Configuration de l'initiation VPN automatique sur un client VPN Cisco dans un environnement réseau local sans fil

Contenu

Introduction
Conditions préalables
Conventions
Conditions requises
Composants utilisés
Configurez
Diagramme du réseau
Configurations
Vérifiez
Vérifiez la configuration d'Automatique-initiation du numéroteur VPN
Vérifiez la caractéristique d'Automatique-initiation dans l'environnement WLAN
Vérifiez le journal d'événements de client vpn
Vérifiez un état différent d'Automatique-initiation
Informations connexes

Introduction

Ce document décrit comment configurer le Client VPN Cisco pour initier automatiquement des connexions VPN d'IPSec aux concentrateurs de Cisco VPN 3000 dans de câble/à environnement Sans fil du RÉSEAU LOCAL (WLAN).

Dans l'environnement WLAN, le client sans fil s'associe d'abord à un point d'accès sans fil (AP). Basé sur la plage d'adresses IP qu'elle reçoit de la connexion Sans fil, le client vpn installé sur la radio lance automatiquement une demande de connexion VPN au concentrateur correspondant VPN sur le site. La connexion VPN d'IPSec est alors utilisée afin de sécuriser le trafic de la radio 802.11x. Sans établissement réussi de la connexion VPN de Cisco, les clients sans fil n'ont aucun accès aux ressources de réseau.

Cette configuration d'échantillon affiche que la configuration du client vpn activait la caractéristique d'autoinitiation.

Conditions préalables

Conventions

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

Conditions requises

Avant que vous tentiez cette configuration, assurez-vous que vous êtes au courant de ces concepts :

- Comprenez comment installer et configurer le concentrateur de Client VPN Cisco et de Cisco VPN 3000 afin d'établir un tunnel VPN d'IPSec
- Comprenez les configurations liées aux réseaux locaux Sans fil

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version 4.x de Client VPN Cisco
- Version 3.6 de concentrateur de Cisco VPN 3000
- Point d'accès de Gamme Cisco Aironet 340
- Adaptateur LAN sans fil de Gamme Cisco Aironet 350 (version 5.0.1)

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.

Remarque: Dans cet exemple, le Cisco Network Registrar est utilisé pendant qu'un serveur du protocole DHCP (DHCP) afin de fournir des adresses IP aux clients sans fil et aux clients vpn.

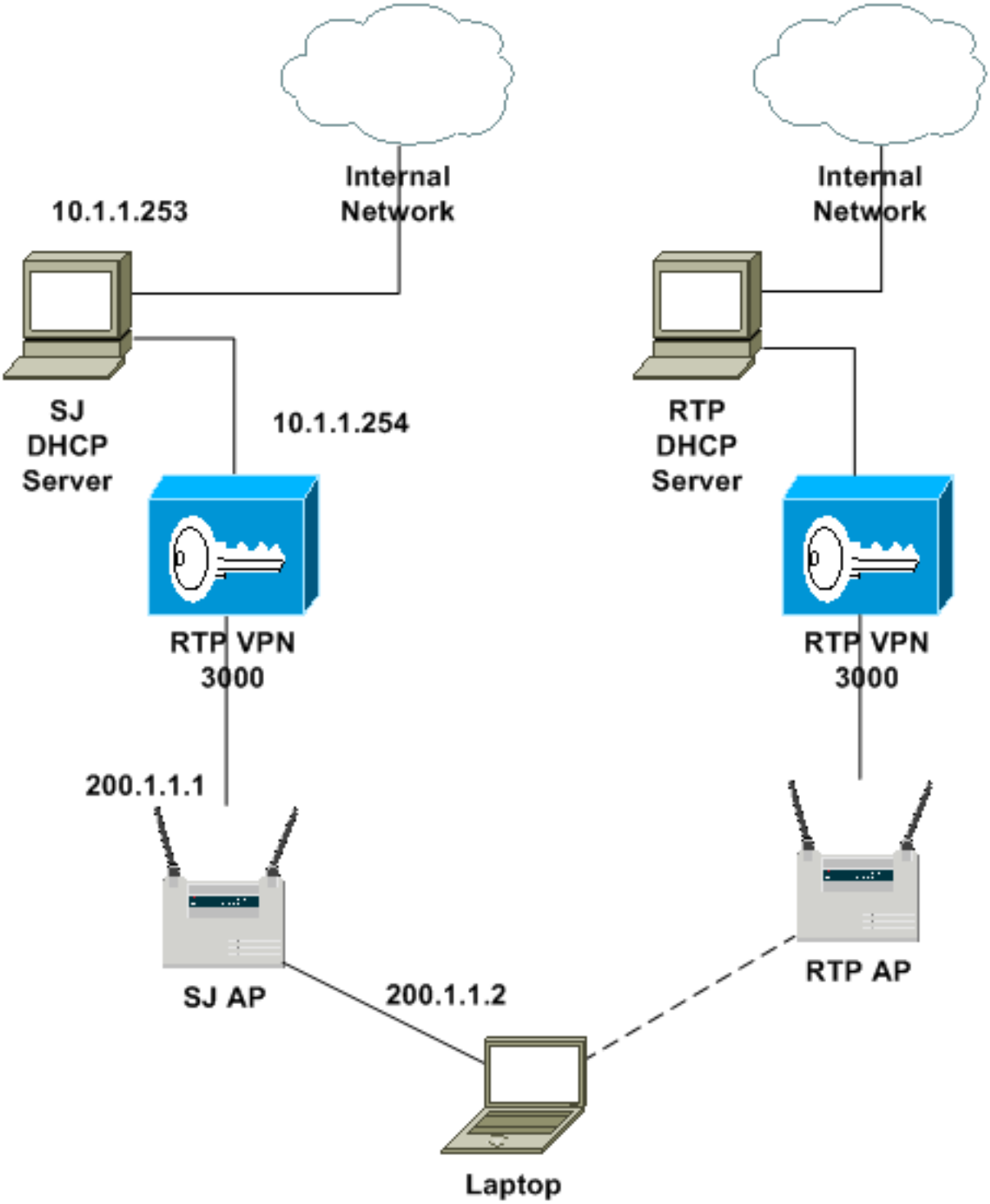
Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Remarque: Dans cette installation, le serveur DHCP SJ est utilisé afin de fournir des adresses IP aux connexions Sans fil et aux connexions VPN. Il fait définir deux plages d'adresses IP :

- Pour les connexions Sans fil, les utilisateurs de sans fil reçoivent une adresse IP dans la plage de 200.1.1.50 à 200.1.1.250.
- Pour des connexions VPN, les clients vpn reçoivent une adresse IP dans la plage de 50.1.1.1 à 50.1.1.254.

Configurations

Dans cet exemple, basé sur dans lequel le site l'utilisateur erre, le client sans fil lance automatiquement l'un ou l'autre une des deux connexions VPN (à savoir SJWireless ou RTPWireless) qui sont prédéfinies dans le numéroteur VPN. Plus spécifiquement, si l'utilisateur de

