Exemple de configuration d'un VPN client sur un réseau local sans fil avec WLC

Contenu

Introduction

Ce document présente le concept d’un réseau privé virtuel (VPN) dans un environnement sans fil. Le document explique les configurations utilisées dans le déploiement d’un tunnel VPN entre un client sans fil et un serveur VPN par un contrôleur LAN sans fil (WLC).

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Connaissance des WLC et configuration de leurs paramètres de base
- Connaissance des concepts du WPA (Wi-Fi Protected Access)
- Connaissances de base du VPN et de ses types
- Connaissance d’IPSec
- Connaissances de base des algorithmes de chiffrement, d’authentification et de hachage disponibles

Components Used

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

- Cisco 2006 WLC qui exécute la version 4.0.179.8
- Point d'accès allégé (LAP) Cisco, série 1000
- Cisco 3640 qui exécute Cisco IOS®, version 12.4(8) du logiciel
- Cisco VPN Client, version 4.8

Remarque : ce document utilise un routeur 3640 comme serveur VPN. Pour prendre en charge des fonctions de sécurité avancées, vous pouvez également utiliser un serveur VPN dédié.

Remarque : pour qu'un routeur puisse agir en tant que serveur VPN, il doit exécuter un ensemble de fonctionnalités prenant en charge IPsec de base.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Informations générales

Un VPN est un réseau de données privé utilisé pour transmettre en toute sécurité les données d'un réseau privé par l'infrastructure de télécommunications publique comme Internet. Ce VPN assure la confidentialité des données grâce à l'utilisation de procédures de sécurité et d'un protocole de tunnellisation.

VPN d'accès à distance

La configuration d'un VPN d'accès à distance permet aux clients de logiciels VPN, tels que les utilisateurs mobiles, d'accéder en toute sécurité aux ressources réseau centralisées qui se trouvent derrière un serveur VPN. Dans les terminologies Cisco, ces serveurs et ces clients VPN sont également appelés le serveur Cisco Easy VPN et le périphérique à distance Cisco Easy VPN.

Un périphérique à distance Cisco Easy VPN peut être un routeur Cisco IOS, un appareil de sécurité Cisco PIX, le client matériel Cisco VPN 3002 et le client VPN Cisco. Ils servent à recevoir des politiques de sécurité sur une connexion par tunnel VPN à partir d'un serveur Cisco Easy VPN. Ainsi, au lieu éloigné, les exigences de configuration sont réduites au minimum. Le client VPN Cisco est un client logiciel qui peut être installé sur PC et sur ordinateur portable, notamment.

Un serveur Cisco Easy VPN peut être un routeur Cisco IOS, un appareil de sécurité Cisco PIX et un concentrateur Cisco VPN 3000.

Dans ce document, c'est le logiciel Cisco VPN Client qui s'exécute sur un ordinateur portable en

tant que client VPN et le routeur Cisco 3640 IOS en tant que serveur VPN. Le document utilise la norme IPSec pour établir un tunnel VPN entre un client et un serveur.

IPsec

IPSec consiste en un cadre de normes ouvertes qui est élaboré par l'IETF (Internet Engineering Task Force). IPSec assure la sécurité des transmissions d'informations sensibles sur des réseaux non protégés tels qu'Internet.

IPSec fournit le chiffrement des données réseau au niveau des paquets IP, offrant ainsi une solution de sécurité robuste reposant sur des normes. La principale tâche d'IPSec consiste à autoriser l'échange d'informations privées sur une connexion non sécurisée. IPSec utilise le chiffrement pour protéger l'information contre les écoutes clandestines ou les interceptions. Toutefois, pour utiliser efficacement le chiffrement, les deux parties doivent partager un secret qui sert à la fois pour le chiffrement et le déchiffrement de l'information.

IPSec fonctionne en deux phases pour permettre l'échange confidentiel d'un secret partagé :

- Phase 1 : La gestion de la négociation des paramètres de sécurité nécessaires pour l'établissement d'un canal sécurisé entre deux homologues IPSec. La mise en œuvre de la phase 1 se fait généralement par le protocole IKE (Internet Key Exchange). Si l'homologue IPSec distant ne peut pas exécuter IKE, vous pouvez alors procéder à la configuration manuelle avec des clés prépartagées pour mettre fin à la phase 1.
- Phase 2 : L'utilisation du tunnel sécurisé créé à la phase 1 pour échanger les paramètres de sécurité requis pour la transmission des données de l'utilisateur. Les tunnels sécurisés servant pour ces deux phases reposent sur des associations de sécurité (SA) employées à chaque point d'extrémité d'IPSec. Les SA décrivent les paramètres de sécurité, comme le type d'authentification et de chiffrement, que les deux points d'extrémité conviennent d'utiliser.

Les paramètres de sécurité échangés à la phase 2 servent à créer un tunnel IPSec qui est utilisé à son tour pour le transfert de données entre le client VPN et le serveur.

Consultez la section Configuration d'IPSec pour en savoir plus sur IPSec et sa configuration.

Lorsqu'un tunnel VPN est créé entre le client VPN et le serveur, *les politiques de sécurité définies sur le serveur VPN sont envoyées au client*. Ainsi, au lieu éloigné, les exigences de configuration sont réduites au minimum.

Remarque : Utilisez l'outil de recherche de commandes (clients inscrits seulement) pour en savoir plus sur les commandes figurant dans le présent document.

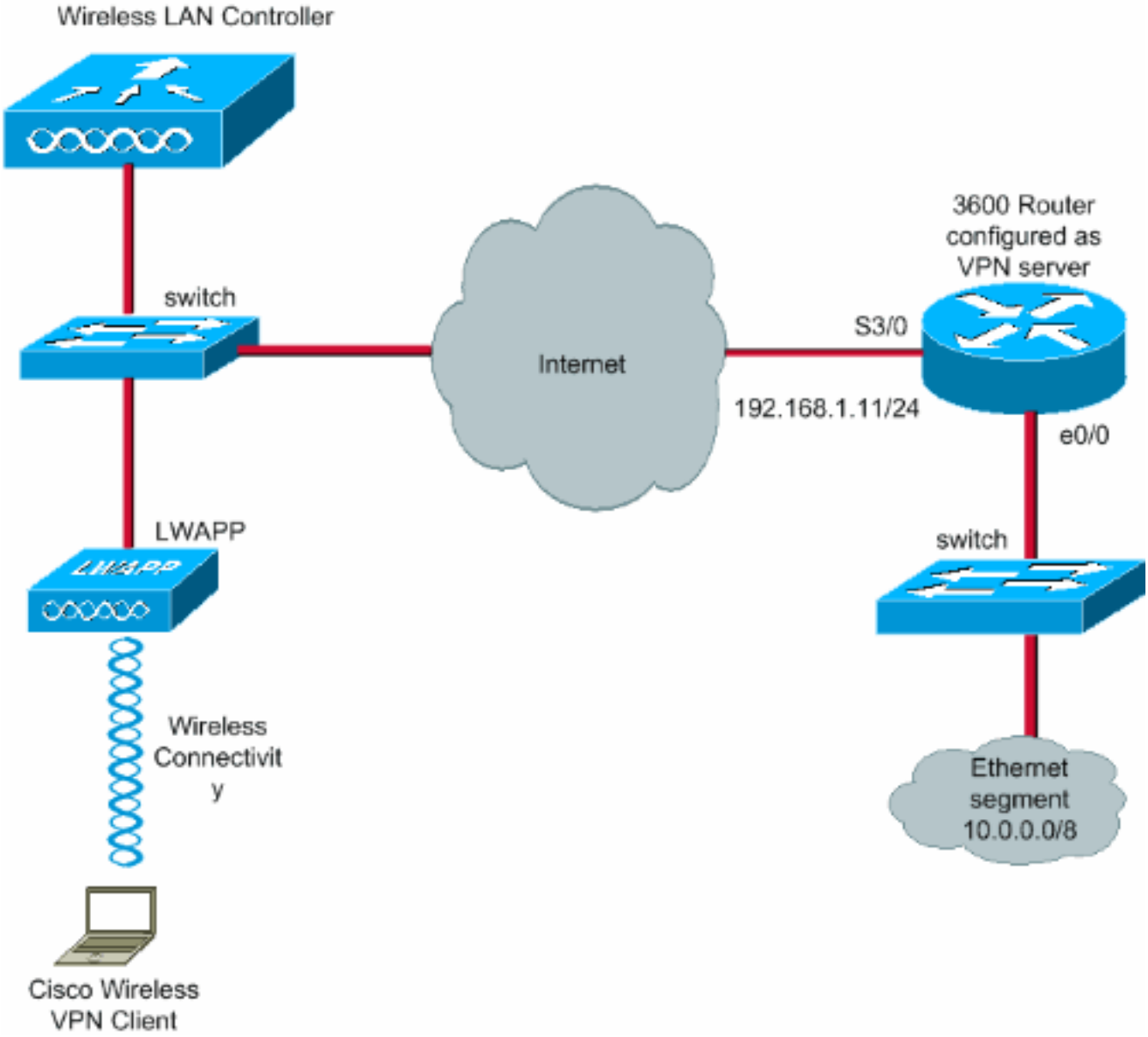
Diagramme du réseau

Ce document utilise les configurations suivantes :

- Adresse IP de l'interface de gestion du WLC : 172.16.1.10/16
- Adresse IP de l'interface du gestionnaire du point d'accès du WLC : 172.16.1.11/16
- Passerelle par défaut : 172.16.1.20/16**Remarque :** Dans un réseau actif, cette passerelle par défaut doit pointer vers l'interface entrante du routeur immédiat qui connecte le WLC au reste du réseau et/ou à Internet.
- Adresse IP du serveur VPN s3/0 : 192.168.1.11/24**Remarque :** Cette adresse IP doit pointer

vers l'interface qui termine le tunnel VPN côté serveur VPN. Dans le présent exemple, « s3/0 » correspond à l'interface qui met fin au tunnel VPN sur le serveur VPN.

