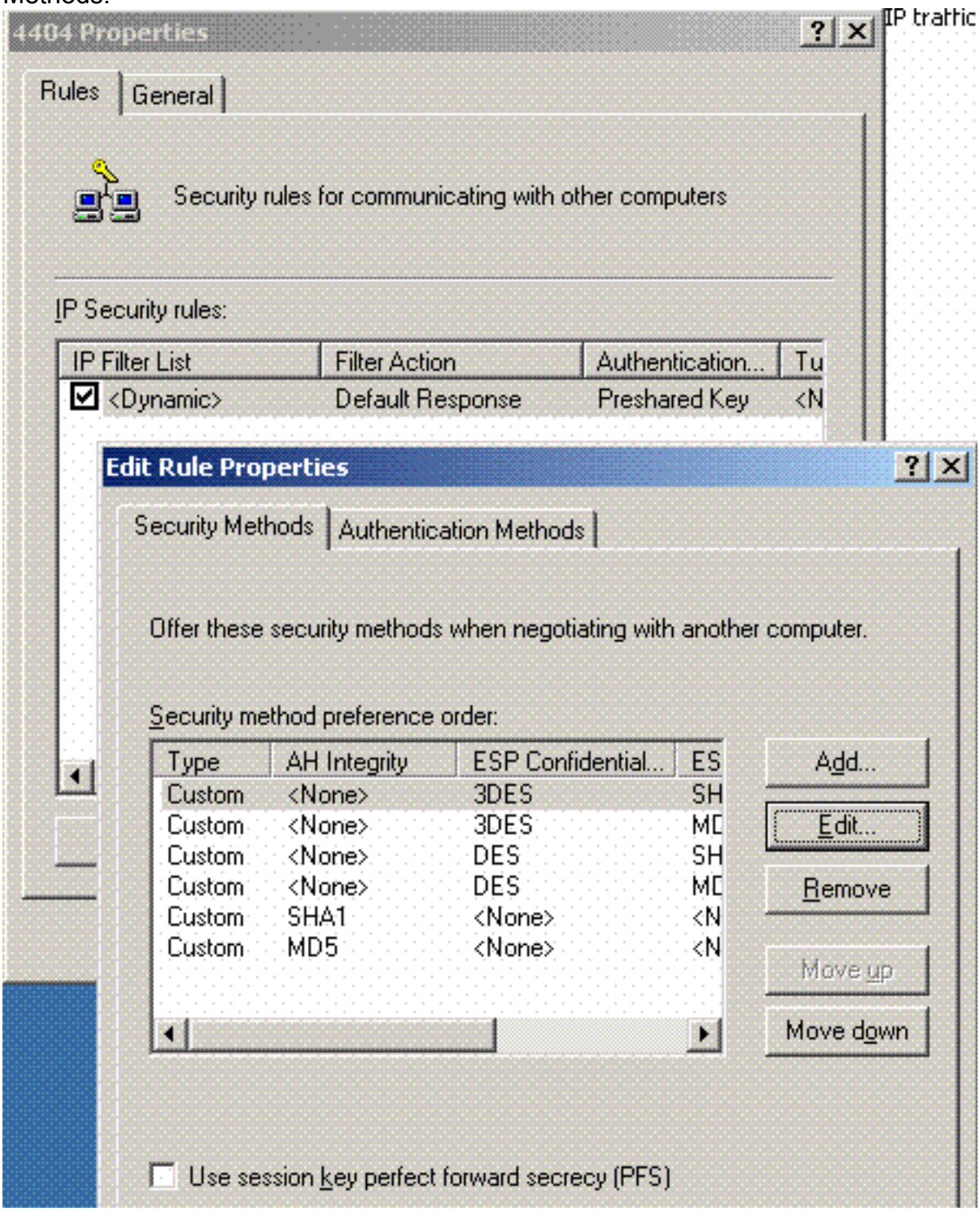


4. В окне менеджера Windows 2003 Default Domain Security Settings создайте другую новую IP-безопасность Политика по политике Active Directory, такой как **4404**.