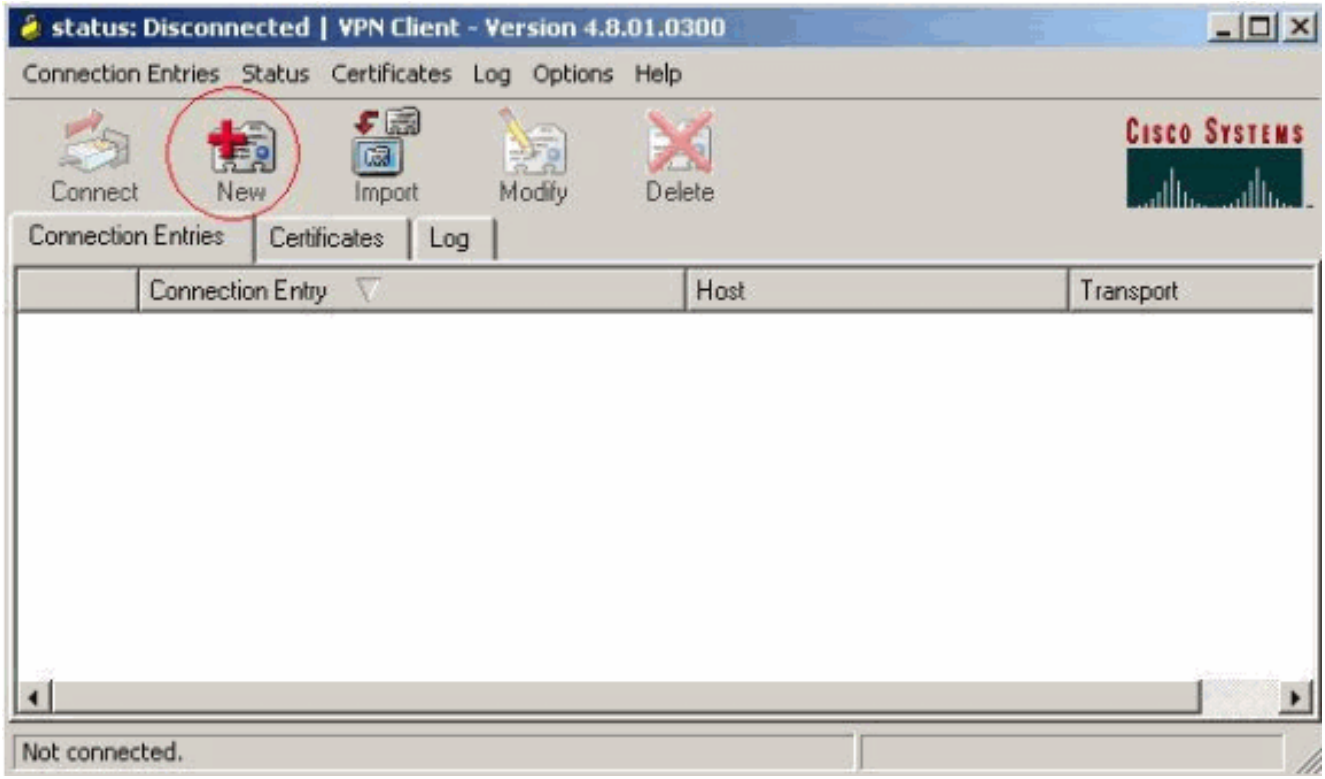
sans fil obtient une adresse IP de l'ordre de 200.1.1.0/24 de l'association Sans fil au SJ AP, il lance la connexion de SJWireless du numéroteur VPN. S'il obtient une adresse IP de l'ordre de 150.1.1.0/24 de l'association Sans fil au RTP AP, il lance la connexion de RTPWireless du numéroteur VPN.

Dans cette section, les connexions VPN sont d'abord configurées sous le numéroteur VPN, puis le fichier vpnclient.ini est édité pour ajouter la configuration d'autoinitiation. Une fois que ces étapes sont terminées sur un client vpn, les profils générés VPN (fichiers .pcf) et vpnclient.ini configuré peuvent être empaquetés, avec l'image de client vpn, afin de distribuer aux utilisateurs finaux. Le lancement de connexion VPN est transparent aux utilisateurs finaux après l'installation de client vpn.

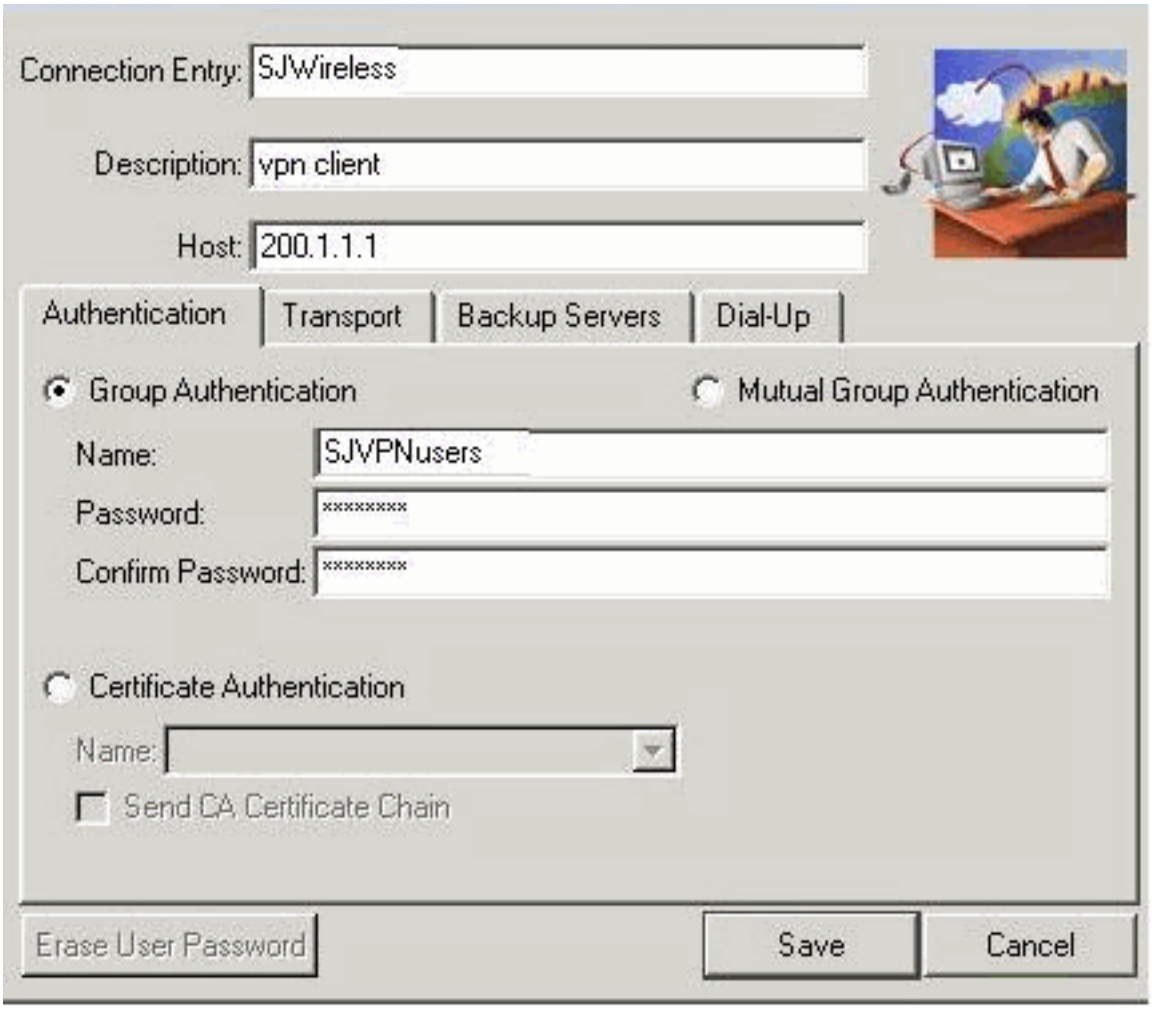
Configuration de numéroteur VPN

Terminez-vous ces étapes de configuration :

1. Choisissez le début > les programmes > le client vpn de Cisco Systems > le client vpn. Cliquez sur New afin de lancer la nouvelle fenêtre d'entrée de connexion VPN de création.



2. Entrez le nom de l'entrée de connexion avec une description. Écrivez l'adresse IP extérieure du concentrateur VPN dans la case d'hôte. Entrez alors le nom et le mot de passe de groupe VPN, et cliquez sur la **sauvegarde**.



3. Répétez les étapes 1 et 2 afin de créer une autre connexion VPN avec le nom **RTPWireless du** numéroteur de Cisco VPN.Quand le deuxième processus de configuration est complet, deux profils de connexion VPN ont nommé SJWireless.pcf et RTPWireless.pcf sont générés sur le PC client.
4. Terminez-vous ces étapes afin d'éditer le fichier du par défaut vpnclient.ini avéré sur le PC client afin d'activer la caractéristique d'autoinitiation :Activez la caractéristique d'autoinitiation avec le mot clé d'**AutoInitiationEnable** sous [la section de canalisation].Définissez l'**AutoInitiationList**. Chaque élément dans la liste correspond à une section, où le nom de la plage d'adresses IP de connexion VPN et de radio sont associés.Dans cet exemple, la connexion VPN de SJWireless correspond à 200.1.1.0/24 et la connexion de RTPWireless correspond à 150.1.1.0/24.Quand fait un pas a et b sont complets, le fichier vpnclient.ini ressemble à ceci :