- Le segment LAN du serveur VPN utilise la plage d'adresses IP 10.0.0.0/8.



Configuration

Dans une architecture WLAN centralisée, pour qu'un client VPN sans fil, p. ex. un ordinateur portable, puisse créer un tunnel VPN avec un serveur VPN, le client doit être associé à un point d'accès allégé (LAP), qui doit à son tour être enregistré sur un WLC. Dans ce document, le LAP est déjà enregistré sur le WLC grâce au processus de détection de la diffusion du sous-réseau local expliqué dans la section sur l'enregistrement d'un point d'accès allégé à un contrôleur (WLC) WLAN.

L'étape suivante consiste à configurer le WLC pour le VPN.

Terminaison VPN et relais

Avec les WLC de la série Cisco 4000 antérieurs à la version 4, la fonction appelée « Terminaison IPSec VPN » (soutien IPSec) est prise en charge. Cette fonction permet à ces contrôleurs de mettre fin directement aux sessions VPN client. En résumé, cette fonctionnalité permet au

contrôleur d’agir comme serveur VPN. Pour ce faire, il faut qu’un module matériel de terminaison VPN distinct soit installé dans le contrôleur.

Le VPN IPSec n’est pas pris en charge par ce qui suit :

- WLC Cisco, série 2000
- Tout WLC qui exécute les versions 4.0 ou ultérieures

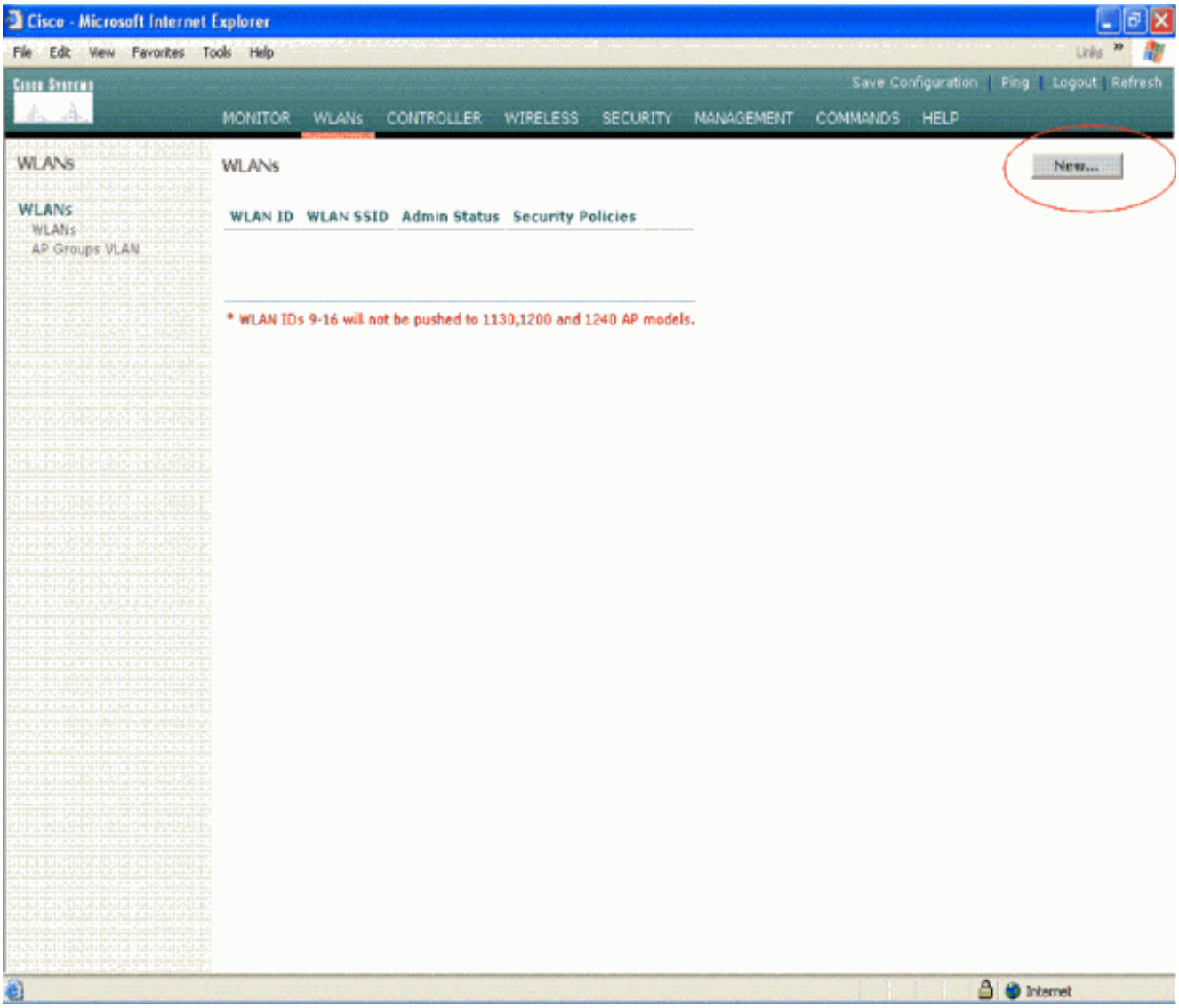
Or, la seule fonction VPN prise en charge dans les versions ultérieures à 4.0 est le relais VPN. Cette fonction est également prise en charge par les contrôleurs WLC Cisco de série 2000.

Le relais VPN est une fonction permettant à un client de créer un tunnel seulement grâce à un serveur VPN en particulier. Donc, si vous devez accéder en toute sécurité au serveur VPN configuré ainsi qu’à un autre serveur VPN ou à Internet, l’activation du relais VPN sur le contrôleur est impossible. Dans de telles circonstances, vous devez désactiver le relais VPN. Toutefois, le WLC peut être configuré comme relais vers plusieurs passerelles VPN lorsqu’un ACL approprié est créé, puis appliqué au WLAN correspondant. Dans l’éventualité où vous souhaitiez atteindre plusieurs passerelles VPN pour une question de redondance, désactivez le relais VPN, puis créez un ACL qui permet l’accès aux passerelles VPN et l’application de l’ACL au WLAN.

