Configurez la sécurité IPSec de RADIUS serveur pour de WLCs et de Microsoft Windows 2003 IAS

Contenu

Introduction

Documents de ce guide comment configurer la caractéristique de RADIUS IPSec prise en charge par WCS et ces contrôleurs WLAN :

- Gamme 4400
- WiSM
- 3750G

La caractéristique de RADIUS IPSec de contrôleur se trouve sur le GUI de contrôleur sous la **Sécurité > l'AAA > la** section de **serveurs d'authentification RADIUS**. La caractéristique fournit une méthode pour que vous chiffriez toutes les transmissions de RADIUS entre les contrôleurs et les serveurs de RADIUS (IAS) avec IPSec.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- La connaissance sur LWAPP
- La connaissance sur l'authentification et l'IPSec de RADIUS

- La connaissance sur la façon dont configurer des services sur le système d'exploitation de serveur Windows 2003

Composants utilisés

Ces le réseau et les composants logiciels doivent être installés et configurés afin de déployer la caractéristique de RADIUS IPSec de contrôleur :

- WLC 4400, WiSM, ou contrôleurs 3750G. Cet exemple utilise WLC 4400 qui exécute la version de logiciel 5.2.178.0
- Point d'accès léger (recouvrements). Cet exemple utilise le RECOUVREMENT de gamme 1231.
- Commutez avec le DHCP
- Serveur de Microsoft 2003 configuré comme contrôleur de domaine installé avec Microsoft Certificate Authority et avec le Service d'authentification Internet de Microsoft (IAS).
- Sécurité de domaine de Microsoft
- Adaptateur client sans fil du 802.11 a/b/g de Cisco avec la version 3.6 ADU configurée avec WPA2/ PEAP

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configuration RADIUS d'IPSec

Ce guide de configuration n'adresse pas l'installation ou la configuration de Microsoft WinServer, autorité de certification, Répertoire actif ou client de 802.1x WLAN. Ces composants doivent être installés et configurés avant le déploiement de la caractéristique d'IPSec RADIUS de contrôleur. Le reste des documents de ce guide comment configurer IPSec RADIUS sur ces composants :

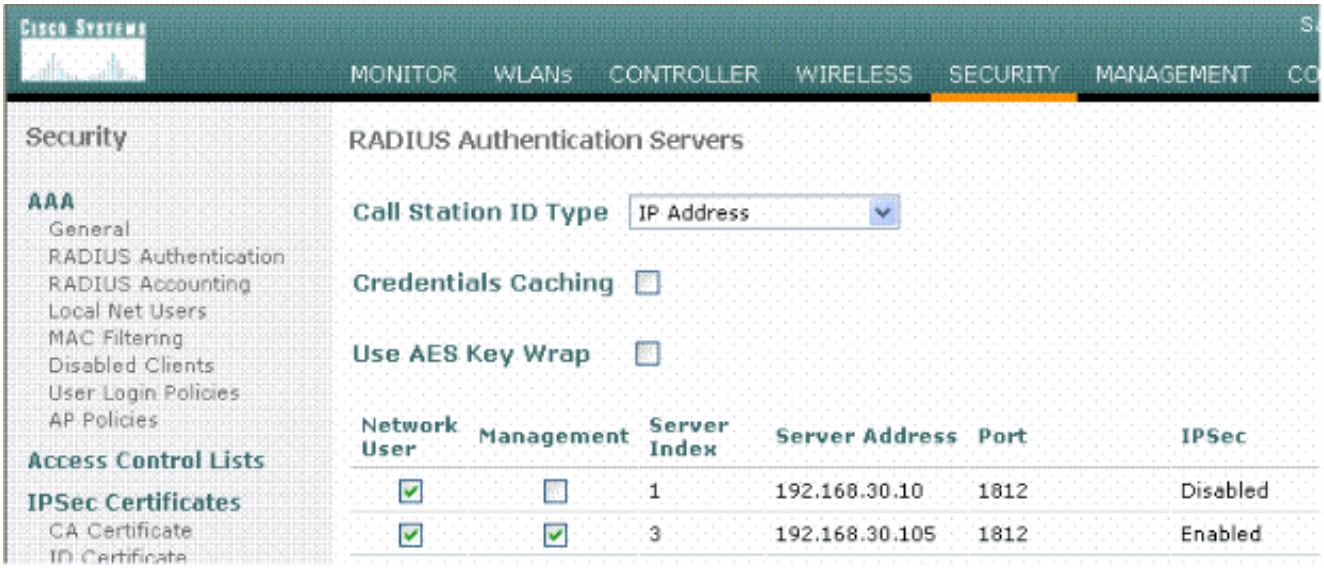
1. Contrôleurs de WLAN Cisco
2. Windows 2003 IAS
3. Paramètres de sécurité de domaine de Microsoft Windows

Configurez le WLC

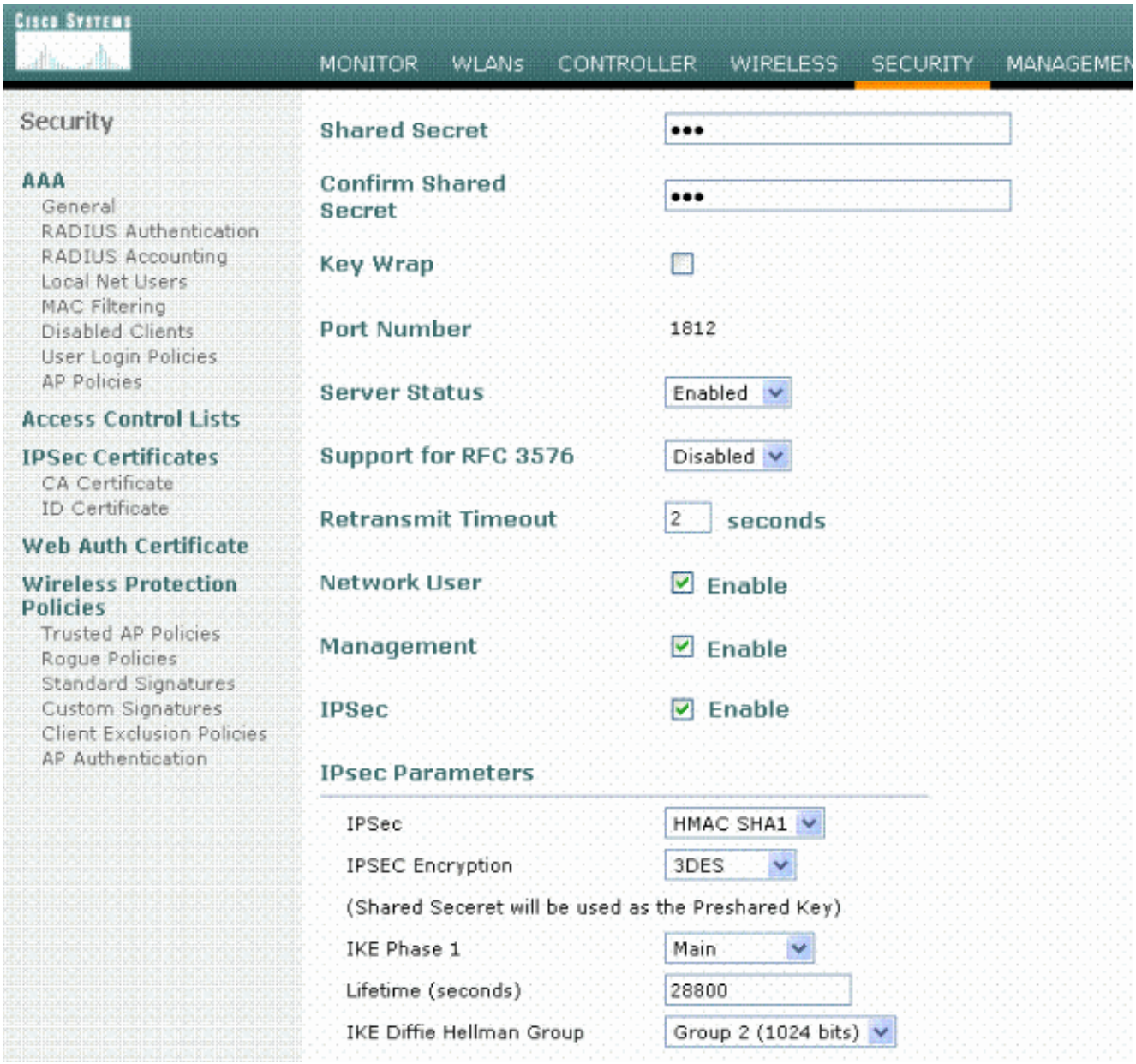
Cette section explique comment configurer IPSec sur le WLC par le GUI.

Du GUI de contrôleur, terminez-vous ces étapes.

1. Naviguez vers l'onglet de **Sécurité > d'authentification d'AAA > de RADIUS** dans le GUI de contrôleur, et ajoutez un nouveau serveur de RADIUS.