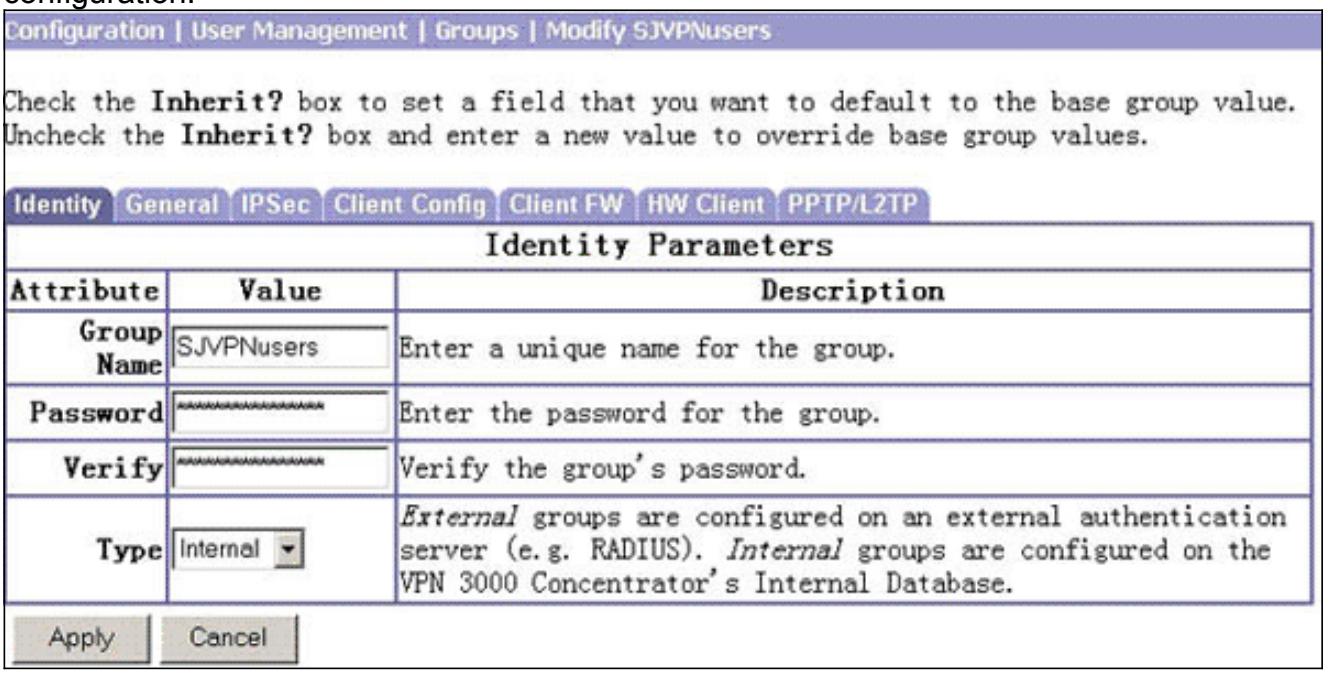
```
[LOG.CVPND]
LogLevel=1
[LOG.CERT]
LogLevel=3
[LOG.PPP]
LogLevel=2
[LOG.CM]
LogLevel=1
[LOG.IPSEC]
LogLevel=3
[main]
AutoInitiationEnable=1 AutoInitiationRetryInterval=3 AutoInitiationList=SJVPN,RTPVPN
EnableLog=1 [SJVPN] Network=200.1.1.0 Mask=255.255.255.0 ConnectionEntry=SJWireless
[RTPVPN] Network=150.1.1.0 Mask=255.255.255.0 ConnectionEntry=RTPWireless RunAtLogon=0
EnableLog=1 XAuthHandler=ipsxauth.exe IsNoTrayIcon=0 StatefulFirewall=0 [LOG.DIALER]
LogLevel=2 [LOG.IKE] LogLevel=3 [LOG.XAUTH] LogLevel=3 [LOG.CLI] LogLevel=1 [LOG.FIREWALL]
LogLevel=1
```

5. Après qu'étapes 1 - 3 sont complètes sur un client vpn, le vpnclient.ini et les profils de connexion VPN (.pcf) peuvent être collectés et distribués aux utilisateurs finaux dans le module d'installation. Référez-vous au guide de l'administrateur VPNCLIENT, version 3.6 pour les informations sur la façon dont préconfigurer les clients VPN pour des utilisateurs distants.

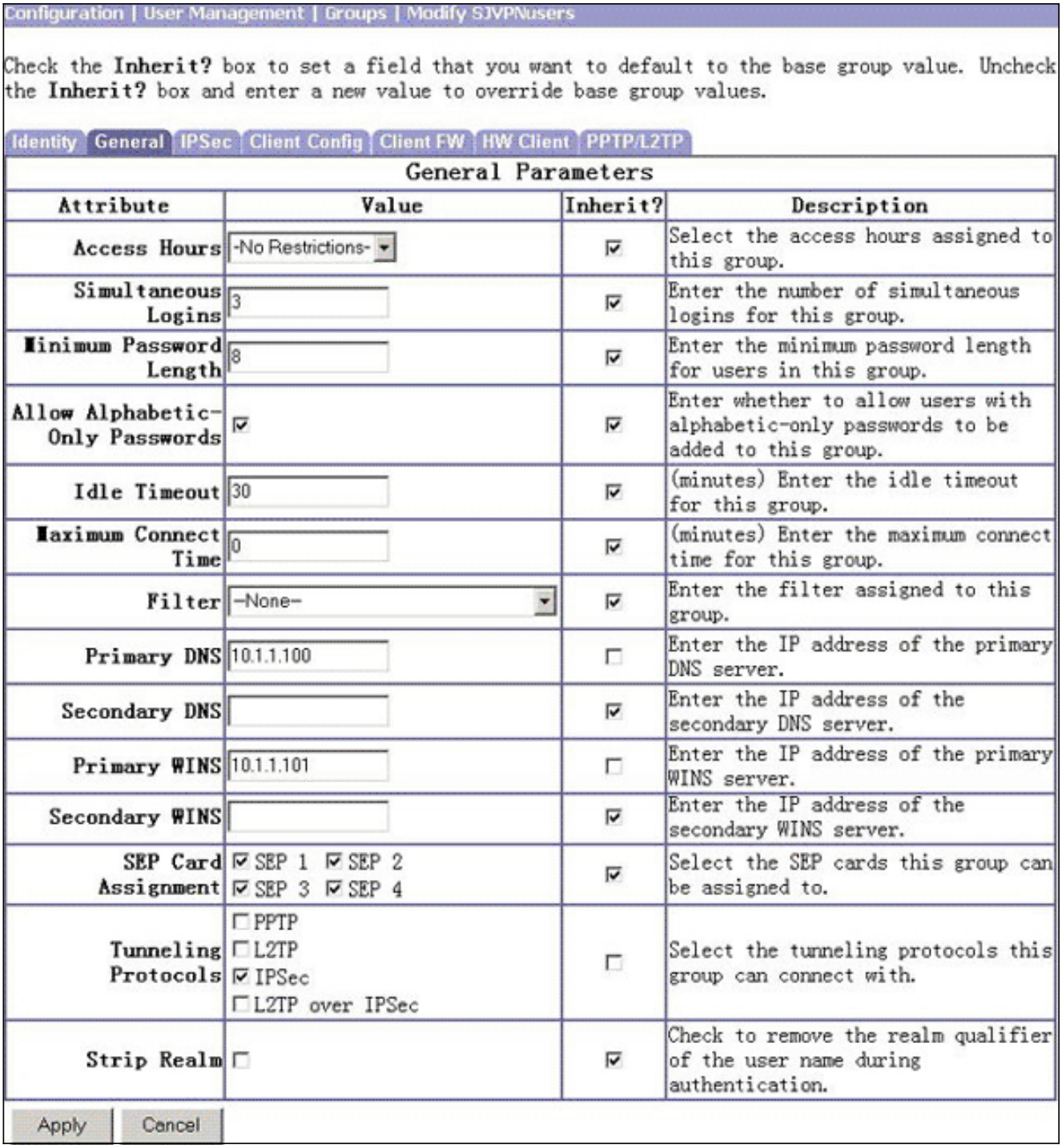
Configuration du concentrateur de Cisco VPN 3000

Terminez-vous ces étapes de configuration :

1. Sur des concentrateurs VPN 3000, les groupes VPN doivent être configurés pour établir une connexion d'IPSec avec le client vpn. Dans l'exemple, les utilisateurs de sans fil peuvent se connecter à différents concentrateurs VPN basés sur le site dans lequel ils errent. Ici, seulement les importantes tâches de configuration sur le concentrateur SJ VPN sont mises en valeur. Un groupe VPN a appelé **SJVPNusers**, qui apparie le nom de groupe VPN sur le client, est créé.
2. Choisissez le **Configuration > User Management > Groups** et choisissez **SJVPNusers de la** liste en cours de groupe. Choisi **modifiez le groupe de l'**option d'actions si le groupe est déjà créé, ou **ajoutez le groupe** et puis **modifiez le groupe** si le groupe doit être créé.
3. Cliquez sur l'onglet d'identité.La fenêtre de paramètres d'identité apparaît. Vérifiez que l'information affichée dans cette fenêtre est correcte pour votre configuration.