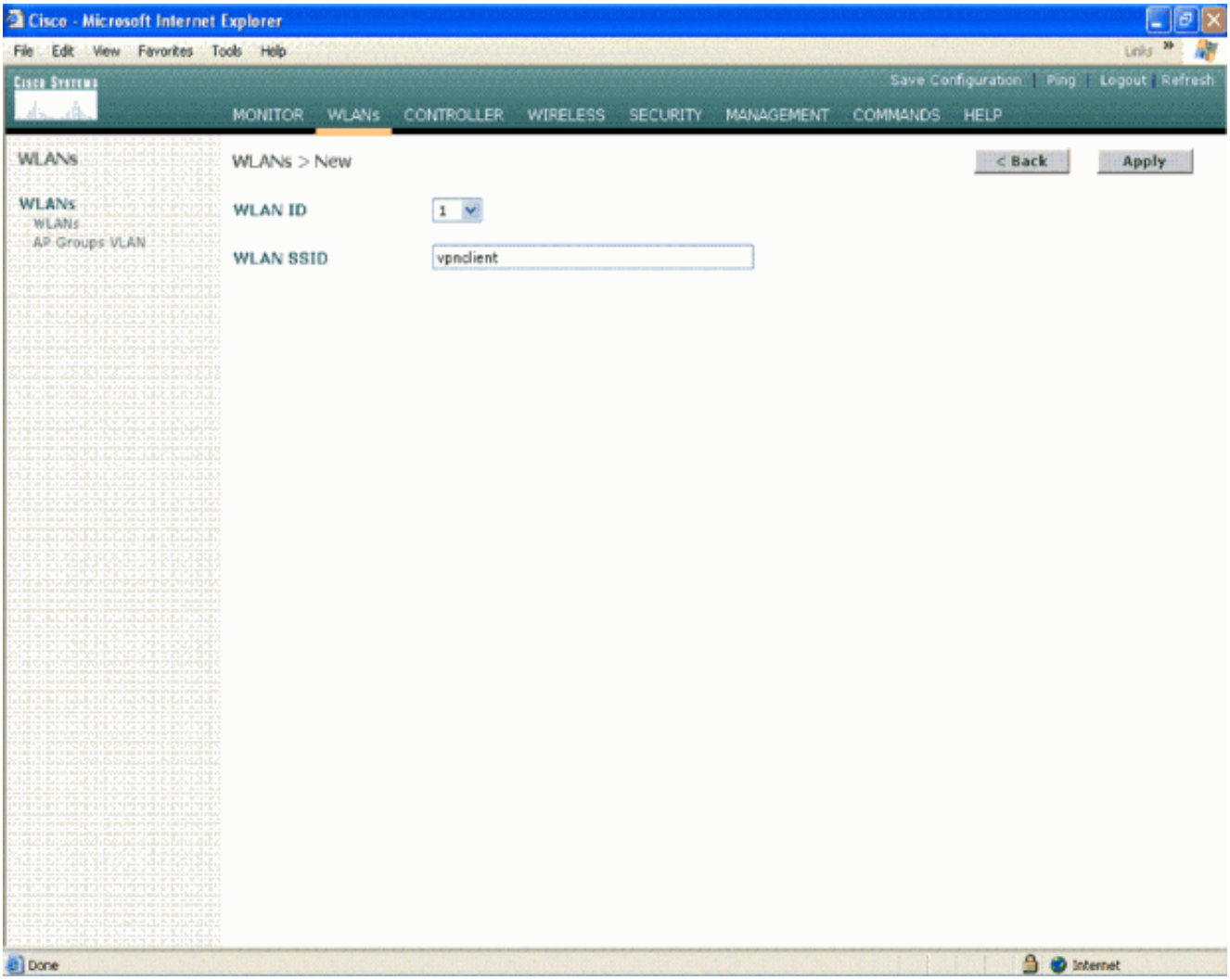
Configurez le WLC pour le relais VPN

Voici la marche à suivre pour configurer le relais VPN :

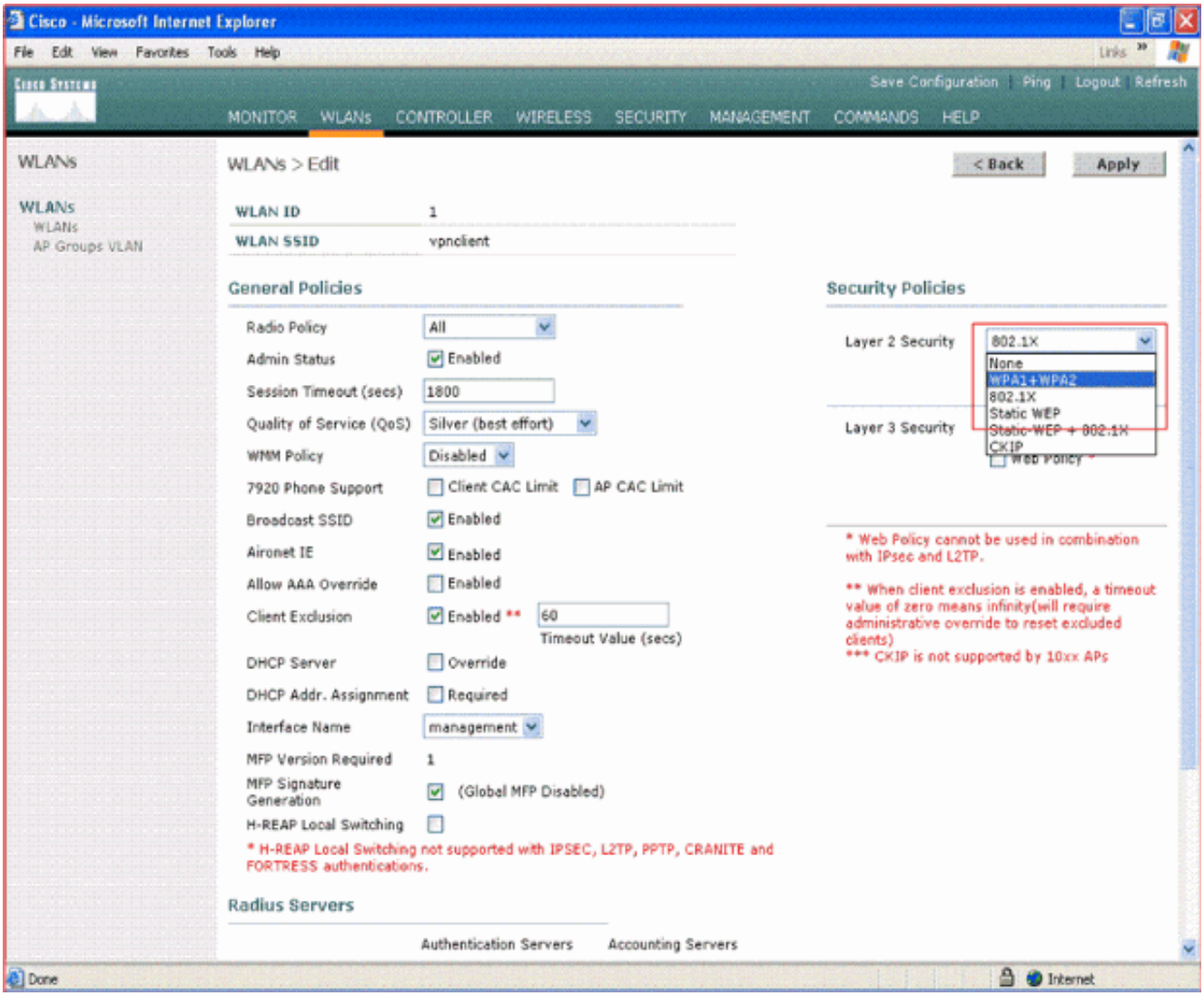
1. Dans l’interface GUI du WLC, cliquez sur **WLAN pour accéder à la page correspondante.**
2. Cliquez sur New [nouveau] pour créer un autre WLAN.



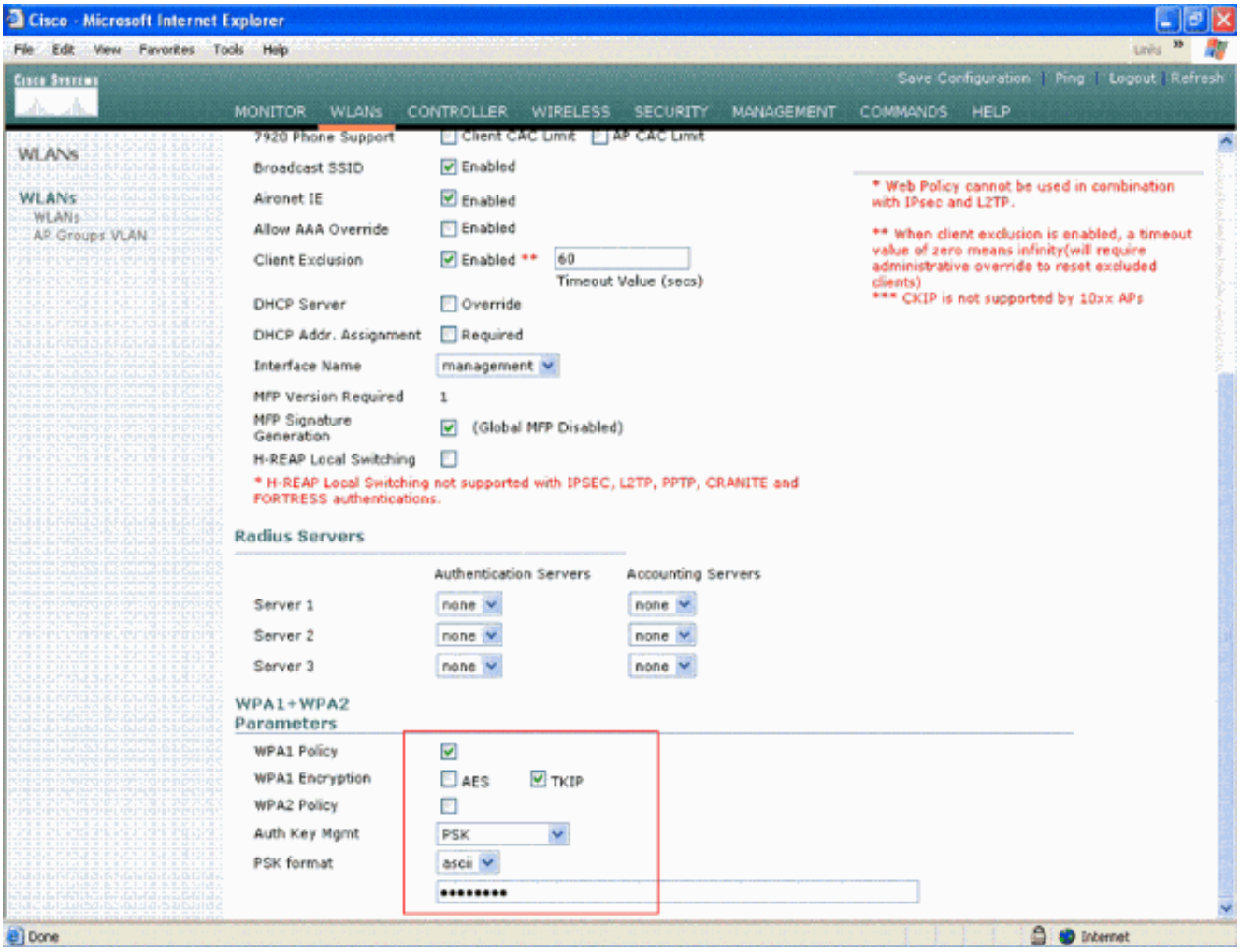
3. L'identificateur de l'ensemble de service (SSID) du WLAN est vpnclient dans le présent exemple. Cliquez sur
   Apply.