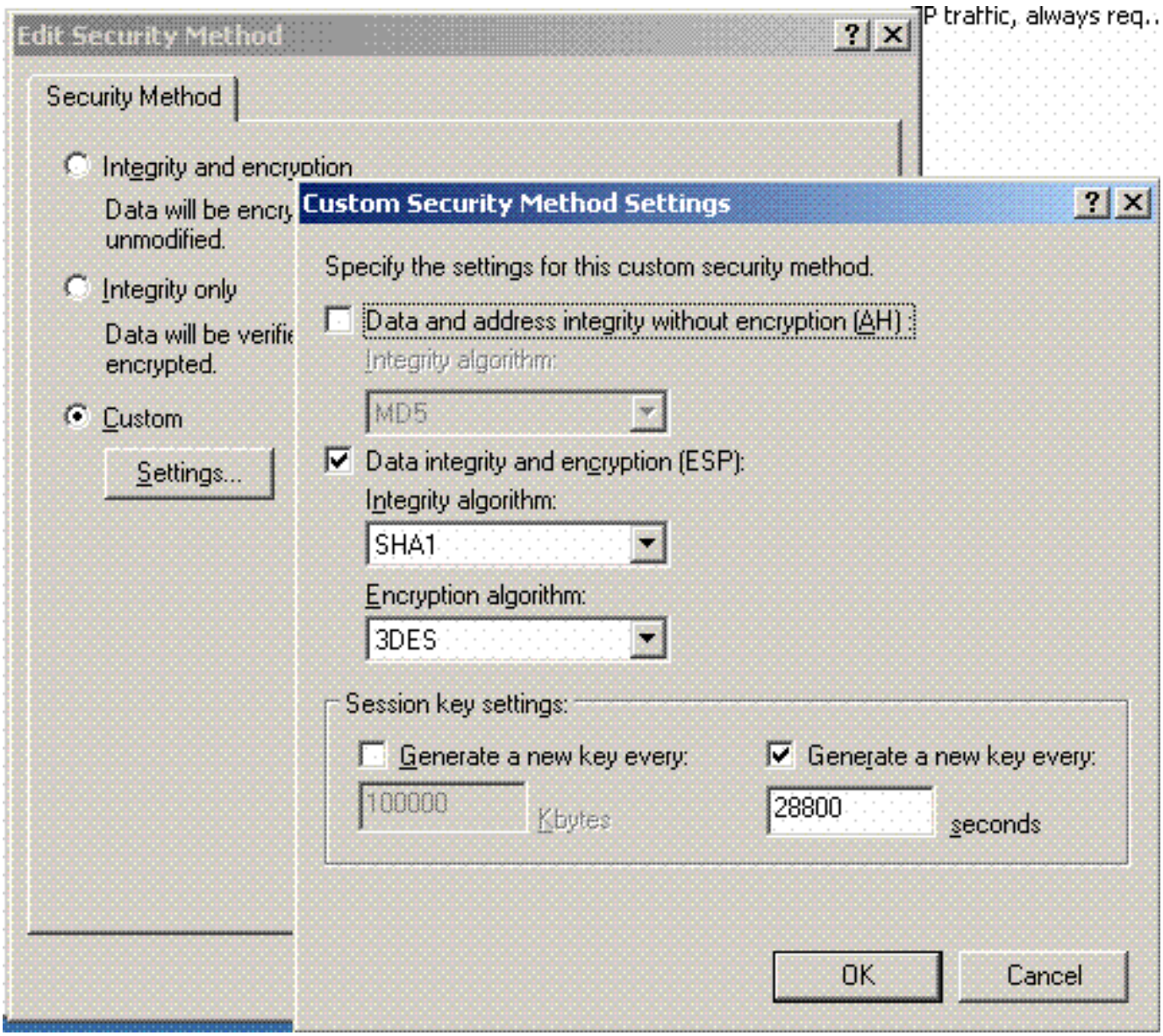


5. Отредактируйте новые 4404 свойства policy и нажмите вкладку **Rules**. Добавьте новое