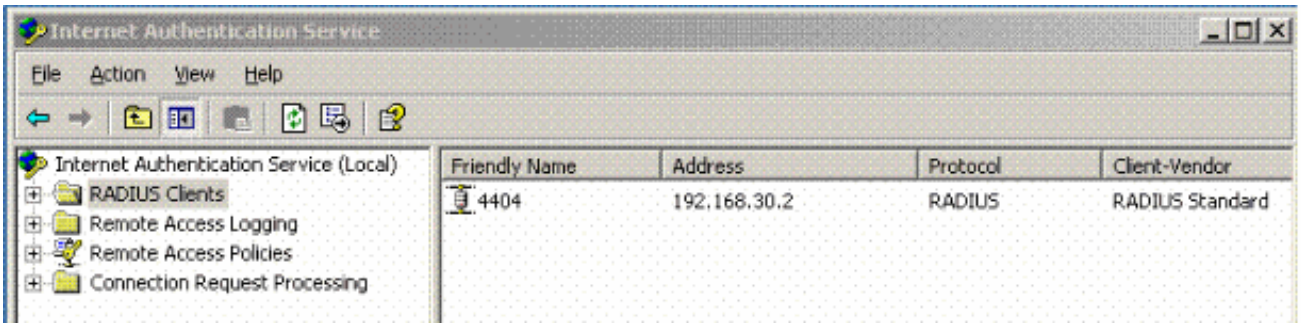
2. Configurez l'adresse IP, le port 1812, et un secret partagé du nouveau serveur de RADIUS. Cochez l'**IPSec activent la** case, configurent ces paramètres d'IPSec, et puis cliquent sur Apply.**Remarque:** Le secret partagé est utilisé pour authentifier le serveur de RADIUS et comme clé pré-partagée (PSK) pour l'authentification d'IPSec.



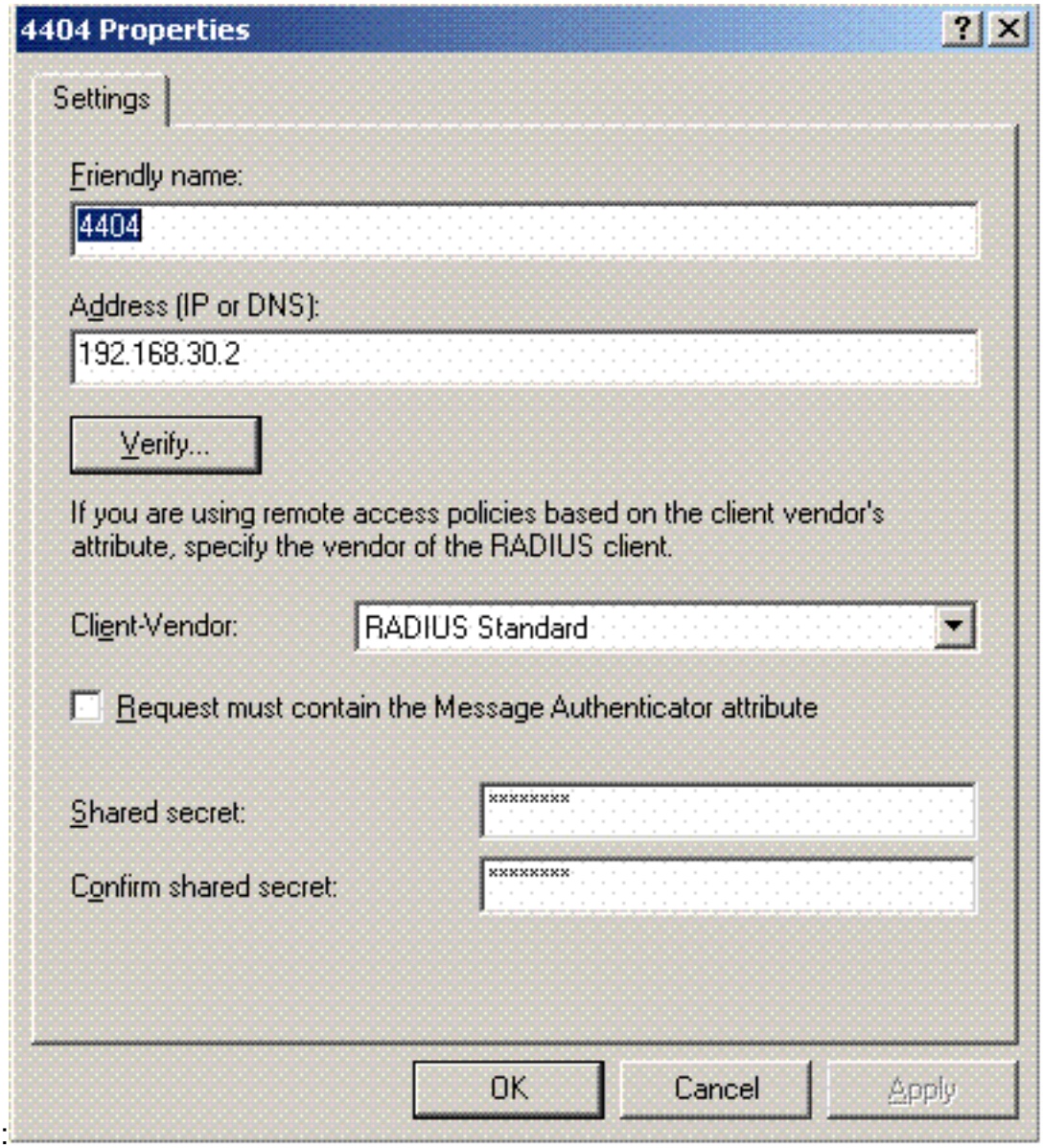
Configurez IAS

Terminez-vous ces étapes sur IAS :

1. Naviguez vers le gestionnaire d'IAS dans Win2003 et ajoutez un nouveau client RADIUS.

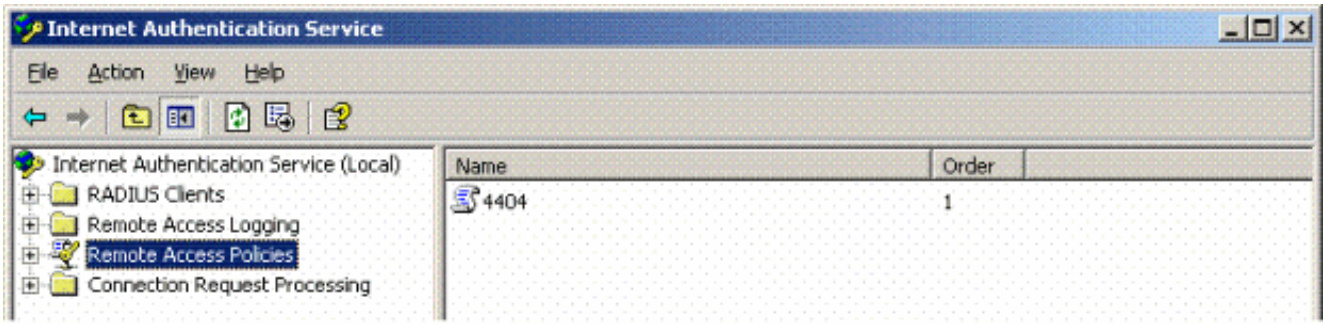


2. Configurez les propriétés de client RADIUS avec l'adresse IP et le secret partagé configurés sur le contrôleur

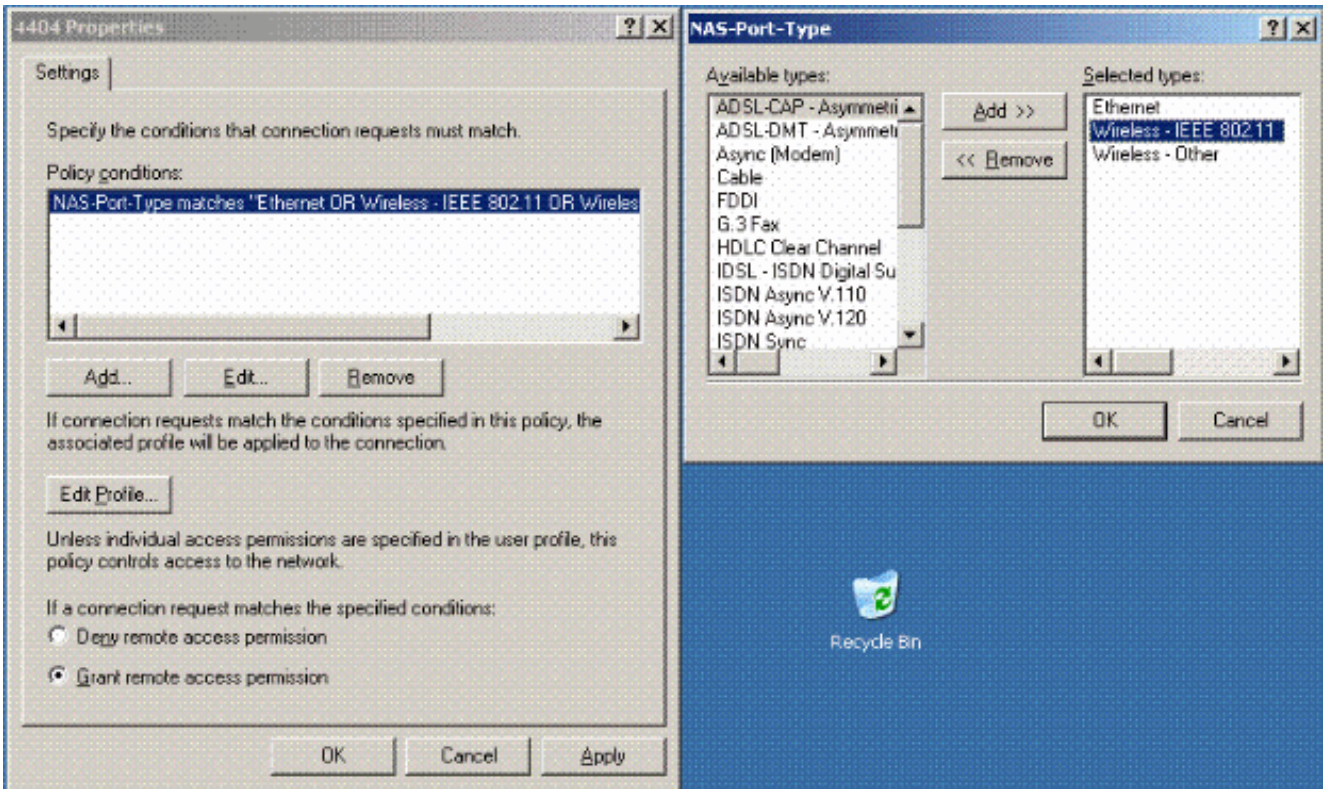


:

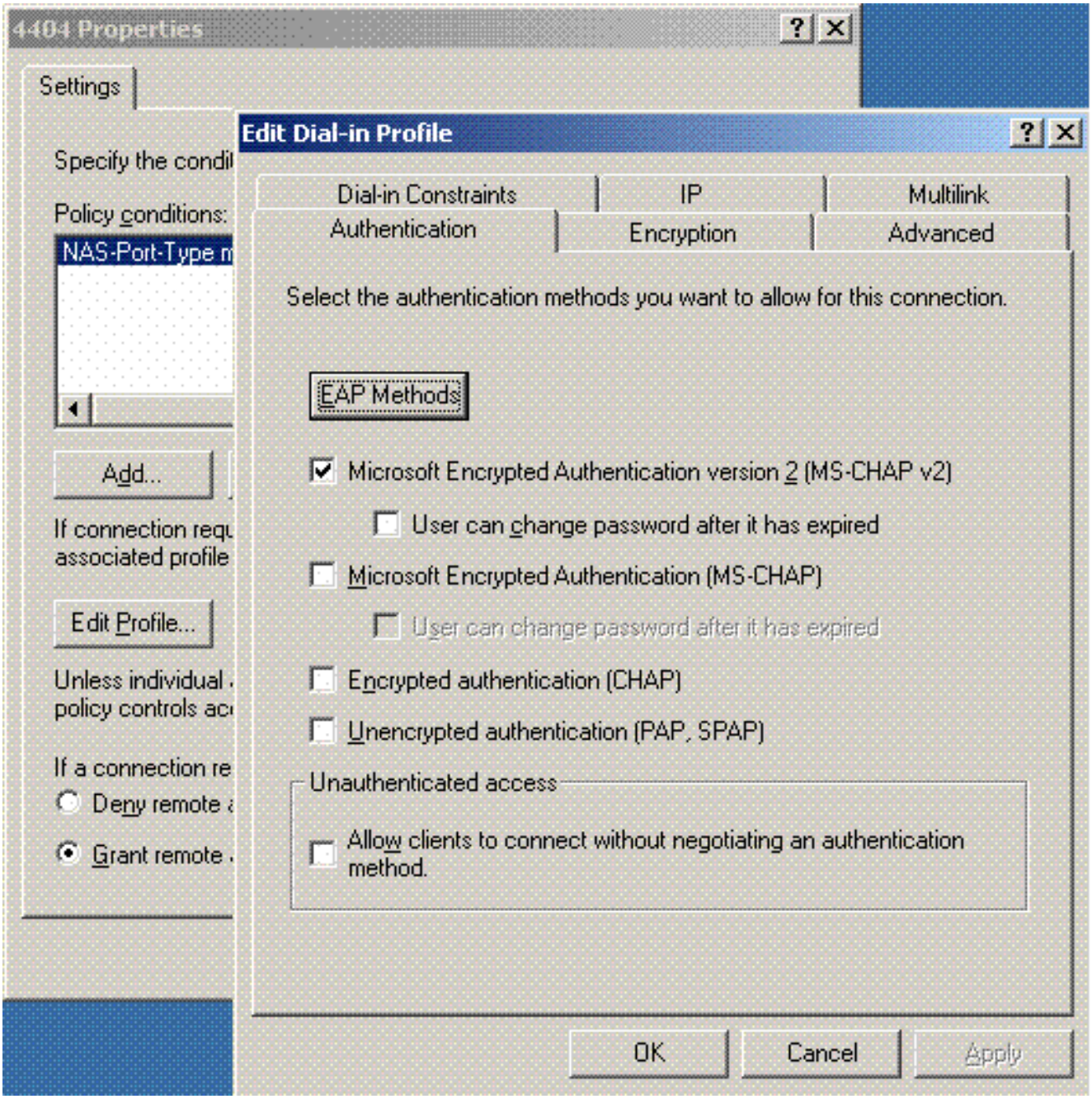
3. Configurez une nouvelle stratégie d'accès à distance pour le contrôleur :



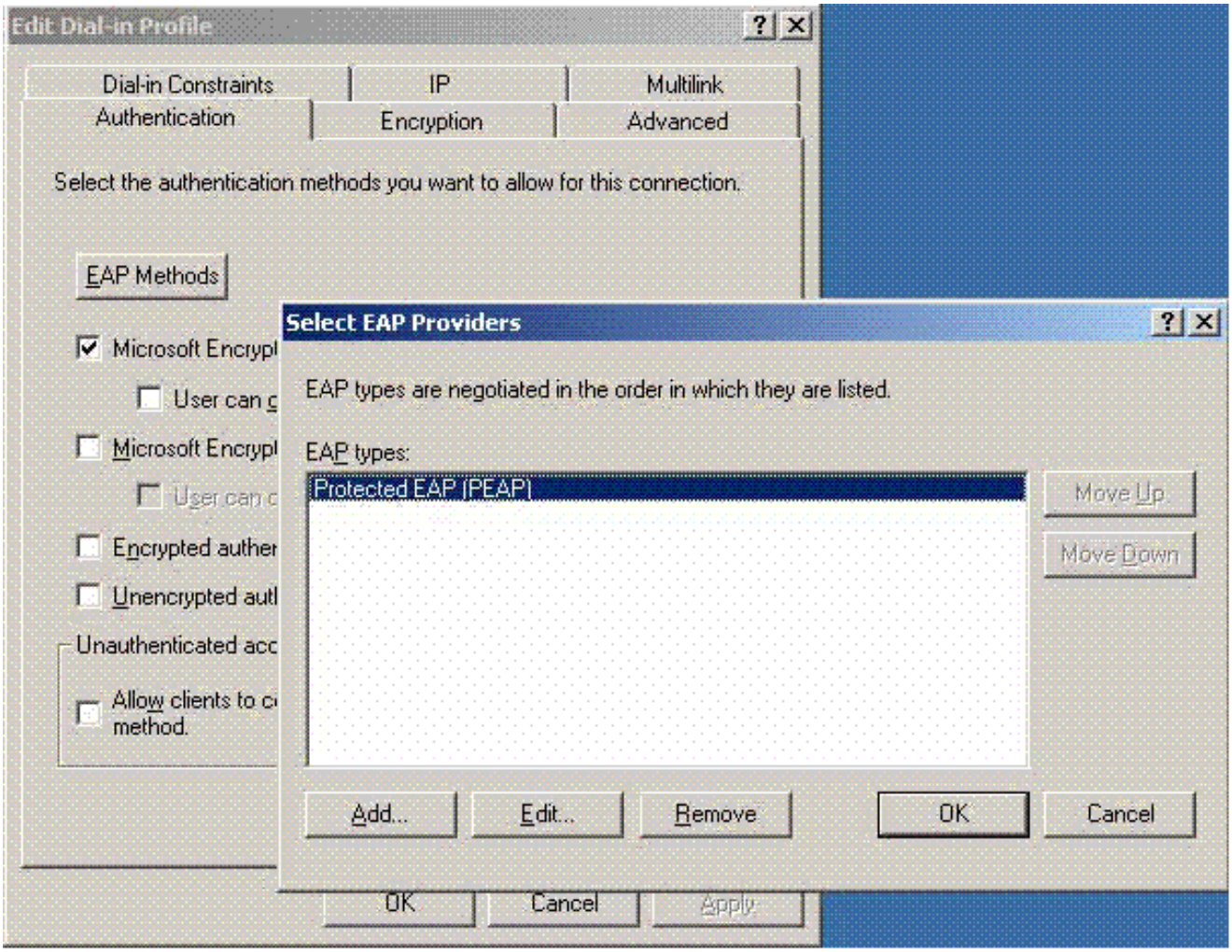
4. Éditez les propriétés de la stratégie d'accès à distance de contrôleur. Veillez à ajouter le type de Nas-port - Radio – IEEE 802.11
:



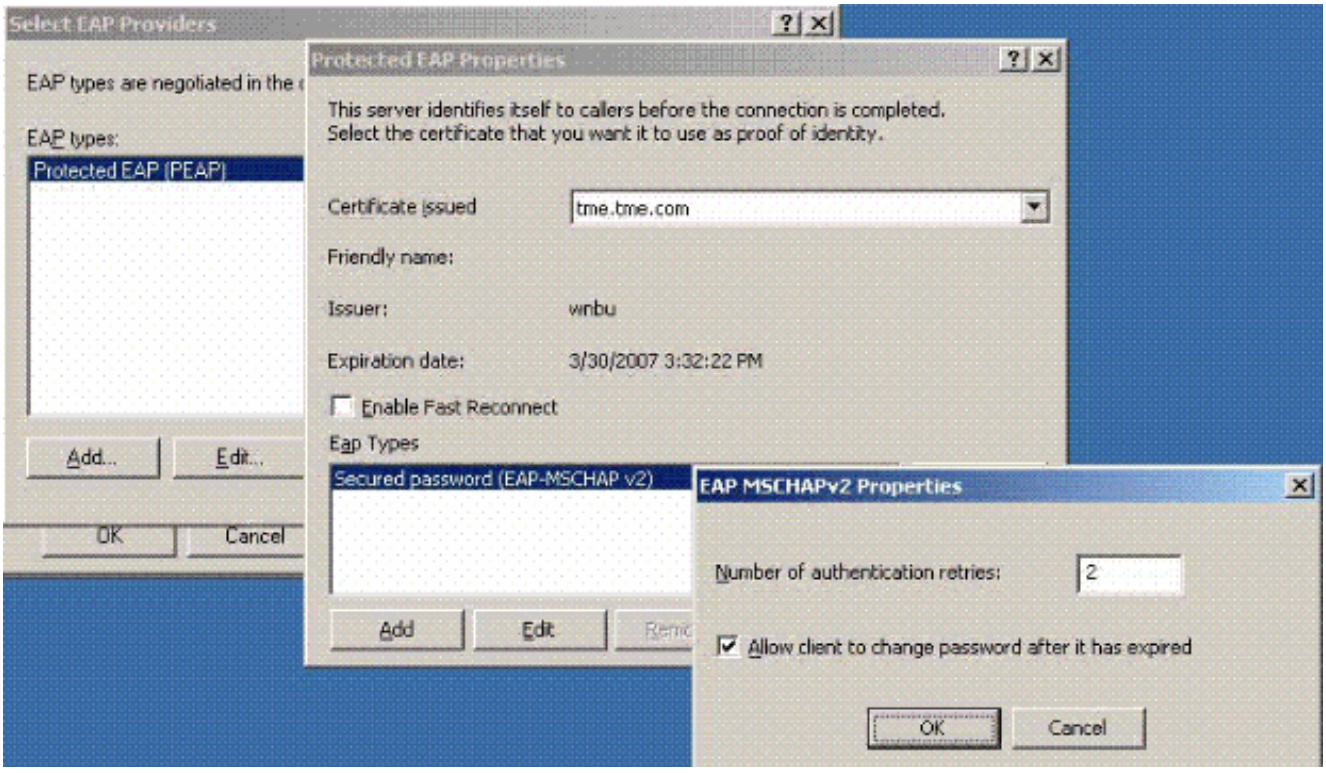
5. Cliquez sur Edit le **profil**, cliquez sur l'onglet d'**authentification**, et le contrôle MS-CHAP v2 pour l'authentification
:



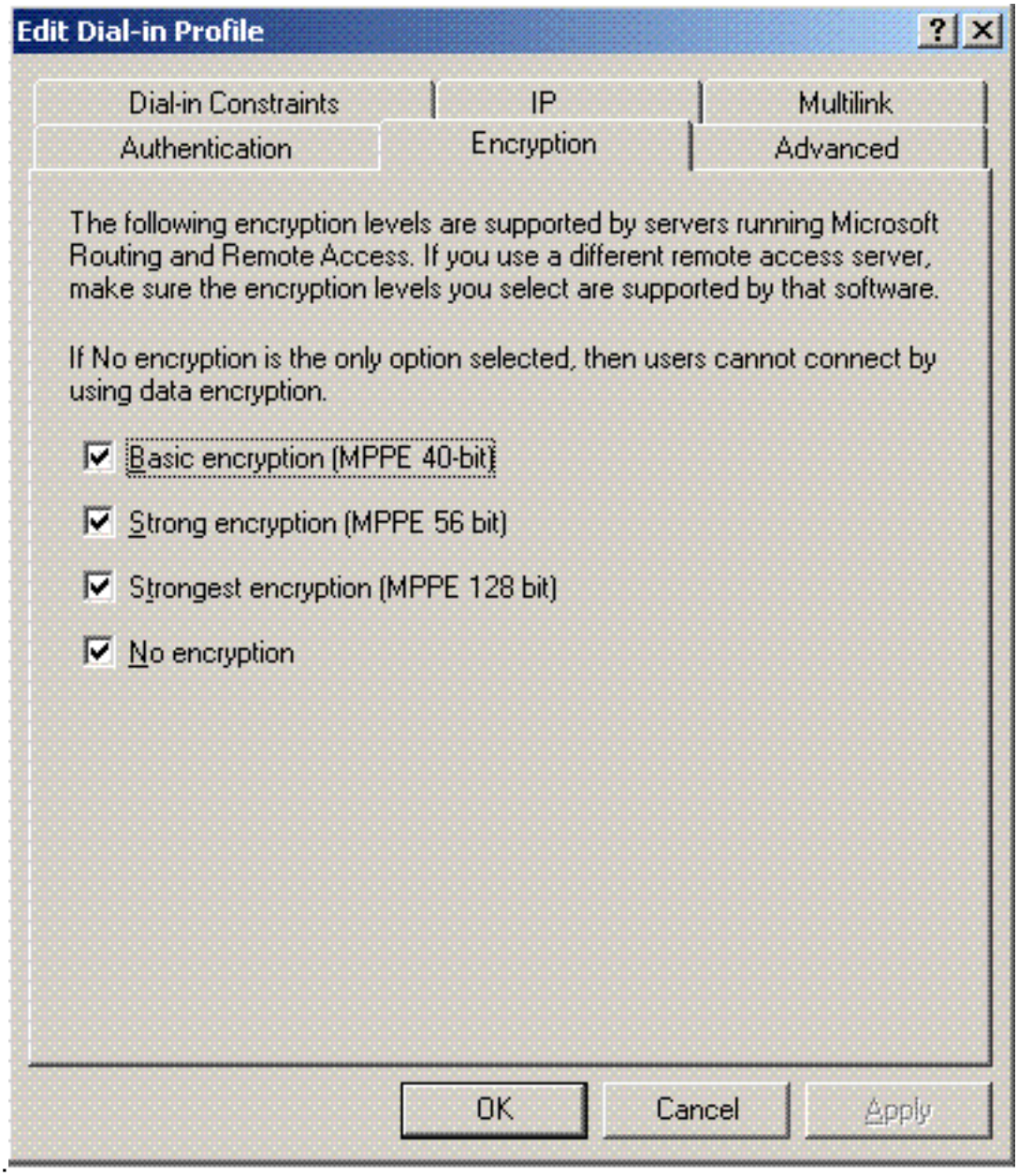
6. Cliquez sur les **méthodes d'EAP**, sélectionnez les fournisseurs d'EAP, et ajoutez le PEAP comme type d'EAP
   :



7. Cliquez sur Edit sur des fournisseurs d'EAP Select et choisissez du menu de traction vers le bas que le serveur a associé avec vos comptes utilisateurs de Répertoire actif et CA (par exemple tme.tme.com). Ajoutez le type MSCHAP v2 d'EAP
:

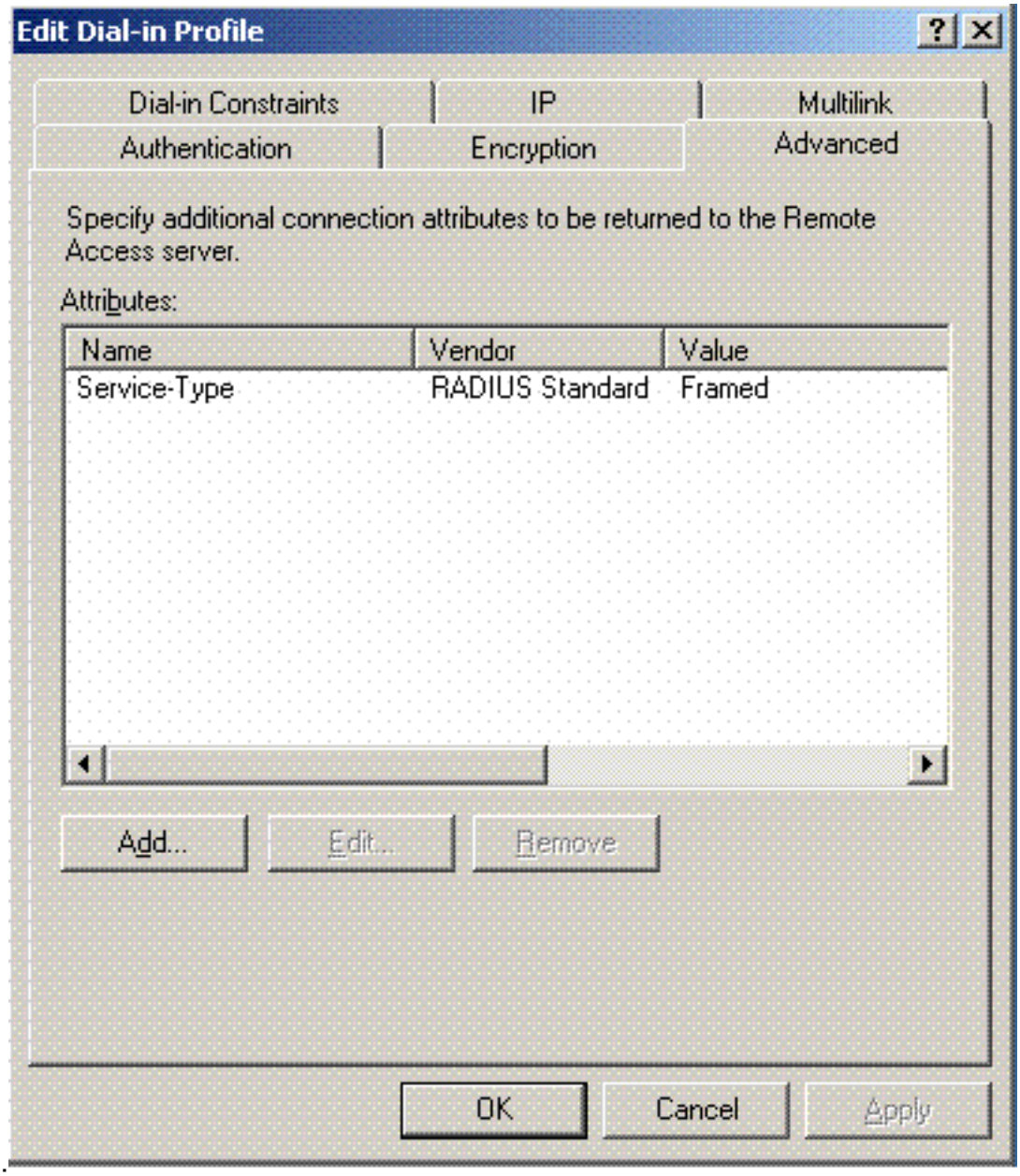


8. Cliquez sur l'onglet de **cryptage**, et vérifiez tous les types de cryptage pour l'Accès à distance



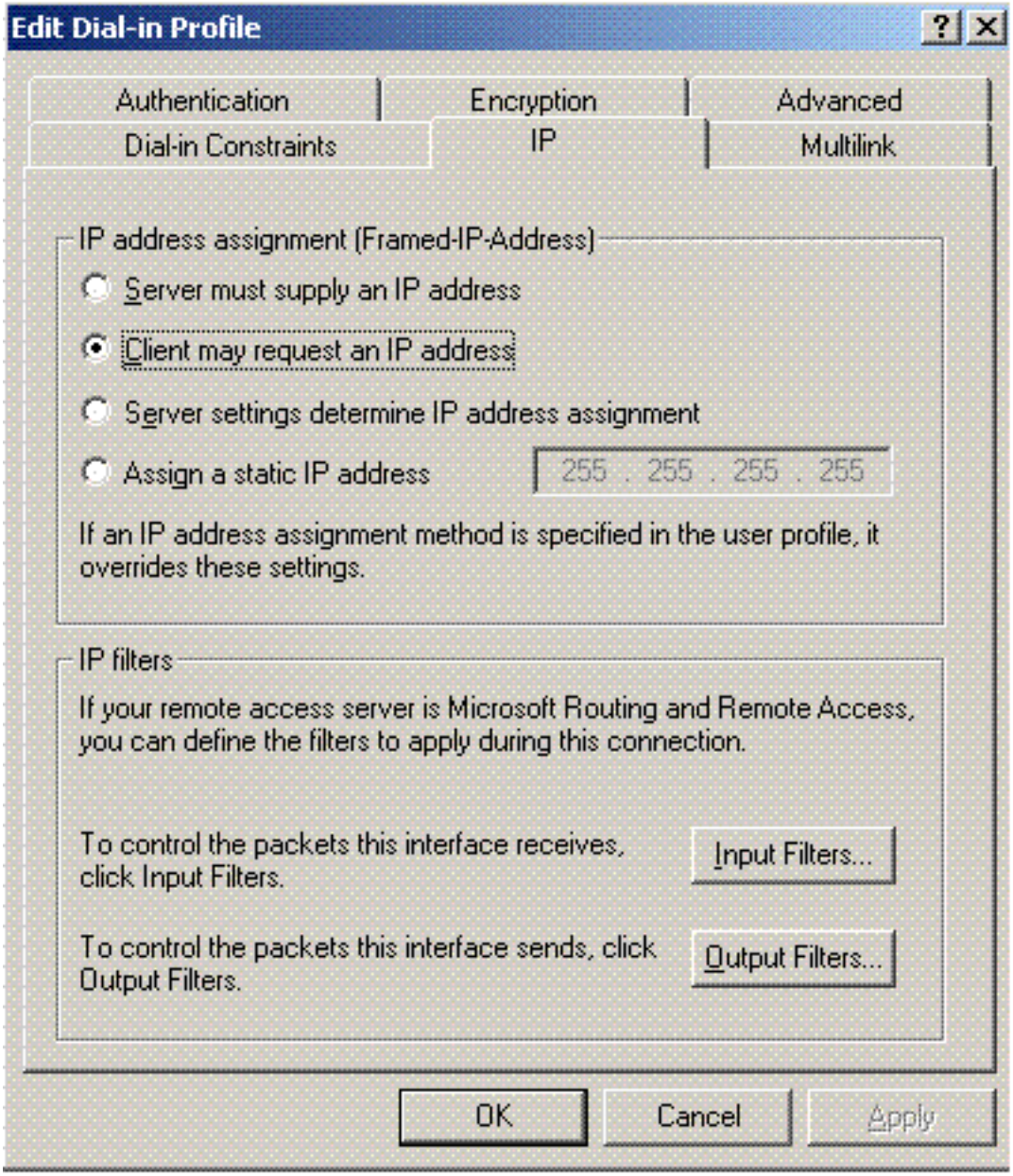
:

9. Cliquez sur l'**onglet Avancé**, et ajoutez le RADIUS Standard/vue comme type de service



:

10. Cliquez sur l'onglet **IP**, et le **client de** contrôle **peut demander une adresse IP**. Ceci suppose que vous avez le DHCP activé sur un commutateur ou un

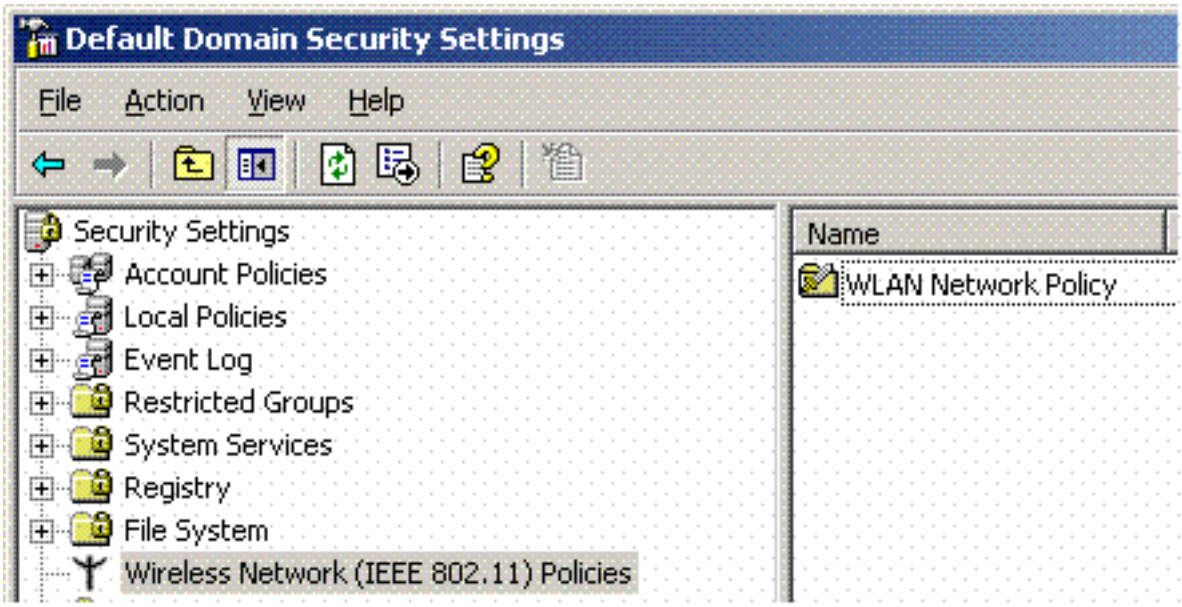


WinServer.