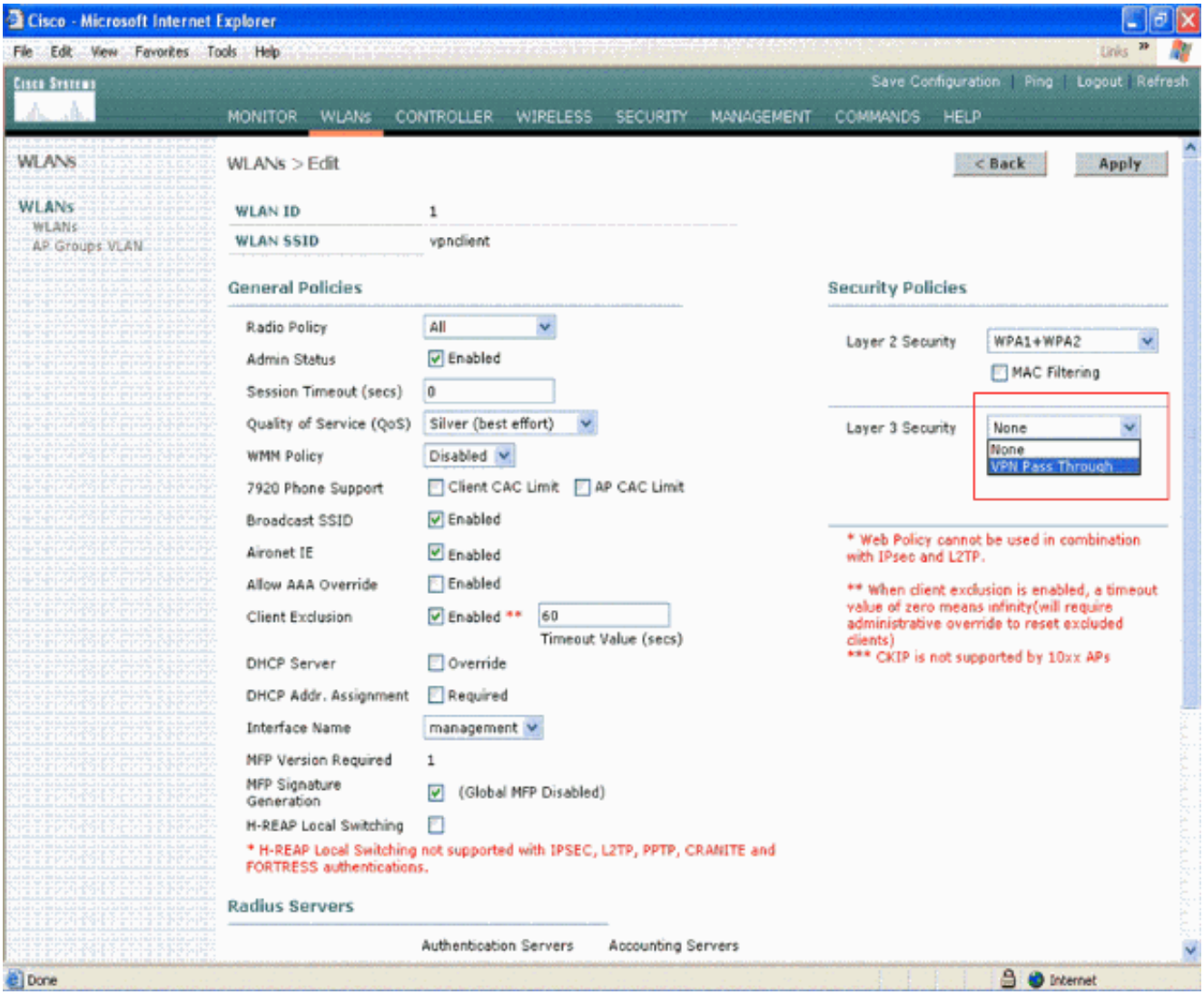
4. Configurez le SSID vpnclient en utilisant la sécurité de couche 2. *Ceci est facultatif.*Le présent exemple utilise **WPA1 + WPA2 comme type de sécurité.**



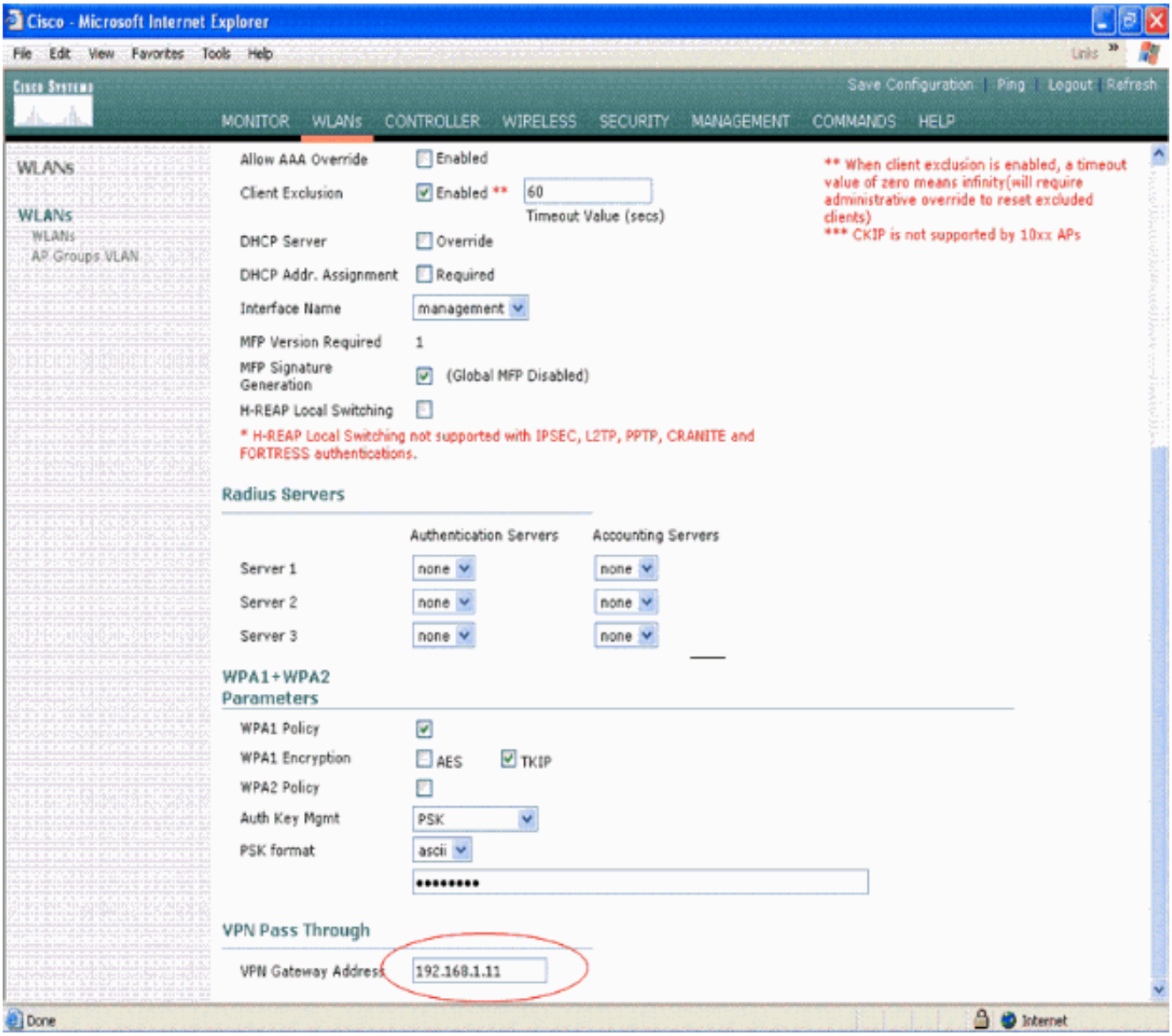
5. Configurez la politique WPA ainsi que le type de gestion des clés d'authentification à utiliser.Le présent exemple montre une **clé prépartagée (PSK) pour la gestion des clés d'authentification.** Une fois l'option PSK sélectionnée, choisissez **ASCII comme format PSK et saisissez-en la valeur.** La valeur doit être la même dans la configuration SSID du client sans fil pour que les clients qui appartiennent au SSID soient associés à ce WLAN.