4. Cliquez sur l'onglet Général et puis cochez la case d'**IPSec** pour l'attribut de protocoles de Tunnellisation.



Configuration | User Management | Groups | Modify SJVPNusers

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

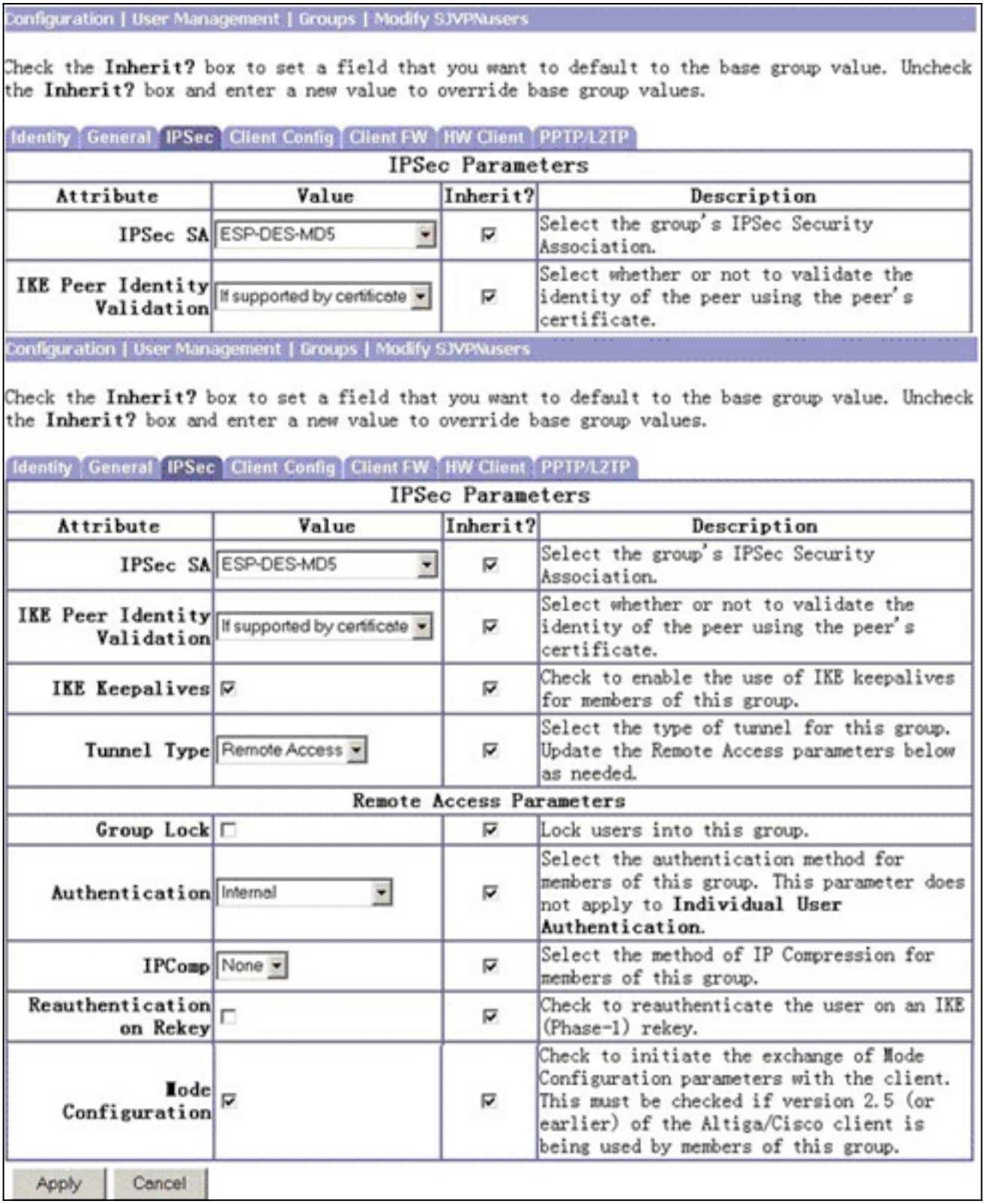
Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

General Parameters

Attribute	Value	Inherit?	Description
Access Hours	-No Restrictions-	☑	Select the access hours assigned to this group.
Simultaneous Logins	3	☑	Enter the number of simultaneous logins for this group.
Minimum Password Length	8	☑	Enter the minimum password length for users in this group.
Allow Alphabetic-Only Passwords	☑	☑	Enter whether to allow users with alphabetic-only passwords to be added to this group.
Idle Timeout	30	☑	(minutes) Enter the idle timeout for this group.
Maximum Connect Time	0	☑	(minutes) Enter the maximum connect time for this group.
Filter	-None-	☑	Enter the filter assigned to this group.
Primary DNS	10.1.1.100	☐	Enter the IP address of the primary DNS server.
Secondary DNS		☑	Enter the IP address of the secondary DNS server.
Primary WINS	10.1.1.101	☐	Enter the IP address of the primary WINS server.
Secondary WINS		☑	Enter the IP address of the secondary WINS server.
SEP Card Assignment	☑ SEP 1 ☑ SEP 2 ☑ SEP 3 ☑ SEP 4	☑	Select the SEP cards this group can be assigned to.
Tunneling Protocols	☐ PPTP ☐ L2TP ☑ IPSec ☐ L2TP over IPSec	☐	Select the tunneling protocols this group can connect with.
Strip Realm	☐	☑	Check to remove the realm qualifier of the user name during authentication.

Apply | Cancel

5. Cliquez sur l'onglet d'IPSec, puis spécifiez l'association de sécurité d'IPSec (SA) et l'attribut de méthode d'authentification avec les menus déroulants et les cases fournis.Dans ce cas, les utilisateurs VPN sont définis localement sur le concentrateur VPN 3000, ainsi la méthode d'authentification est
interne.


Configuration | User Management | Groups | Modify SJVPNusers

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

IPSec Parameters

Attribute	Value	Inherit?	Description
IPSec SA	ESP-DES-MD5	☑	Select the group's IPSec Security Association.
IKE Peer Identity Validation	If supported by certificate	☑	Select whether or not to validate the identity of the peer using the peer's certificate.

Configuration | User Management | Groups | Modify SJVPNusers

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

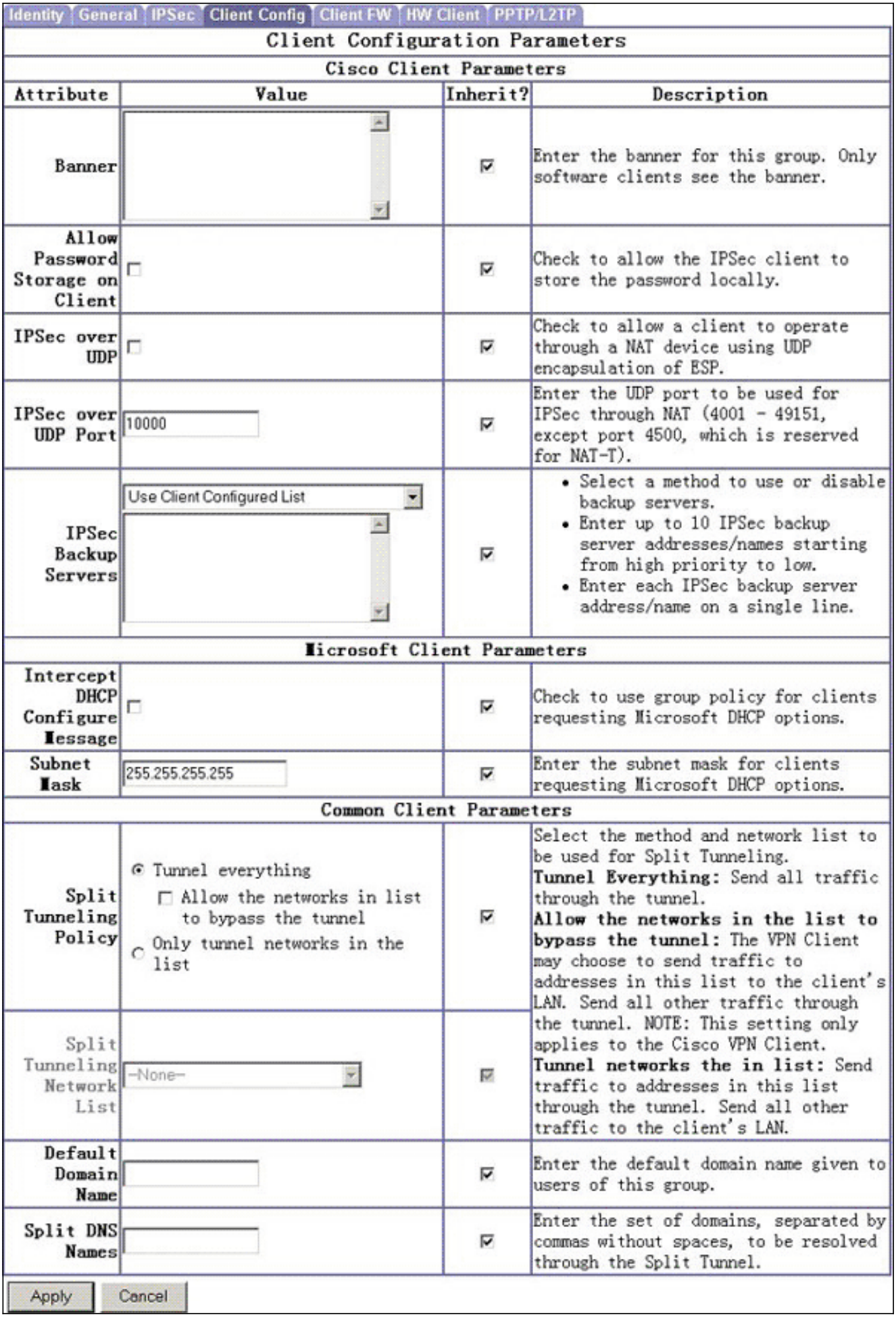
Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