Paramètres de sécurité de domaine de Microsoft Windows 2003

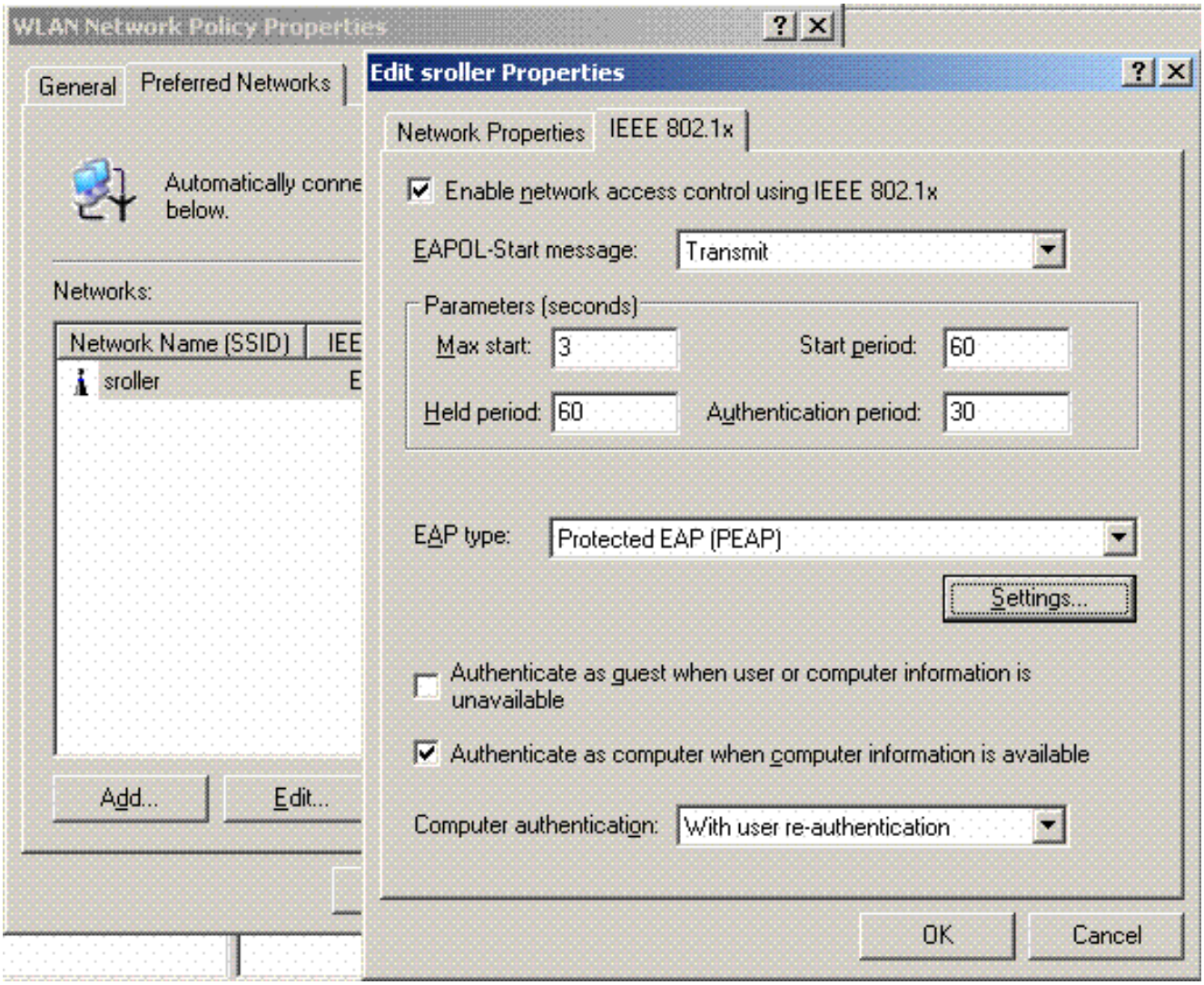
Terminez-vous ces étapes afin de configurer Windows 2003 paramètres de sécurité de domaine :

1. Lancez le gestionnaire par défaut de paramètres de sécurité de domaine, et créez une nouvelle stratégie de sécurité pour des stratégies de réseau sans fil (IEEE



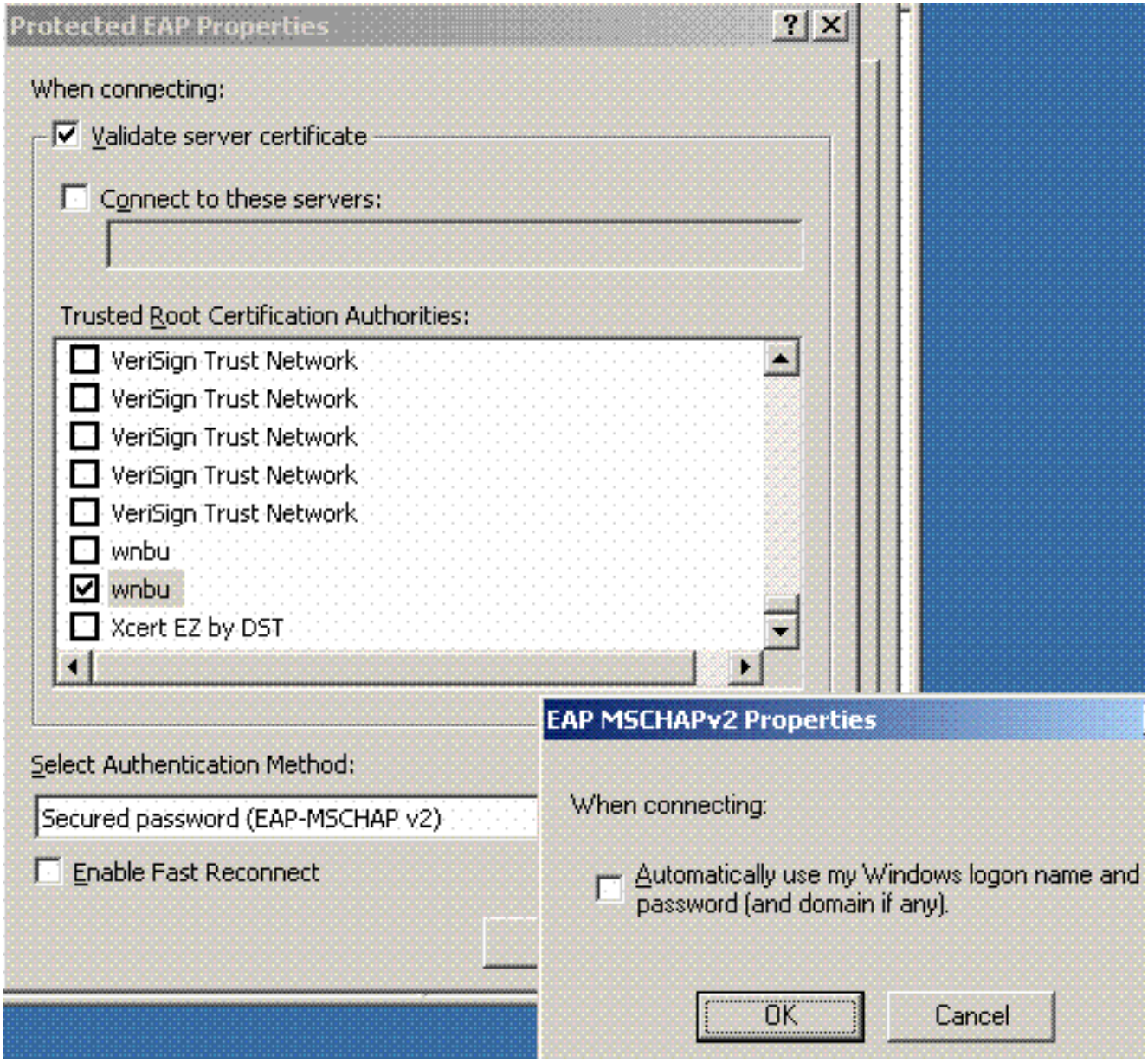
802.11).

2. La stratégie Properties de réseau WLAN ouvert, et le clic **ont préféré des réseaux**. Ajoutez un nouveau WLAN préféré et introduisez le nom de votre WLAN SSID, tel que la `radio`. Double-cliquer ce nouveau réseau préféré, et cliquez sur le **802.1x** tableau d'**IEEE** choisissent le PEAP comme type d'EAP
:

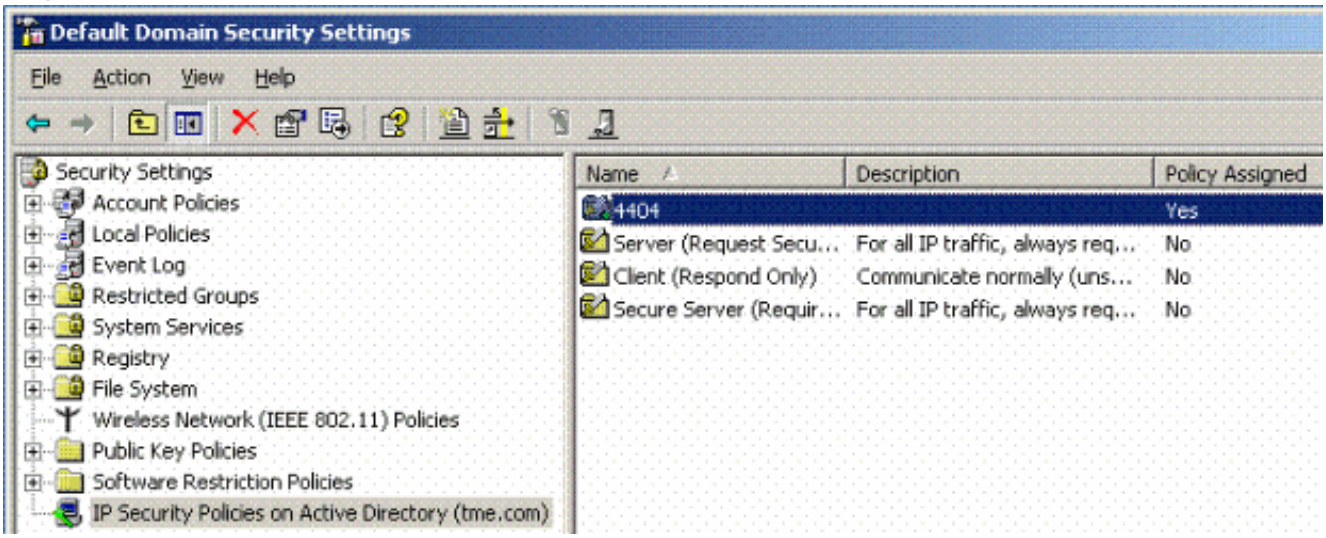


3. Cliquez sur les **configurations PEAP**, le contrôle **valident le certificat de serveur**, et sélectionnent le CERT de confiance de racine installé sur l'autorité de certification. Afin de tester, décochez le CHAP de MS que la case v2 pour automatiquement utilisent ma

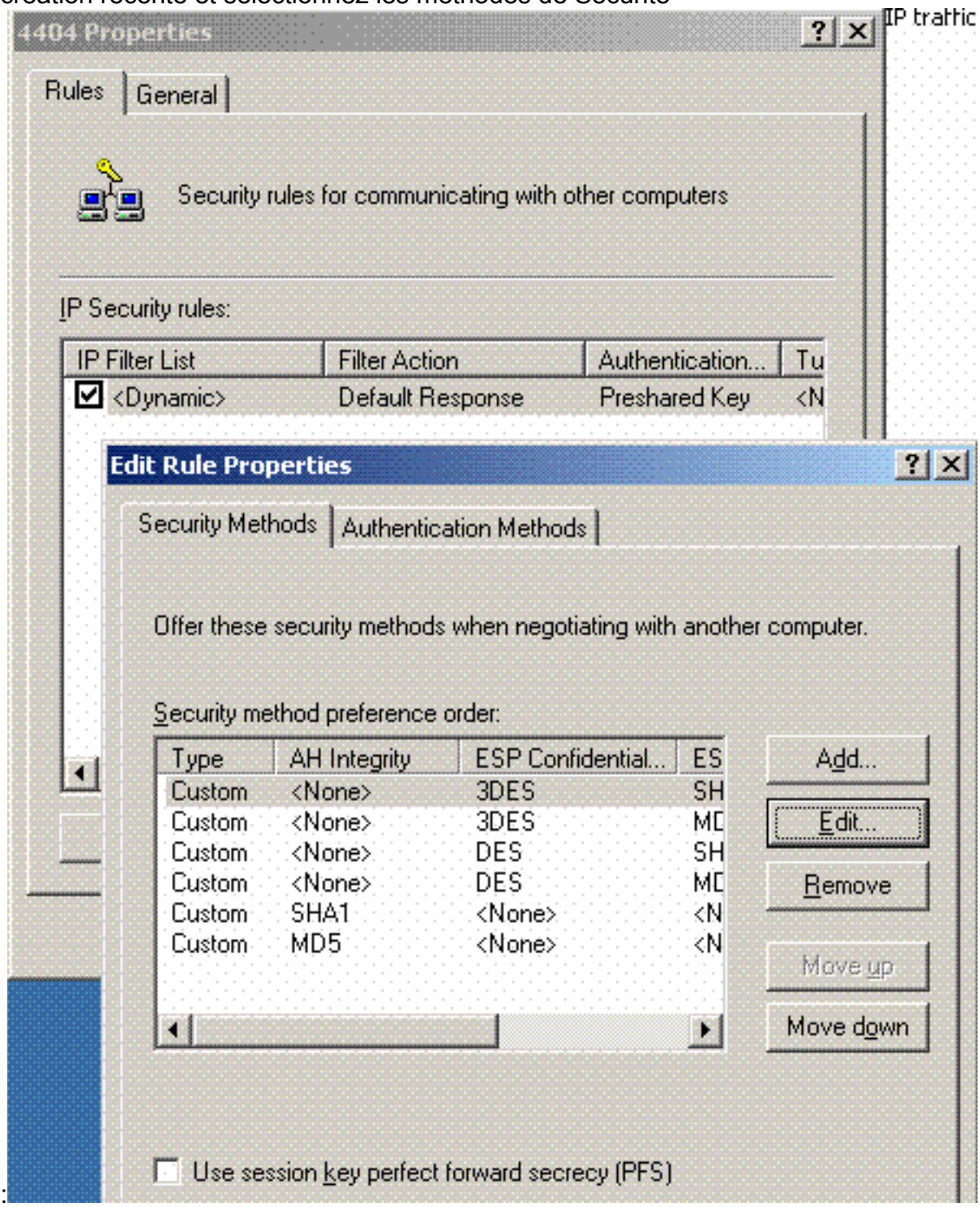
procédure de connexion et mot de passe de Windows.



4. Dans la fenêtre par défaut de gestionnaire de paramètres de sécurité de domaine de Windows 2003, créez des autres nouvelles stratégies de sécurité IP sur la stratégie de Répertoire actif, telle que **4404**.

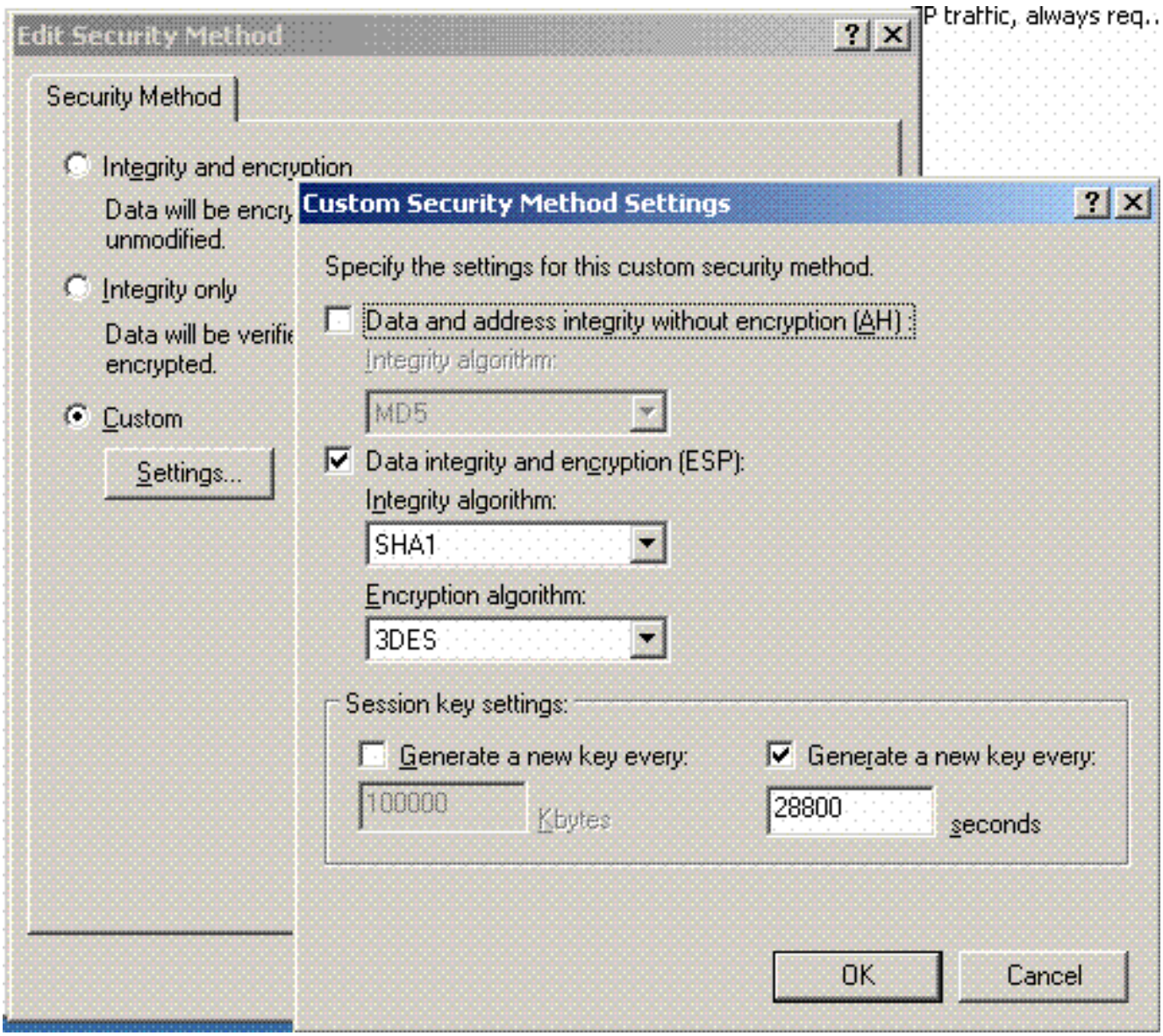


5. Éditez les nouvelles 4404 propriétés de stratégie, et cliquez sur les **règles que** tableau ajoutent une nouvelle règle de filtrage - liste de filet IP (dynamique) ; Action de filtre (réponse par défaut) ; Authentification (PSK) ; Tunnel (aucun). Double-cliquer la règle de filtrage de création récente et sélectionnez les méthodes de Sécurité