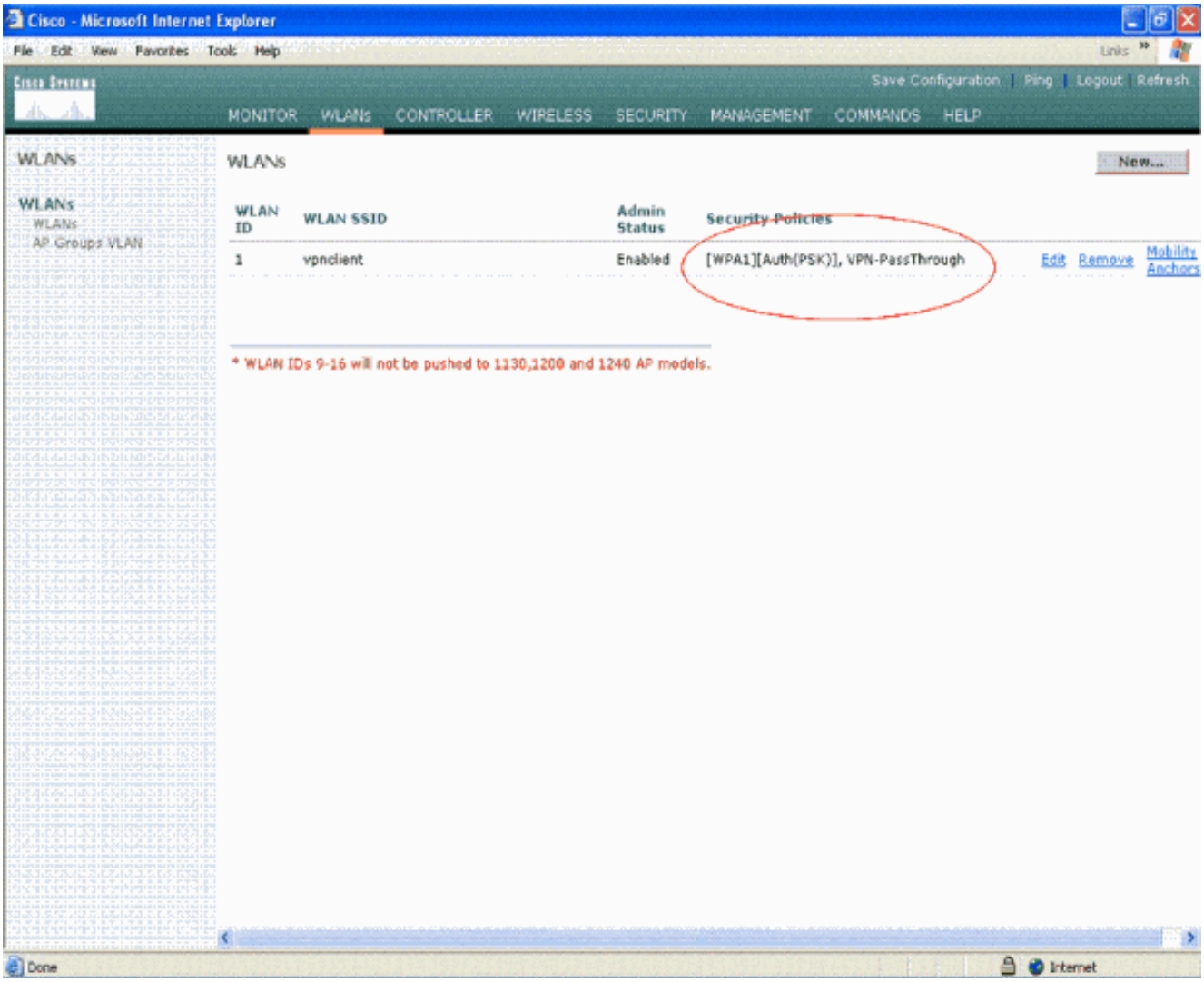
6. Sélectionnez le **relais VPN comme sécurité de couche 3.**
   Exemple :



7. Lorsque le relais VPN est sélectionné comme sécurité de couche 3, ajoutez l'adresse de la passerelle VPN comme l'illustre l'exemple.L'adresse de la passerelle doit correspondre à l'adresse IP de l'interface qui met fin au tunnel VPN du côté du serveur. Dans le présent exemple, l'adresse IP de l'interface s3/0 (192.168.1.11/24) sur le serveur VPN correspond à l'adresse de la passerelle à
configurer.



8. Cliquez sur Apply. Le WLAN *vpnclient est maintenant configuré pour le relais VPN.*



Configuration du serveur VPN

Cette configuration présente le routeur Cisco 3640 en tant que serveur VPN.

Remarque : Pour des raisons de simplicité, cette configuration utilise le routage statique pour maintenir l'accessibilité IP entre les points d'extrémité. Vous pouvez utiliser n'importe quel protocole de routage dynamique, tel que le protocole RIP (Routing Information Protocol) ou le protocole OSPF (Open Shortest Path First), pour garantir l'accessibilité.

Remarque : le tunnel n'est pas établi s'il n'y a aucune accessibilité IP entre le client et le serveur.

Remarque : ce document suppose que l'utilisateur sait comment activer le routage dynamique dans le réseau.

Routeur Cisco 3640
vpnrouter#**show running-config** Building configuration... Current configuration : 1623 bytes ! version 12.4 service timestamps debug datetime msec service timestamps log datetime msec

```
no service password-encryption
!
hostname vpnrouter
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
!
aaa authorization network employee local
!
aaa session-id common
!
resource policy
!
memory-size iomem 10
!
!
ip cef
no ip domain lookup
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
crypto isakmp policy 1
!--- Create an Internet Security Association and Key
Management !--- Protocol (ISAKMP) policy for Phase 1
negotiation. hash md5
!--- Choose the hash algorithm to be md5. authentication
pre-share
!--- The authentication method selected is pre-shared.
group 2
!--- With the group command, you can declare what size
modulus to !--- use for Diffie-Hellman calculation.
Group 1 is 768 bits long, !--- and group 2 is 1024 bits
long.


crypto isakmp client configuration group employee key
cisco123 pool mypool
!
!--- Create the Phase 2 policy for actual data
encryption. crypto ipsec transform-set myset esp-3des
esp-md5-hmac
!--- Create a dynamic map and apply the transform set
that was created. !--- Set reverse-route for the VPN
server. crypto dynamic-map mymap 10 set transform-set
myset reverse-route
```

```
!
crypto map clientmap isakmp authorization list employee
!--- Create the crypto map.
crypto map clientmap client configuration address crypto
map clientmap 10 ipsec-isakmp dynamic mymap
!
!--- Apply the employee group list that was created
earlier.



!
!
!
!
interface Ethernet0/0
 ip address 10.0.0.20 255.0.0.0
 half-duplex
!
interface Serial3/0
 ip address 192.168.1.11 255.255.255.0
 clock rate 64000
 no fair-queue
 crypto map clientmap
!--- Apply the crypto map to the interface. ! interface
Serial3/1 no ip address shutdown ! interface Serial3/2
no ip address shutdown ! interface Serial3/3 no ip
address shutdown ! interface Serial3/4 no ip address
shutdown ! interface Serial3/5 no ip address shutdown !
interface Serial3/6 no ip address shutdown ! interface
Serial3/7 no ip address shutdown ip local pool mypool
10.0.0.50 10.0.0.60
!--- Configure the Dynamic Host Configuration Protocol
!--- (DHCP) pool which assigns the tunnel !--- IP
address to the wireless client. !--- This tunnel IP
address is different from the IP address !--- assigned
locally at the wireless client (either statically or
dynamically). ip http server no ip http secure-server !
ip route 172.16.0.0 255.255.0.0 192.168.1.10 ! ! ! !
control-plane ! ! ! ! ! ! ! ! ! line con 0 line aux 0
line vty 0 4 ! ! end ip subnet-zero . . . ! end
```

Remarque : cet exemple utilise uniquement l'authentification de groupe. L'authentification individuelle des utilisateurs n'est donc pas employée.

Configuration du client VPN

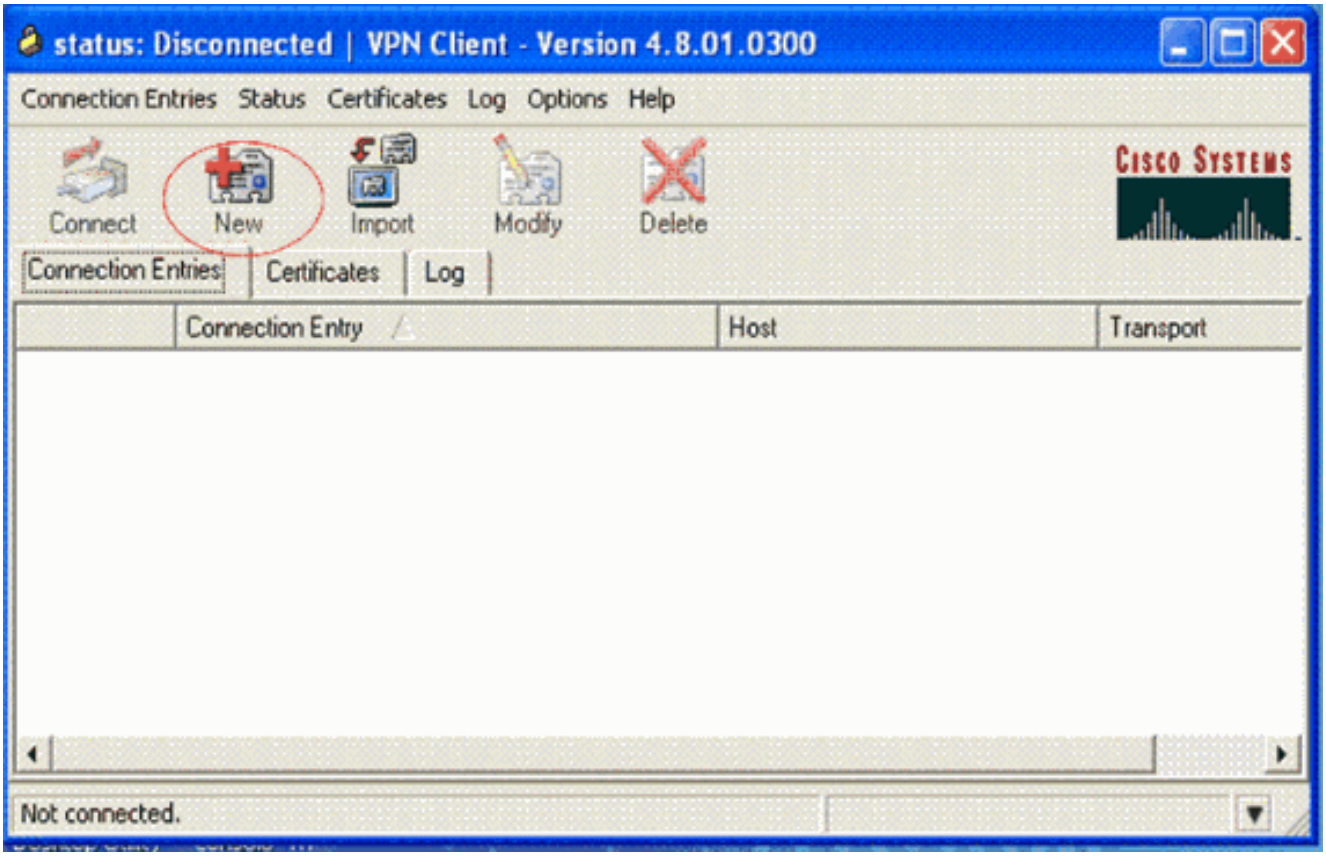
Un client VPN logiciel peut être téléchargé à partir du Centre de logiciel Cisco.com.