IPSec Parameters

Attribute	Value	Inherit?	Description
IPSec SA	ESP-DES-MD5	☑	Select the group's IPSec Security Association.
IKE Peer Identity Validation	If supported by certificate	☑	Select whether or not to validate the identity of the peer using the peer's certificate.
IKE Keepalives	☑	☑	Check to enable the use of IKE keepalives for members of this group.
Tunnel Type	Remote Access	☑	Select the type of tunnel for this group. Update the Remote Access parameters below as needed.
Remote Access Parameters			
Group Lock	☐	☑	Lock users into this group.
Authentication	Internal	☑	Select the authentication method for members of this group. This parameter does not apply to **Individual User Authentication**.
IPComp	None	☑	Select the method of IP Compression for members of this group.
Reauthentication on Rekey	☐	☑	Check to reauthenticate the user on an IKE (Phase-1) rekey.
Mode Configuration	☑	☑	Check to initiate the exchange of Mode Configuration parameters with the client. This must be checked if version 2.5 (or earlier) of the Altiga/Cisco client is being used by members of this group.

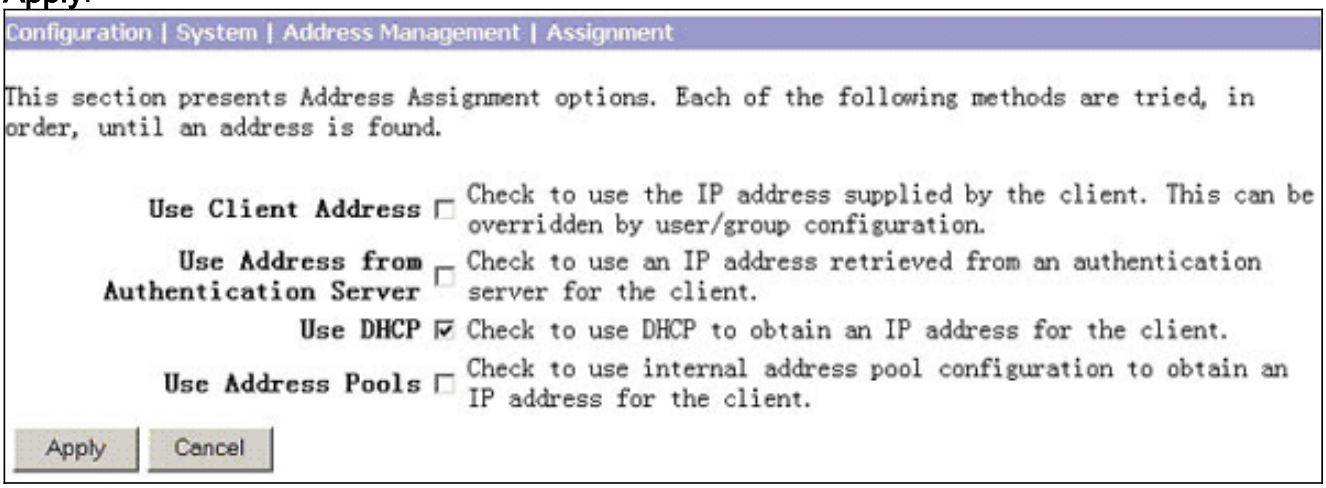
Apply | Cancel

6. Cliquez sur l'onglet de config de client, puis spécifiez les paramètres de configuration de mode sur la fenêtre de paramètres de configuration de client. Cliquez sur **Apply**.Dans ce cas, tout le trafic du client vpn est chiffré et envoyé au tunnel d'IPSec. Ceci est spécifié sous les paramètres communs de
client.

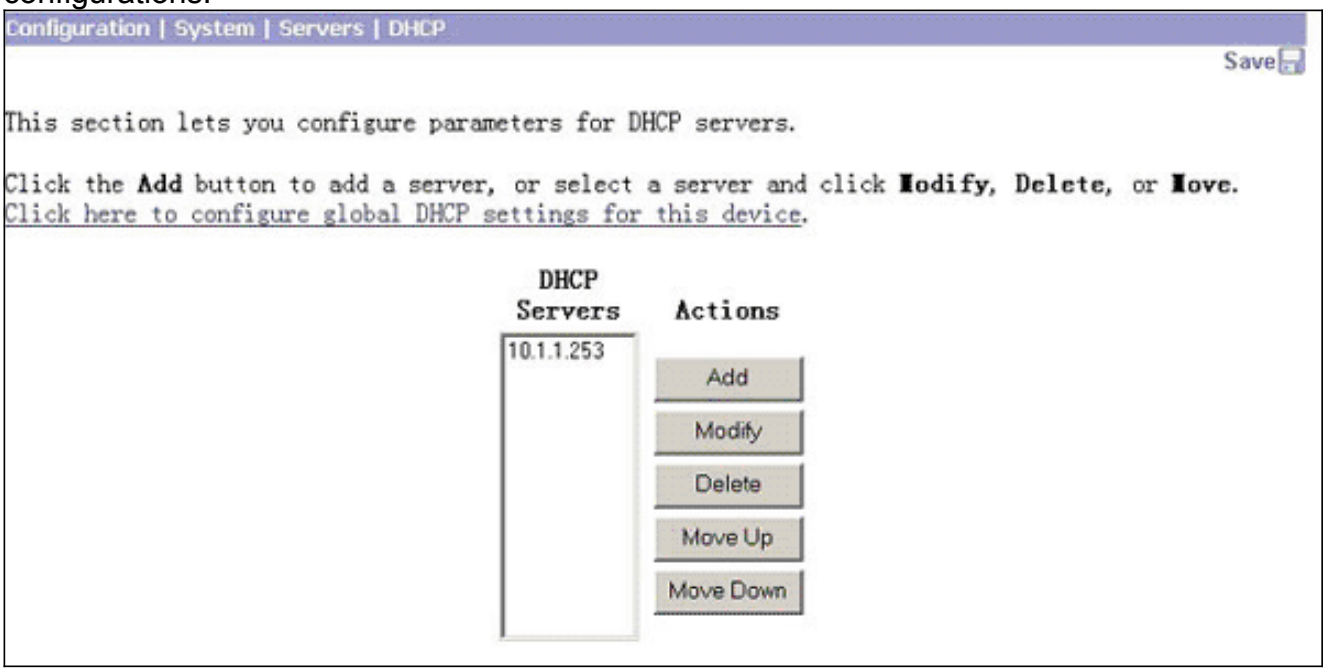


7. Choisissez la **configuration > le système > la gestion d'adresses > l'affectation**. De la fenêtre d'options d'affectation d'adresses, spécifiez la méthode d'affectation d'adresse IP avec les

cases à cocher fournies.Dans ce cas, le client vpn obtient une adresse IP d'un serveur DHCP pendant la négociation d'IKE, ainsi l'option DHCP d'utilisation est vérifiée. Cliquez sur **Apply**.