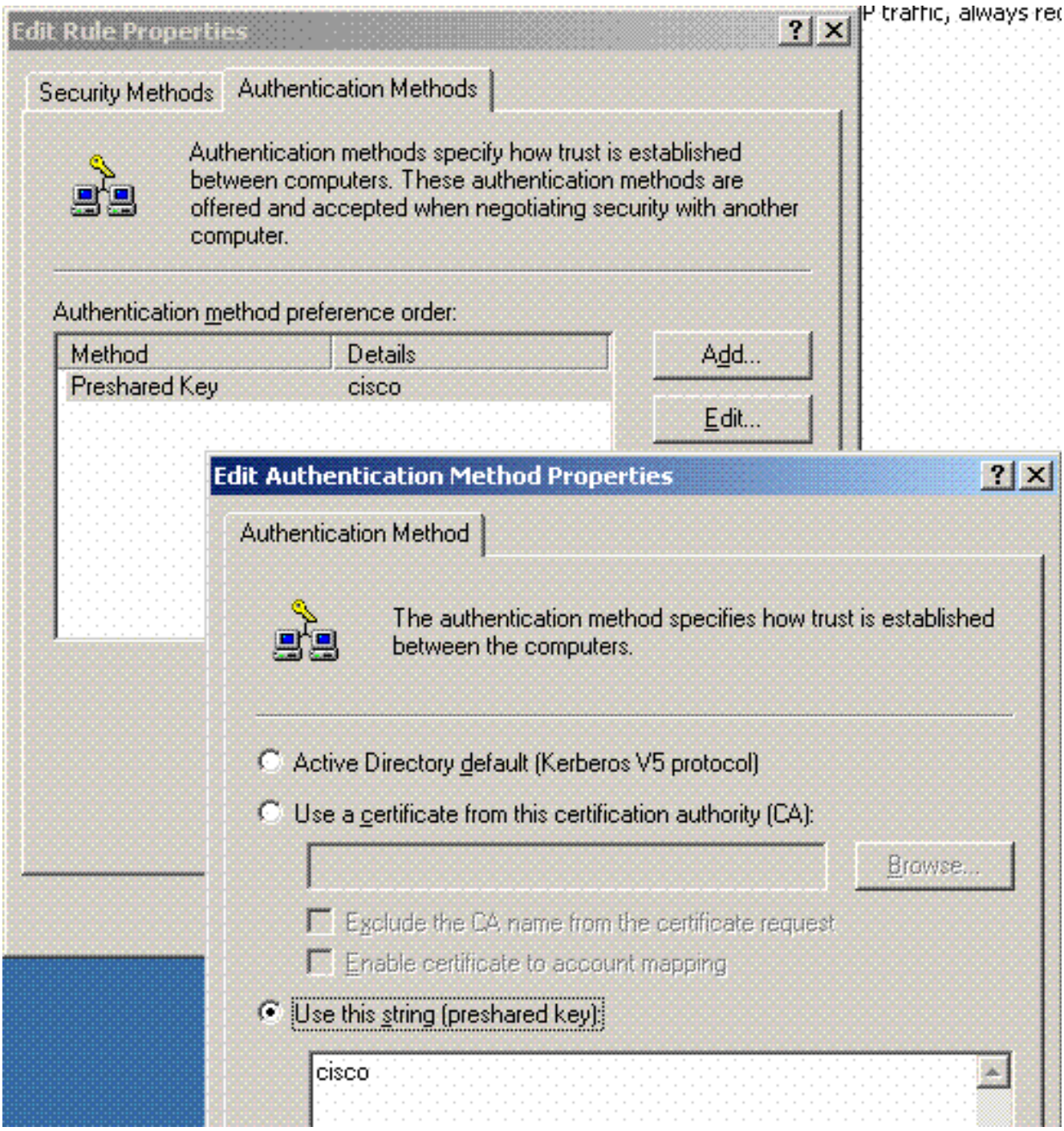


:

6. Cliquez sur Edit la **méthode de Sécurité**, et cliquez sur la case d'option de **paramètres personnalisés**. Choisissez ces configurations.**Remarque:** Ces configurations doivent apparier les paramètres de sécurité de RADIUS IPSec de contrôleur.



7. Cliquez sur l'onglet de **méthode d'authentification** selon la règle Properties d'éditer. Entrez dans la même chose le secret partagé que vous avez précédemment écrit sur la configuration RADIUS de
contrôleur.



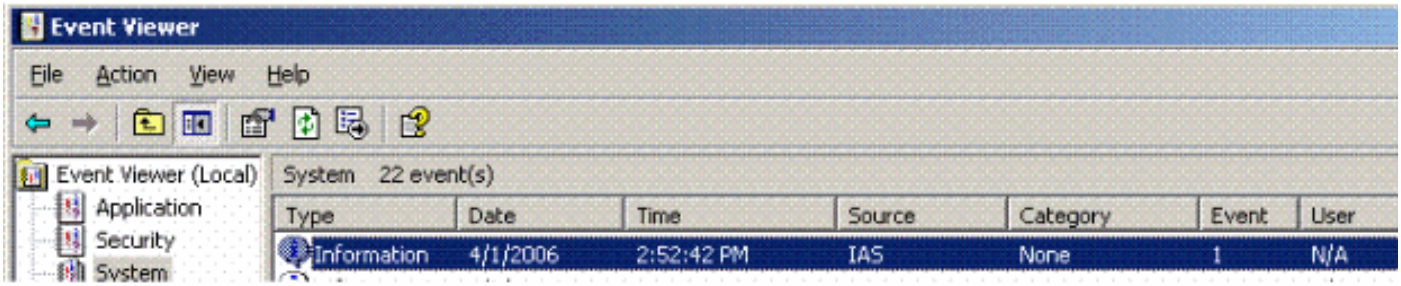
En ce moment, toutes les configurations pour le contrôleur, IAS et paramètres de sécurité de domaine sont terminés. Sauvegardez toutes les configurations sur le contrôleur et WinServer et redémarrez tous les ordinateurs. Sur le client WLAN qui est utilisé pour tester, installez le CERT de racine et le configurez pour WPA2/PEAP. Après que le CERT de racine soit installé sur le client, redémarrez la machine cliente. Après tout les ordinateurs redémarrent, connectent le client au WLAN et capturent ces événements de log.

Remarque: Une connexion client est exigée afin d'installer la connexion d'IPSec entre le contrôleur et le WinServer RADIUS.

Windows 2003 événements de log système

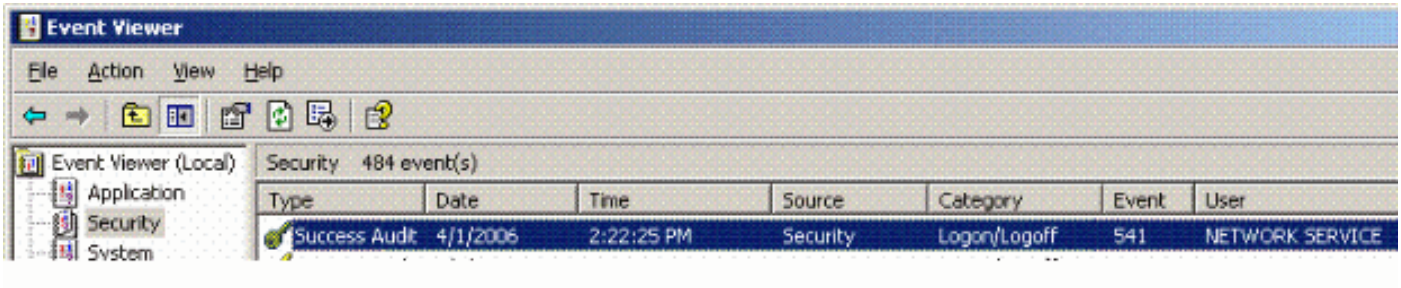
Une connexion réussie de client WLAN configurée pour WPA2/PEAP avec IPSec RADIUS activé génère cet événement de système sur le WinServer :

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)
```

Une connexion réussie de RADIUS IPSec de <> de contrôleur génère cet événement de Sécurité sur les 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
```

Exemple Sans fil de debug de succès de RADIUS IPSec de contrôleur LAN

Vous pouvez employer l'**enable d'ikemsg de debug pm de** commande de débogage sur le contrôleur afin de vérifier cette configuration. Voici un exemple.

```
(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
```

Capture d'Ethreal

Voici une capture d'Ethreal témoin.

```
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
```

Informations connexes

- Guide de configuration du contrôleur LAN sans fil Cisco, version 5.2
- Support et documentation techniques - Cisco Systems