Remarque : certains logiciels Cisco exigent que vous vous connectiez avec un nom d'utilisateur et un mot de passe CCO.

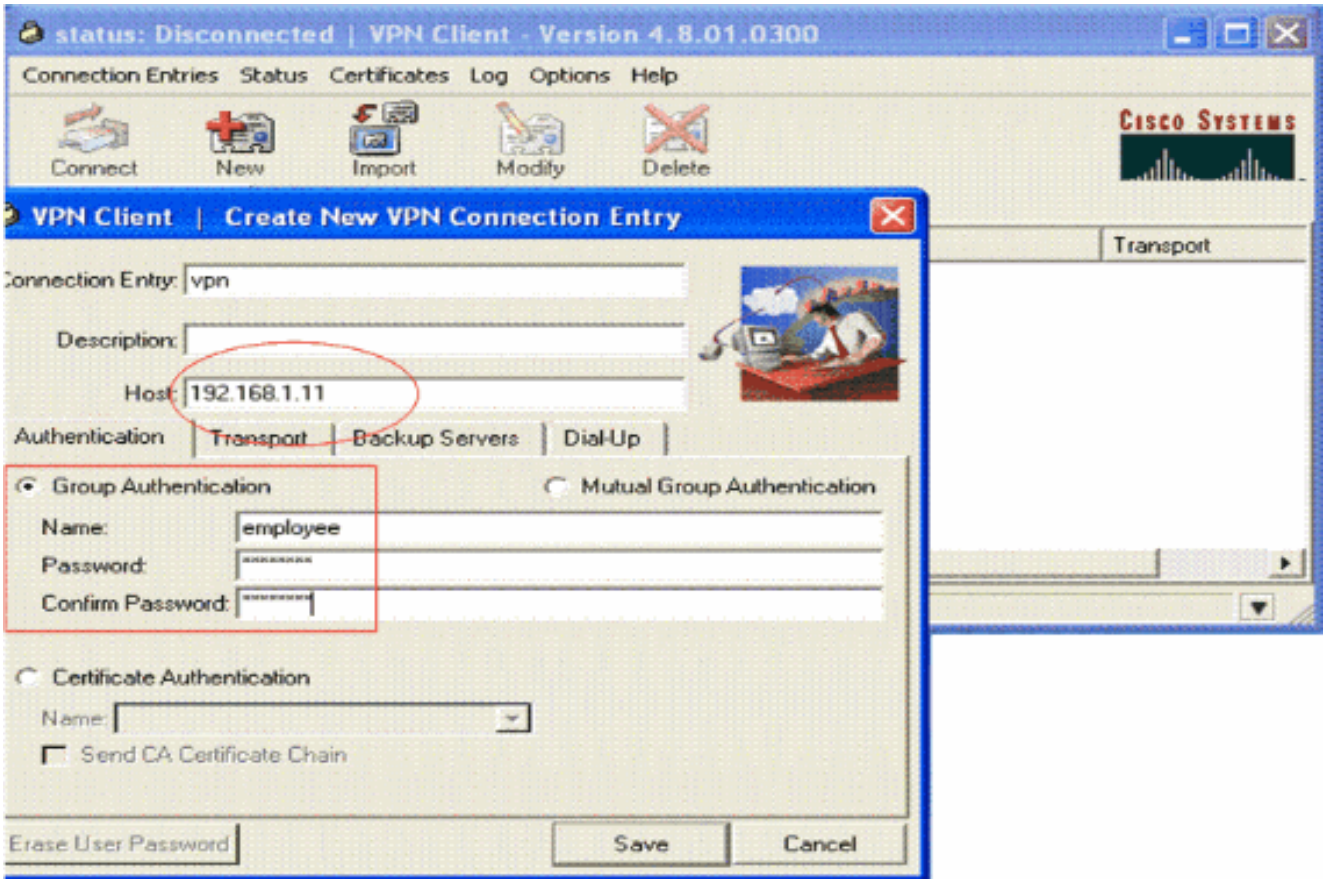
Exécutez les étapes suivantes afin de configurer le client VPN.

1. Pour accéder au client VPN à partir de votre client sans fil (ordinateur portable), allez à **Start [démarrer] > Programs [programmes] > Cisco Systems VPN Client [client VPN Cisco Systems] > VPN Client [client VPN]**. Il s'agit de l'emplacement par défaut où est installé le client VPN.
2. Cliquez sur New [nouveau] pour ouvrir la fenêtre servant à créer une nouvelle entrée pour la

connexion
VPN.



3. Entrez le nom de l'entrée de connexion avec une description. Cet exemple illustre « usesvpn ».Le champ « Description » est facultatif. Saisissez l'adresse IP du serveur VPN dans la case sur l'hôte. Entrez ensuite le nom du groupe VPN et le mot de passe, puis cliquez sur
Save.



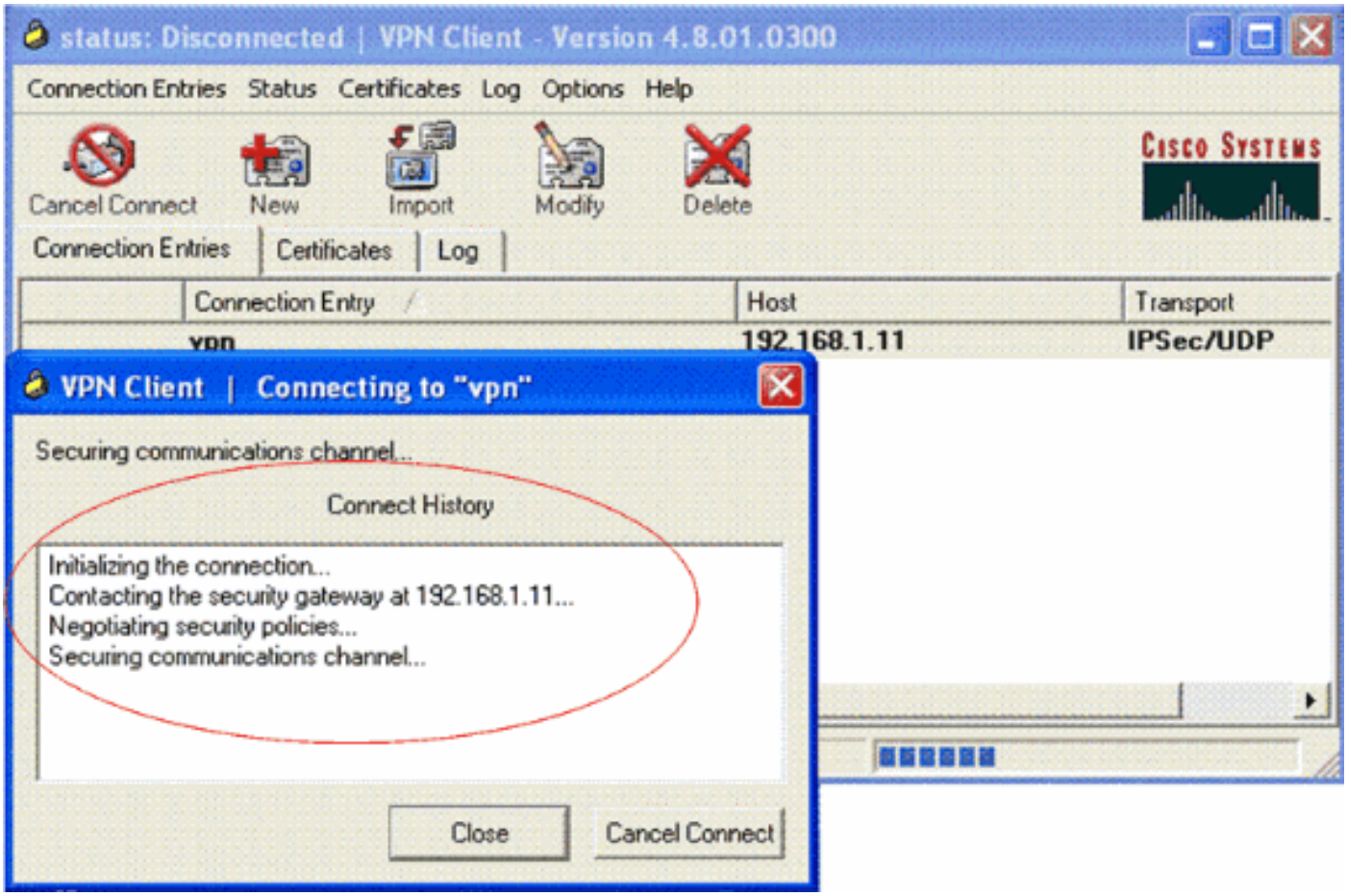
Remarque : Le nom de groupe et le mot de passe configurés ici doivent être identiques à ceux configurés sur le serveur VPN. Le nom d'utilisateur « *employee* » et le mot de passe « *cisco123* » sont utilisés dans le présent exemple.