8. Employez la fenêtre de configuration du serveur DHCP afin d'installer les paramètres de serveur DHCP, et cliquez sur la **sauvegarde** afin de sauvegarder les configurations.



Comme mentionné, un serveur DHCP derrière le concentrateur VPN 3000 est utilisé pour les connexions Sans fil et les connexions VPN. Pour les connexions Sans fil, les servir de concentrateur de DHCP transmettent par relais l'agent pour transmettre par relais le message DHCP entre le point d'accès sans fil et le serveur DHCP.

Vérifiez

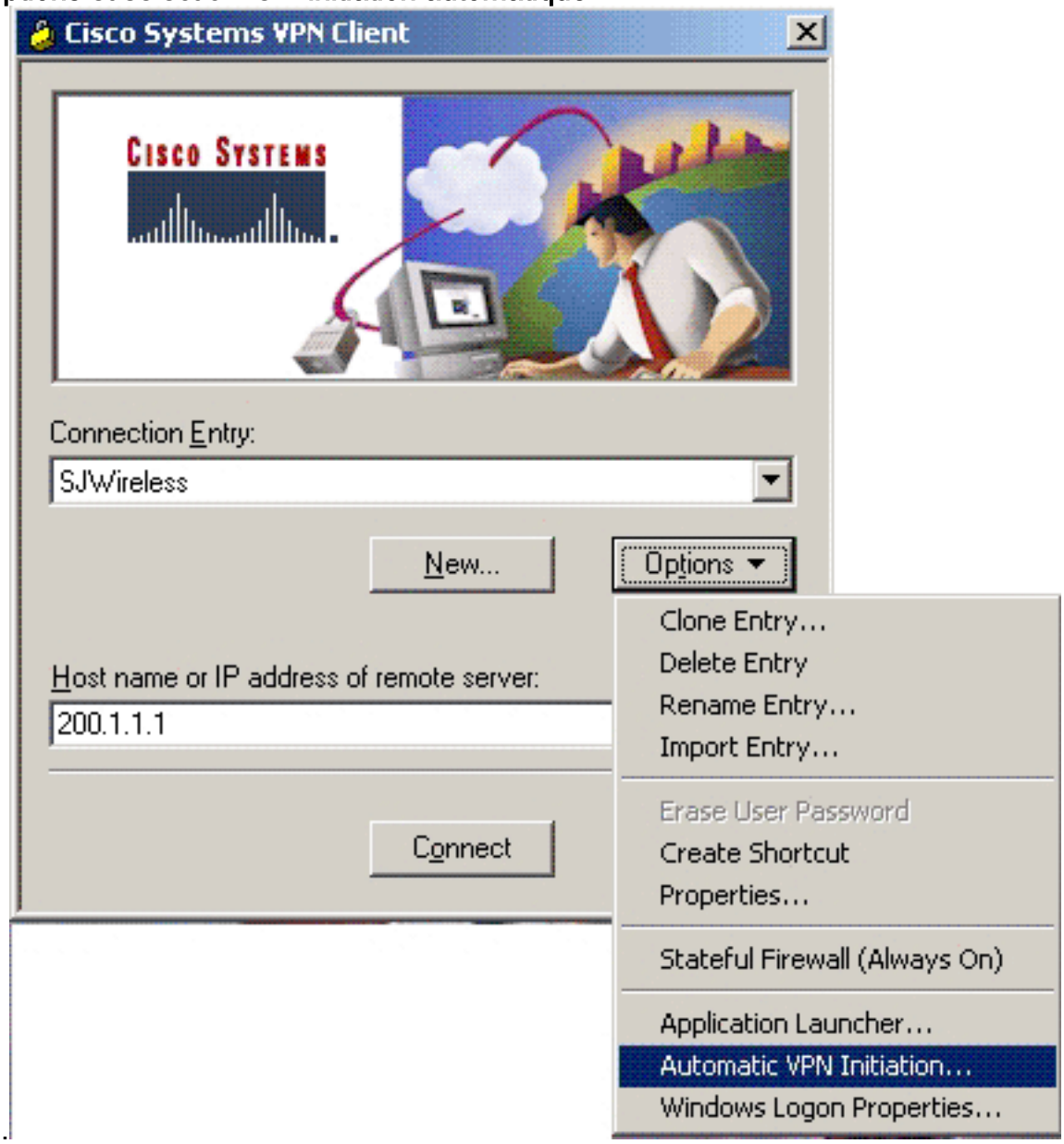
Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Vérifiez la configuration d'Automatique-initiation du numéroteur VPN

Terminez-vous ces étapes afin de vérifier la configuration d'autoinitiation du numéroteur VPN :

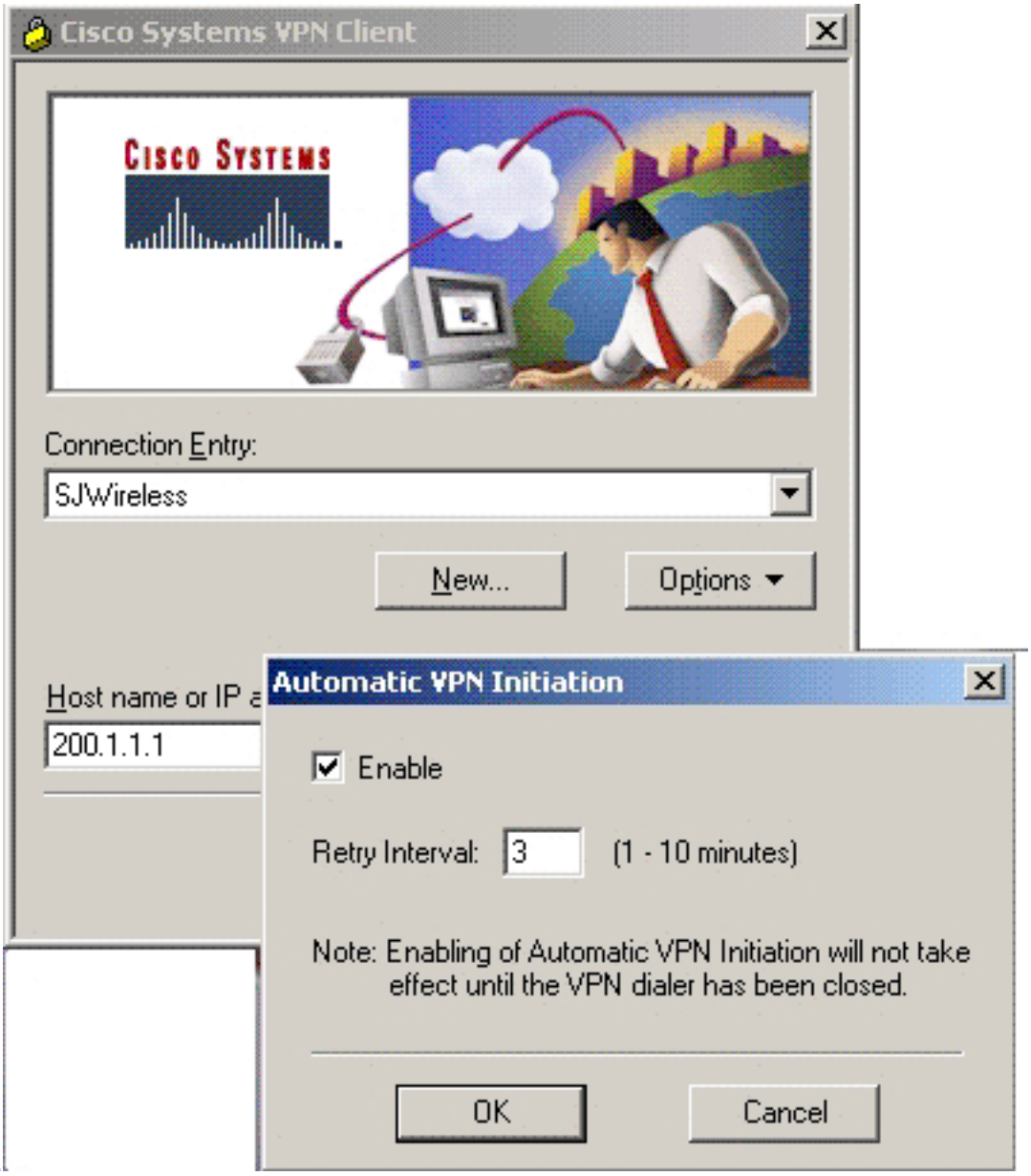
1. De la fenêtre de numéroteur de Cisco VPN sur le poste de travail de client vpn, cliquez sur

les **options** et sélectionnez l'**initiation automatique**



VPN.