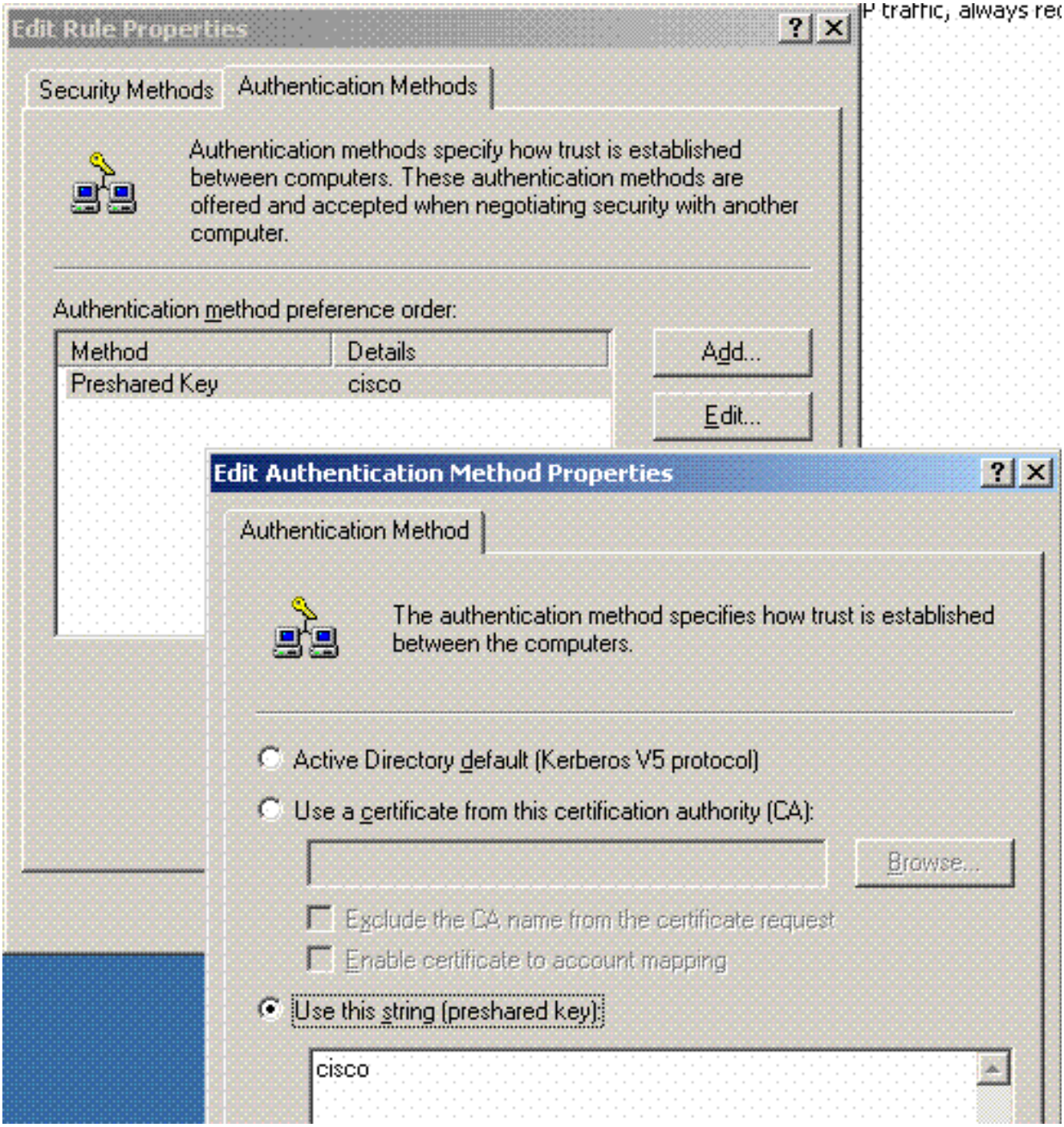
правило фильтрации - (Динамичный) Список Филе IP; Действие фильтрации (Ответ По умолчанию); Аутентификация (PSK); Туннель (Ни один). Двойной щелчок недавно созданное правило фильтрации и выбирает Security Methods:



6. Нажмите **Edit Security Method** и нажмите кнопку с зависимой фиксацией **Custom Settings**. Выберите эти параметры настройки.**Примечание:** Эти параметры настройки должны совпасть с параметрами настройки Безопасности IPsec RADIUS Контроллера.



7. Нажмите **вкладку Authentication Method** под Свойствами Правила Редактирования. Введите тот же общий секретный ключ, что вы ранее ввели в Конфигурацию RADIUS Контроллера.