Vérification

Aux fins de vérification, configurez le SSID **vpnclient** du client sans fil selon les mêmes paramètres de sécurité que le WLC, puis associez le client à ce WLAN. Plusieurs documents expliquent comment configurer un client sans fil avec un nouveau profil.

Une fois que le client sans fil est associé, accédez au client VPN, puis cliquez sur la connexion que vous avez configurée. Ensuite, **connectez-vous à partir de la fenêtre principale du client VPN.**

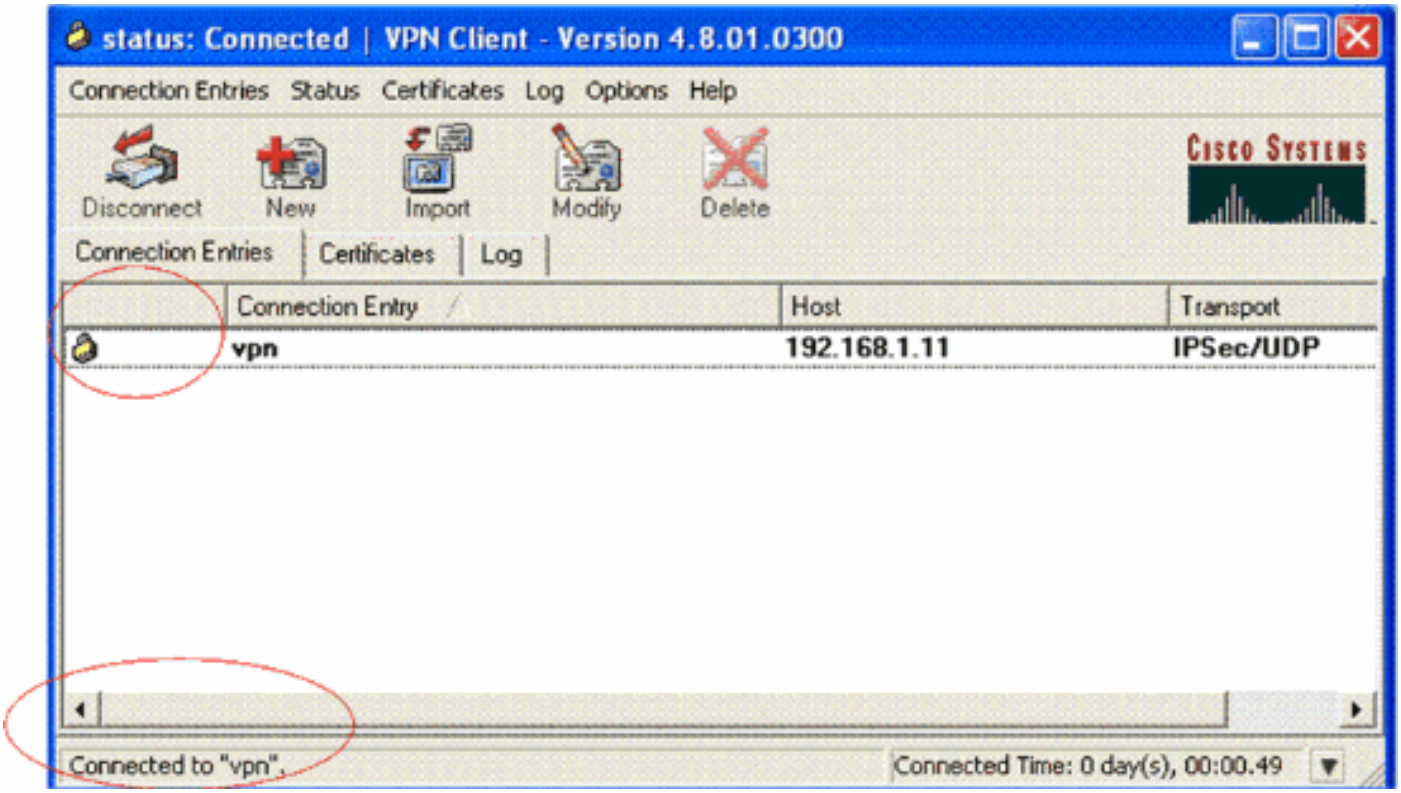
Vous pouvez voir les paramètres de sécurité des phases 1 et 2 qui ont été négociés entre le client et le serveur.



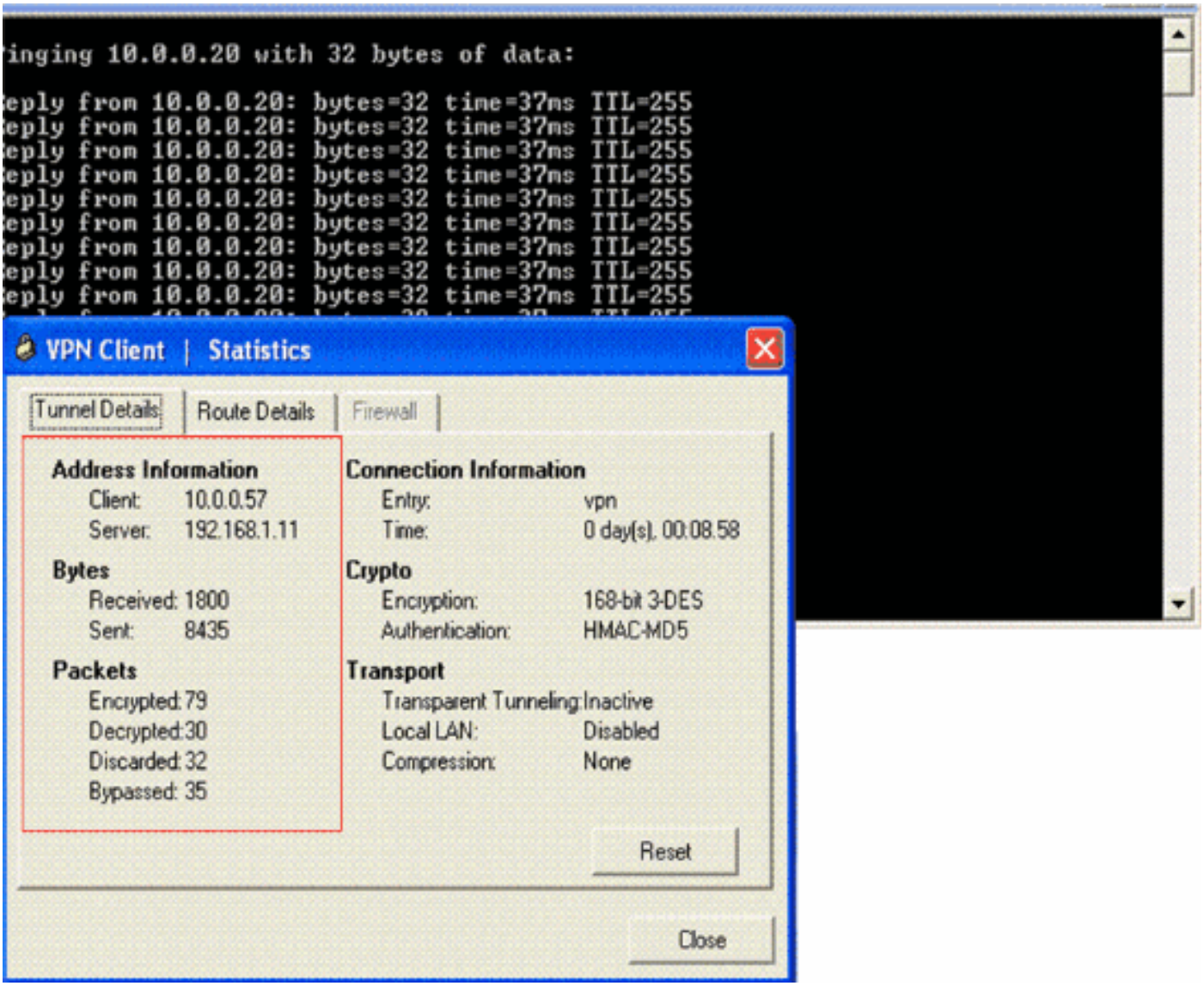
Remarque : afin d'établir ce tunnel VPN, le client VPN et le serveur doivent avoir une accessibilité IP entre eux. Si le client VPN ne parvient pas à entrer en contact avec la passerelle de sécurité (serveur VPN), c'est que le tunnel n'est pas créé. Une case d'alerte s'affiche alors du côté du client, indiquant le message qui suit :

```
Reason 412: The remote peer is no longer responding
```

Afin de vous assurer qu'un tunnel VPN est créé correctement entre le client et le serveur, vous pouvez repérer la présence d'une icône de cadenas à côté du client VPN correspondant. La barre d'état indique également **Connected to "vpn"** [connecté au « VPN »]. Voici un exemple.