2. Sur la fenêtre automatique d'initiation VPN, vérifiez que la case d'enable est cochée. S'il n'est pas, cochez-le. Cliquez sur OK afin de fermer la

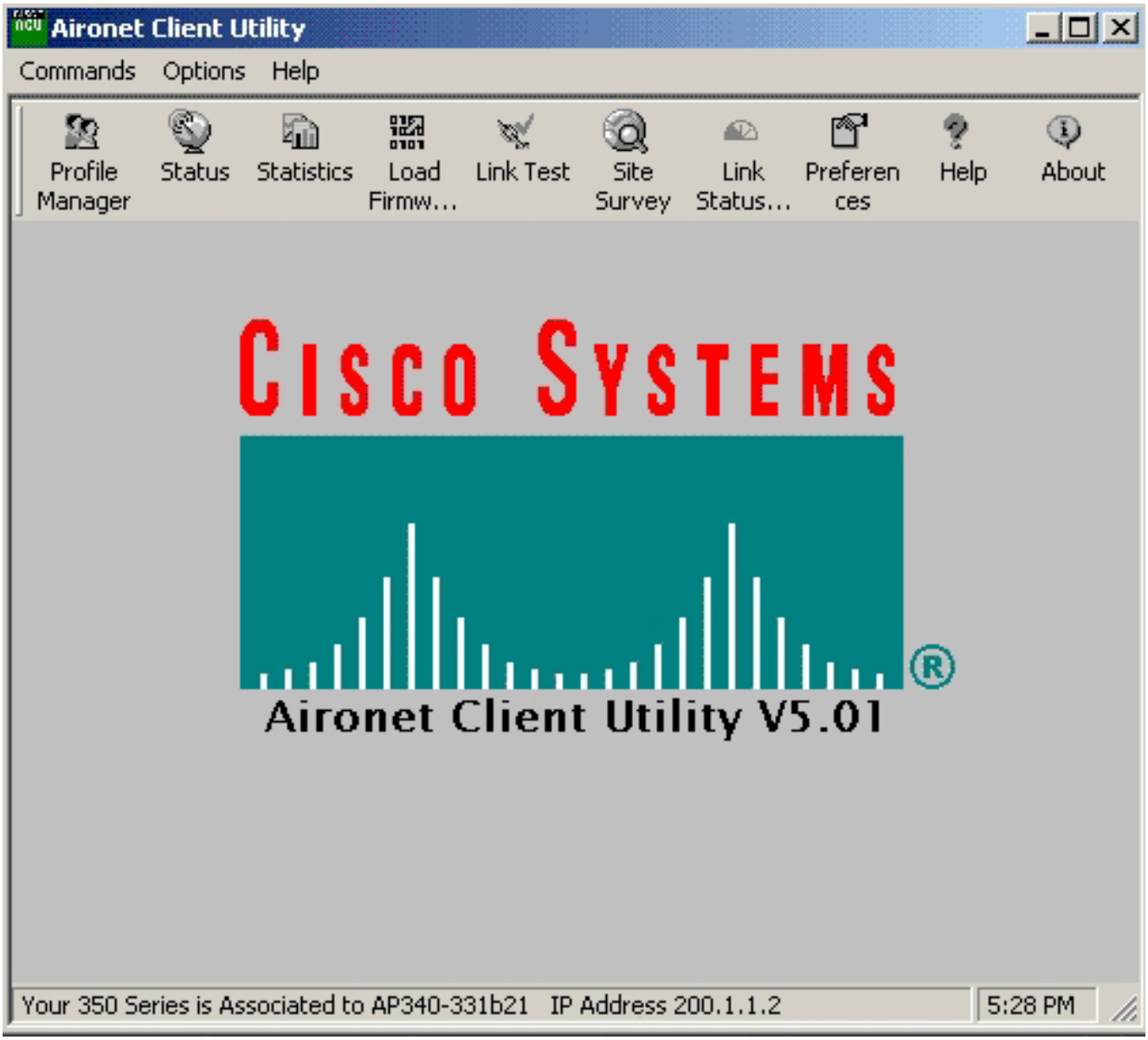


fenêtre.

Vérifiez la caractéristique d'Automatique-initiation dans l'environnement WLAN

Terminez-vous ces étapes afin de vérifier la caractéristique d'autoinitiation dans l'environnement WLAN :

1. Insérez l'adaptateur LAN sans fil dans le PC, et attendez l'association au point d'accès sans fil.Afin de vérifier l'association Sans fil, commencer le logiciel utilitaire d'Aironet Client Utility et vérifier le bas de la fenêtre de client Aironet. Le client sans fil représenté sur la figure peut s'associer au point d'accès sans fil dont l'adresse IP est 200.1.1.2.



2. Une fois que l'association Sans fil est complète, le client vpn lance automatiquement une connexion basée sur l'adresse IP reçue de la connexion Sans fil. Dans ce cas, le client sans fil reçoit 200.1.1.52 du point d'accès sans fil, et le client vpn lance la connexion de SJWireless basée sur la configuration dans vpnclient.ini.Une fois que la connexion VPN est établie, le client peut accéder aux ressources de réseau sous la protection des services sécurisés d'IPSec VPN, comme

affiché.

Vérifiez le journal d'événements de client vpn

Cette section affiche comment vérifier la commande de procédure de connexion d'événement de client vpn pour vérifier que l'autoinitiation poursuit correctement.

Ouvrez le visualiseur de log de Client VPN Cisco et vous voyez les informations semblables à ceci pendant l'autoinitiation. Comme vous pouvez voir, le client vpn reçoit l'adresse IP de 200.1.1.52 de l'association Sans fil, qui tombe dans la liste des réseaux 200.1.1.0/24 définie dans vpnclient.ini. Le client vpn commence alors la connexion de SJWireless en conséquence. Pendant la négociation d'IKE, le Client VPN Cisco reçoit une adresse IP de 50.1.1.8. Il emploie cette adresse IP comme source ip pour accéder au réseau interne derrière le concentrateur de Cisco VPN 3000.

```
222 17:26:05.019 11/19/02 Sev=Info/6 CM/0x63100036 autoinitiation condition detected: Local IP
200.1.1.52 Network 200.1.1.0 Mask 255.255.255.0 Connection Entry "SJWireless" 223 17:26:06.071
11/19/02 Sev=Info/6 DIALER/0x63300002 Initiating connection. 224 17:26:06.081 11/19/02
Sev=Info/4 CM/0x63100002 Begin connection process 225 17:26:06.091 11/19/02 Sev=Info/4
CM/0x63100004 Establish secure connection using Ethernet 226 17:26:06.091 11/19/02 Sev=Info/4
CM/0x63100026 Attempt connection with server "200.1.1.1" 227 17:26:06.091 11/19/02 Sev=Info/6
IKE/0x6300003B Attempting to establish a connection with 200.1.1.1. 228 17:26:06.131 11/19/02
Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID, VID, VID) to
200.1.1.1 229 17:26:06.131 11/19/02 Sev=Info/4 IPSEC/0x63700014 Deleted all keys 230
17:26:06.281 11/19/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 200.1.1.1 231
17:26:06.281 11/19/02 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK AG (SA, KE, NON, ID,
HASH, VID, VID, VID, VID, VID) from 200.1.1.1 232 17:26:06.281 11/19/02 Sev=Info/5
IKE/0x63000059 Vendor ID payload = 12F5F28C457168A9702D9FE274CC0100 233 17:26:06.281 11/19/02
Sev=Info/5 IKE/0x63000001 Peer is a Cisco-Unity compliant peer 234 17:26:06.281 11/19/02
Sev=Info/5 IKE/0x63000059 Vendor ID payload = 09002689DFD6B712 235 17:26:06.281 11/19/02
Sev=Info/5 IKE/0x63000001 Peer supports XAUTH 236 17:26:06.281 11/19/02 Sev=Info/5
IKE/0x63000059 Vendor ID payload = AFCAD71368A1F1C96B8696FC77570100 237 17:26:06.281 11/19/02
Sev=Info/5 IKE/0x63000001 Peer supports DPD 238 17:26:06.281 11/19/02 Sev=Info/5 IKE/0x63000059
Vendor ID payload = 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000 239 17:26:06.281 11/19/02
Sev=Info/5 IKE/0x63000059 Vendor ID payload = 1F07F70EAA6514D3B0FA96542A500306 240 17:26:06.301
11/19/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK AG *(HASH,
NOTIFY:STATUS_INITIAL_CONTACT) to 200.1.1.1 241 17:26:06.311 11/19/02 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 200.1.1.1 242 17:26:06.311 11/19/02 Sev=Warning/2 IKE/0xA3000062
Attempted incoming connection from 200.1.1.1. Inbound connections are not allowed. 243
```