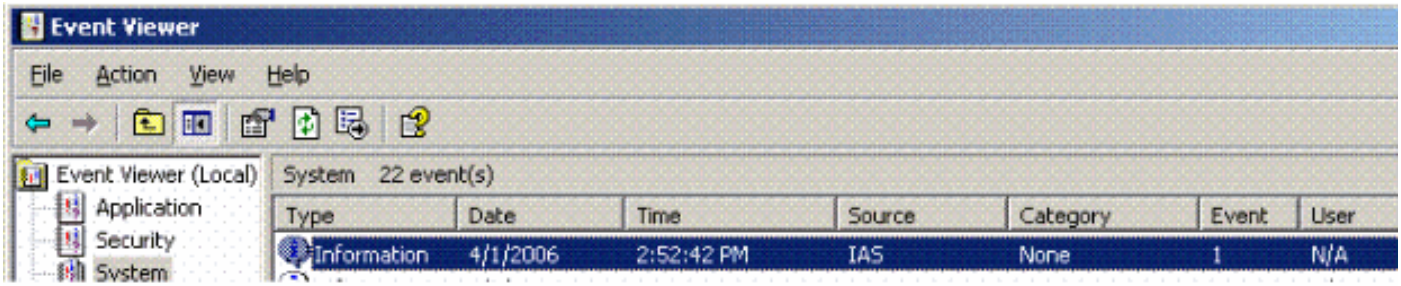
На этом этапе все конфигурации для Контроллера, IAS и Параметров настройки Безопасности домена завершены. Сохраните все конфигурации и на Контроллере и на WinServer и перезагрузке все машины. На клиенте WLAN, который используется для тестирования, установите корневое свидетельство и настройте для WPA2/PEAP. После того, как корневое свидетельство установлено на клиенте, перезагрузите клиентский компьютер. После всей перезагрузки машин подключите клиента с WLAN и перехватите эти регистрационные события.

Примечание: Клиентское соединение требуется для устанавливания IP - безопасного соединения между Контроллером и WinServer RADIUS.

Windows 2003 System Log Events

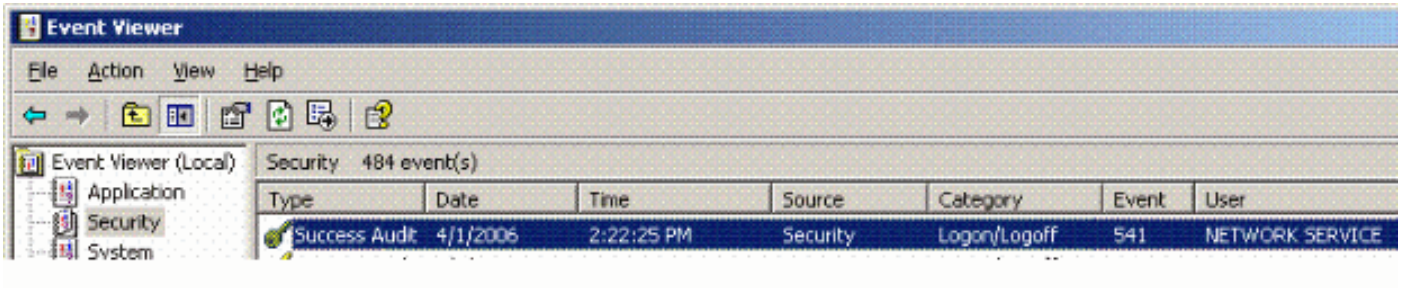
Успешное соединение клиента WLAN, настроенное для WPA2/PEAP с включенным RADIUS IPSec, генерирует это Системное событие на WinServer:

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)
```

Успешный Контроллер <> IP - безопасное соединение RADIUS генерирует это Событие связанное с безопасностью на журналах 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
```

Пример отладки успеха IPSec RADIUS контроллера беспроводной локальной сети

Можно использовать **debug pm** команды отладки **ikemsg, включают** на контроллере для проверки этой конфигурации. Например.

```
(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
```

Перехват Ethreal

Вот типовой Перехват Ethreal.

```
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
```

Дополнительные сведения

- Руководство по конфигурированию контроллера Cisco Wireless LAN, выпуск 5.2
- Cisco Systems – техническая поддержка и документация