De plus, assurez-vous que vous êtes en mesure de transmettre les données au segment LAN du côté du serveur à partir du client VPN, et inversement. Dans le menu principal du client VPN, sélectionnez **Status [statut] > Statistics [statistiques]**. Vous y trouverez les statistiques des paquets chiffrés et déchiffrés qui transitent par le tunnel.



Dans cette capture d'écran, vous pouvez voir l'adresse du client, soit 10.0.0.57. Il s'agit de l'adresse que le serveur VPN a octroyée au client à partir de son bassin configuré localement après la négociation réussie de la phase 1. Une fois que le tunnel est créé, le serveur VPN ajoute automatiquement un routage à cette adresse IP du DHCP dans son tableau de routage.

Vous pouvez également constater l'augmentation du nombre de paquets chiffrés au fur et à mesure que les données sont transférées du client au serveur ainsi que la hausse du nombre de paquets déchiffrés pendant le transfert inverse des données.

Remarque : Puisque le WLC est configuré pour le Passthrough VPN, il permet au client d'accéder uniquement au segment connecté à la passerelle VPN (ici, il s'agit du serveur VPN 192.168.1.11) configuré pour le Passthrough. Tout autre trafic est ainsi filtré.

Aux fins de vérification, vous pouvez utiliser la même configuration sur un autre serveur VPN et paramétrer une nouvelle entrée de connexion pour ce serveur VPN sur le client VPN. À présent, lorsque vous essayez de créer un tunnel avec ce serveur VPN, rien n'aboutit. Cette situation s'explique par le fait que le WLC filtre le trafic et autorise un tunnel seulement vers l'adresse de la passerelle VPN configurée pour le relais VPN.

Vous pouvez également vérifier la configuration à partir de l'interface CLI du serveur VPN.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines

commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

Remarque : Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

Les **commandes show [afficher] utilisées dans le serveur VPN peuvent également vous aider à vérifier l'état du tunnel.**

- La commande **show crypto session [afficher la session avec chiffrement] permet de vérifier l'état du tunnel.** Voici un exemple de sortie pour cette commande.

```
Crypto session current status

Interface: Serial3/0
Session status: UP-ACTIVE
Peer: 172.16.1.20 port 500
  IKE SA: local 192.168.1.11/500 remote 172.16.1.20/500

Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 10.0.0.58
        Active SAs: 2, origin: dynamic crypto map
```

- La commande **show crypto isakmp policy [voir la politique isakmp avec chiffrement] permet d'afficher les paramètres de phase 1.**

Dépannage

Les commandes **debug [débogage] et** show [afficher] expliquées dans la section Verify [vérifier] peuvent également être utilisées pour le dépannage.

- **debug crypto isakmp**
- **debug crypto ipsec**
- **show crypto session [afficher la session avec chiffrement]**

- La commande debug crypto isakmp [débogage d'isakmp avec chiffrement] sur le serveur VPN affiche l'intégralité du processus de négociation de la phase 1 entre le client et le serveur. Voici un exemple d'une négociation réussie de la phase 1.

```
------------------------------------------------------------------
 ----------------------------------------------------------
------------------------------------------------------------------
*Aug 28 10:37:29.515: ISAKMP:(0:0:N/A:0):Checking ISAKMP transform 14
   against priority 1 policy
*Aug 28 10:37:29.515: ISAKMP:      encryption DES-CBC
*Aug 28 10:37:29.515: ISAKMP:      hash MD5
*Aug 28 10:37:29.515: ISAKMP:      default group 2
*Aug 28 10:37:29.515: ISAKMP:      auth pre-share
*Aug 28 10:37:29.515: ISAKMP:      life type in seconds
*Aug 28 10:37:29.515: ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
*Aug 28 10:37:29.515: ISAKMP:(0:0:N/A:0):atts are acceptable. Next payload is 0
*Aug 28
*Aug 28 10:37:29.955: ISAKMP:(0:15:SW:1):SA authentication status:
authenticated
*Aug 28 10:37:29.955: ISAKMP:(0:15:SW:1): Process initial contact,
  bring down existing phase 1 and 2 SA's with local 192.168.1.11
  remote 172.16.1.20 remote port 500
*Aug 28 10:37:29.955: ISAKMP:(0:15:SW:1):returning IP addr to
  the address pool: 10.0.0.57
```

```
*Aug 28 10:37:29.955: ISAKMP (0:134217743): returning address 10.0.0.57 to pool
*Aug 28 10:37:29.959: ISAKMP:(0:14:SW:1):received initial contact, deleting SA
*Aug 28 10:37:29.959: ISAKMP:(0:14:SW:1):peer does not do pade
  1583442981 to QM_IDLE
*Aug 28 10:37:29.963: ISAKMP:(0:15:SW:1):Sending NOTIFY
  RESPONDER_LIFETIME protocol 1
spi 1689265296, message ID = 1583442981
*Aug 28 10:37:29.967: ISAKMP:(0:15:SW:1): sending packet to
  172.16.1.20 my_port 500 peer_port 500 (R) QM_IDLE
*Aug 28 10:37:29.967: ISAKMP:(0:15:SW:1):purging node 1583442981
*Aug 28 10:37:29.967: ISAKMP: Sending phase 1 responder lifetime 86400

*Aug 28 10:37:29.967: ISAKMP:(0:15:SW:1):Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
*Aug 28 10:37:29.967: ISAKMP:(0:15:SW:1):Old State = IKE_R_AM2
  New State = IKE_P1_COMPLETE
```

- La commande debug crypto ipsec [débogage d'IPSec avec chiffrement] sur le serveur VPN affiche la négociation réussie de la phase 1 d'IPSec et la création réussie du tunnel VPN. Voici un exemple :

```
------------------------------------------------------------------------
 ------------------------------------------------------------------
------------------------------------------------------------------------
*Aug 28 10:40:04.267: IPSEC(key_engine): got a queue event with 1 kei messages
*Aug 28 10:40:04.271: IPSEC(spi_response): getting spi 2235082775 for SA
from 192.168.1.11 to 172.16.1.20 for prot 3
*Aug 28 10:40:04.279: IPSEC(key_engine): got a queue event with 2 kei messages
*Aug 28 10:40:04.279: IPSEC(initialize_sas): ,
  (key eng. msg.) INBOUND local= 192.168.1.11, remote= 172.16.1.20,
    local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    remote_proxy= 10.0.0.58/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac  (Tunnel),
    lifedur= 2147483s and 0kb,
    spi= 0x8538A817(2235082775), conn_id= 0, keysize= 0, flags= 0x2
*Aug 28 10:40:04.279: IPSEC(initialize_sas): ,
  (key eng. msg.) OUTBOUND local= 192.168.1.11, remote= 172.16.1.20,
    local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    remote_proxy= 10.0.0.58/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac  (Tunnel),
    lifedur= 2147483s and 0kb,
    spi= 0xFFC80936(4291299638), conn_id= 0, keysize= 0, flags= 0xA
*Aug 28 10:40:04.283: IPSEC(rte_mgr): VPN Route Event create routes for
  peer or rekeying for peer 172.16.1.20
*Aug 28 10:40:04.283: IPSEC(rte_mgr): VPN Route Refcount 1 Serial3/0
*Aug 28 10:40:04.283: IPSEC(rte_mgr): VPN Route Added
  10.0.0.58 255.255.255.255 via 172.16.1.20 in IP DEFAULT TABLE with tag 0
*Aug 28 10:40:04.283: IPSec: Flow_switching Allocated flow for sibling 8000001F
*Aug 28 10:40:04.283: IPSEC(policy_db_add_ident): src 0.0.0.0, dest 10.0.0.58,
  dest_port 0

*Aug 28 10:40:04.287: IPSEC(create_sa): sa created,
  (sa) sa_dest= 192.168.1.11, sa_proto= 50,
    sa_spi= 0x8538A817(2235082775),
    sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2002
*Aug 28 10:40:04.287: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.16.1.20, sa_proto= 50,
    sa_spi= 0xFFC80936(4291299638),
    sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2001
```

Informations connexes

- Présentation du chiffrement IPSec (IP Security)
- Page de support pour Protocole IKE/Négociation Ipsec
- Configuration de la sécurité des réseaux IPSec
- FAQ – Cisco Easy VPN
- Guide de configuration du contrôleur LAN sans fil Cisco, version 4.0
- Exemple de configuration de listes de contrôle d'accès sur un contrôleur de réseau local sans fil
- Contrôleur de réseau local sans fil (WLC) - Forum Aux Questions
- Page de prise en charge du mode sans fil
- Support et documentation techniques - Cisco Systems