17:26:06.311 11/19/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 200.1.1.1 244 17:26:06.311 11/19/02 Sev=Warning/2 IKE/0xA3000062 Attempted incoming connection from 200.1.1.1. Inbound connections are not allowed. 245 17:26:06.321 11/19/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 200.1.1.1 246 17:26:06.321 11/19/02 Sev=Warning/2 IKE/0xA3000062 Attempted incoming connection from 200.1.1.1. Inbound connections are not allowed. 247 17:26:06.321 11/19/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 200.1.1.1 248 17:26:06.321 11/19/02 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 200.1.1.1 249 17:26:06.321 11/19/02 Sev=Info/4 CM/0x63100015 Launch xAuth application 250 17:26:10.397 11/19/02 Sev=Info/4 CM/0x63100017 xAuth application returned 251 17:26:10.397 11/19/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 200.1.1.1 252 17:26:10.697 11/19/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 200.1.1.1 253 17:26:10.697 11/19/02 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 200.1.1.1 254 17:26:10.697 11/19/02 Sev=Info/4 CM/0x6310000E Established Phase 1 SA. 1 Phase 1 SA in the system 255 17:26:10.707 11/19/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 200.1.1.1 256 17:26:11.779 11/19/02 Sev=Info/5 IKE/0x6300005D Client sending a firewall request to concentrator 257 17:26:11.779 11/19/02 Sev=Info/5 IKE/0x6300005C Firewall Policy: Product=Cisco Integrated Client, Capability= (Centralized Protection Policy). 258 17:26:11.779 11/19/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 200.1.1.1 259 17:26:11.809 11/19/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 200.1.1.1 260 17:26:11.809 11/19/02 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 200.1.1.1 **261 17:26:11.809 11/19/02 Sev=Info/5 IKE/0x63000010 MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_ADDRESS: , value = 50.1.1.8 262 17:26:11.809 11/19/02 Sev=Info/5 IKE/0x63000010 MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_DNS(1): , value = 10.1.1.100 263 17:26:11.809 11/19/02 Sev=Info/5 IKE/0x63000010 MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NBNS(1) (a.k.a. WINS) : , value = 10.1.1.101** 264 17:26:11.809 11/19/02 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SAVEPWD: , value = 0x00000000 265 17:26:11.809 11/19/02 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_PFS: , value = 0x00000000 266 17:26:11.809 11/19/02 Sev=Info/5 IKE/0x6300000E MODE_CFG_REPLY: Attribute = APPLICATION_VERSION, value = Cisco Systems, Inc./ VPN 3000 Concentrator Version 3.6.Rel built by vmurphy on Aug 06 2002 10:41:35 267 17:26:11.819 11/19/02 Sev=Info/4 CM/0x63100019 Mode Config data received 268 17:26:11.839 11/19/02 Sev=Info/5 IKE/0x63000055 Received a key request from Driver for IP address 200.1.1.1, GW IP = 200.1.1.1 269 17:26:11.839 11/19/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 200.1.1.1 270 17:26:11.849 11/19/02 Sev=Info/5 IKE/0x63000055 Received a key request from Driver for IP address 10.10.10.255, GW IP = 200.1.1.1 271 17:26:11.849 11/19/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 200.1.1.1 272 17:26:11.859 11/19/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 200.1.1.1 273 17:26:11.859 11/19/02 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK INFO *(HASH, NOTIFY:STATUS_RESP_LIFETIME) from 200.1.1.1 274 17:26:11.859 11/19/02 Sev=Info/5 IKE/0x63000044 RESPONDER-LIFETIME notify has value of 86400 seconds 275 17:26:11.859 11/19/02 Sev=Info/5 IKE/0x63000046 This SA has already been alive for 5 seconds, setting expiry to 86395 seconds from now 276 17:26:11.859 11/19/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 200.1.1.1 277 17:26:11.859 11/19/02 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID, NOTIFY:STATUS_RESP_LIFETIME) from 200.1.1.1 278 17:26:11.859 11/19/02 Sev=Info/5 IKE/0x63000044 RESPONDER-LIFETIME notify has value of 28800 seconds 279 17:26:11.859 11/19/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK QM *(HASH) to 200.1.1.1 280 17:26:11.859 11/19/02 Sev=Info/5 IKE/0x63000058 Loading IPSec SA (Message ID = 0xF9D733A7 OUTBOUND SPI = 0x1AD0BBA1 INBOUND SPI = 0xA99C00B3) 281 17:26:11.859 11/19/02 Sev=Info/5 IKE/0x63000025 Loaded OUTBOUND ESP SPI: 0x1AD0BBA1 282 17:26:11.859 11/19/02 Sev=Info/5 IKE/0x63000026 Loaded INBOUND ESP SPI: 0xA99C00B3 283 17:26:11.859 11/19/02 Sev=Info/4 CM/0x6310001A One secure connection established 284 17:26:11.879 11/19/02 Sev=Info/6 DIALER/0x63300003 Connection established. 285 17:26:11.889 11/19/02 Sev=Info/6 DIALER/0x63300008 MAPI32 Information - Outlook not default mail client 286 17:26:11.929 11/19/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 200.1.1.1 287 17:26:11.929 11/19/02 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID, NOTIFY:STATUS_RESP_LIFETIME) from 200.1.1.1 288 17:26:11.929 11/19/02 Sev=Info/5 IKE/0x63000044 RESPONDER-LIFETIME notify has value of 28800 seconds 289 17:26:11.929 11/19/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK QM *(HASH) to 200.1.1.1 290 17:26:11.939 11/19/02 Sev=Info/5 IKE/0x63000058 Loading IPSec SA (Message ID = 0x0660AF57 OUTBOUND SPI = 0x5E6E8676 INBOUND SPI = 0xF5EAA827) 291 17:26:11.939 11/19/02 Sev=Info/5 IKE/0x63000025 Loaded OUTBOUND ESP SPI: 0x5E6E8676 292 17:26:11.939 11/19/02 Sev=Info/5 IKE/0x63000026 Loaded INBOUND ESP SPI: 0xF5EAA827 293 17:26:11.939 11/19/02 Sev=Info/4 CM/0x63100022 Additional Phase 2 SA established. 294 17:26:12.891 11/19/02 Sev=Info/4 IPSEC/0x63700014 Deleted all keys 295 17:26:12.891 11/19/02 Sev=Info/4 IPSEC/0x63700010 Created a new key structure 296 17:26:12.891 11/19/02 Sev=Info/4 IPSEC/0x6370000F Added key with SPI=0xa1bbd01a into key list 297 17:26:12.891 11/19/02 Sev=Info/4 IPSEC/0x63700010 Created a new

```
key structure 298 17:26:12.891 11/19/02 Sev=Info/4 IPSEC/0x6370000F Added key with
SPI=0xb3009ca9 into key list 299 17:26:12.891 11/19/02 Sev=Info/4 IPSEC/0x63700010 Created a new
key structure 300 17:26:12.891 11/19/02 Sev=Info/4 IPSEC/0x6370000F Added key with
SPI=0x76866e5e into key list 301 17:26:12.891 11/19/02 Sev=Info/4 IPSEC/0x63700010 Created a new
key structure 302 17:26:12.891 11/19/02 Sev=Info/4 IPSEC/0x6370000F Added key with
SPI=0x27a8eaf5 into key list 303 17:26:21.904 11/19/02 Sev=Info/6 IKE/0x6300003D Sending DPD
request to 200.1.1.1, seq# = 2877451244 304 17:26:21.904 11/19/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK INFO *(HASH, NOTIFY:DPD_REQUEST) to 200.1.1.1
```

Vérifiez un état différent d'Automatique-initiation

Référez-vous utilisant des informations antérieures d'initiation automatique VPN sur d'autres états d'autoinitiation.

Informations connexes

- Volume de référence de concentrateur de la gamme VPN 3000 I : Configuration
- Page d'assistance des concentrateurs VPN Cisco 3000
- Page d'assistance du Client VPN 3000 Series Cisco
- Page d'assistance IPsec
- Support et documentation techniques - Cisco Systems