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

Contenu

Introduction

Ce document introduit le concept du réseau privé virtuel (VPN) dans un environnement sans fil. Le document explique les configurations impliquées 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 :

- La connaissance de WLCs et comment configurer les paramètres de base WLC
- La connaissance des concepts de Protocole WPA (Wi-Fi Protected Access)
- Connaissance de base de VPN et de ses types
- La connaissance d'IPsec
- Connaissance de base du cryptage, de l'authentification et des algorithmes de hachage disponibles

Composants utilisés

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 léger (LAP) de gamme Cisco 1000
- Cisco 3640 qui exécute la version de logiciel 12.4(8) de Cisco IOS®
- Version 4.8 de Client VPN Cisco

Remarque: Ce document utilise un routeur 3640 en tant que serveur VPN. Afin de prendre en charge plus de fonctionnalités de sécurité avancée, vous pouvez également utiliser un serveur VPN dédié.

Remarque: Pour qu'un routeur agisse en tant que serveur VPN, il doit exécuter un ensemble de caractéristiques qui prend en charge IPsec de base.

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.

Informations générales

Un VPN est un réseau informatique de données privées qui est utilisé pour transmettre sécurisé les données dans un réseau privé par l'infrastructure de télécommunication publique telle que l'Internet. Ce VPN met à jour la confidentialité des données par le recours à un protocole et à des procédures de sécurité de Tunnellisation.

Accès à distance VPN

Une configuration du VPN d'Accès à distance est utilisée pour permettre à des clients de logiciel VPN tels que des utilisateurs nomades pour accéder à sécurisé les ressources de réseau centralisées qui résident derrière un serveur VPN. En terminologies Cisco, ces serveurs VPN et clients s'appellent également le serveur de Solution Cisco Easy VPN et le périphérique distant de Solution Cisco Easy VPN.

Un périphérique distant de Solution Cisco Easy VPN peut être des routeurs Cisco IOS, des dispositifs de sécurité de Cisco PIX, des Cisco VPN 3002 Hardware Client et le Client VPN Cisco. Ils sont utilisés pour recevoir des stratégies de sécurité sur une connexion de tunnel VPN d'un serveur de Solution Cisco Easy VPN. Ceci réduit des configurations requises au site distant. Le Client VPN Cisco est un client logiciel qui peut être installé sur des PC, des ordinateurs portables, et ainsi de suite.

Un serveur de Solution Cisco Easy VPN peut être des routeurs Cisco IOS, des dispositifs de sécurité de Cisco PIX, et des concentrateurs de Cisco VPN 3000.

Ce document utilise le logiciel de Client VPN Cisco qui fonctionne sur un ordinateur portable routeur comme de client vpn et de Cisco 3640 IOS en tant que serveur VPN. Le document emploie la norme d'IPsec pour établir un tunnel VPN entre un client et un serveur.

IPsec

IPsec est un cadre des standards ouverts développés par l'Internet Engineering Task Force (IETF). IPsec fournit la Sécurité pour la transmission des informations confidentielles au-dessus des réseaux non protégés tels que l'Internet.

IPsec fournit le chiffrement de données de réseau au niveau de paquet IP, qui offre une solution de sécurité robuste qui est basée sur des standards. La tâche principale d'IPsec est de permettre l'échange des informations personnelles au-dessus d'une connexion non sécurisée. IPsec emploie le cryptage pour protéger les informations contre l'interception ou l'écoute illicite. Cependant, pour utiliser le cryptage efficacement, les deux interlocuteurs devraient partager un secret qui est utilisé pour le cryptage et le déchiffrement des informations.

IPsec procède par deux étapes pour permettre l'échange confidentiel d'un secret partagé :

- Phase 1 — Manipule la négociation des paramètres de Sécurité requis établir un canal de sécuriser entre deux pairs d'IPsec. Le Phase 1 est généralement mis en application par le protocole d'Échange de clés Internet (IKE). Si le pair distant d'IPsec ne peut pas exécuter l'IKE, vous pouvez employer la configuration manuelle avec des clés pré-partagées pour finir le Phase 1.
- Phase 2 — Utilise le tunnel sécurisé établi dans le Phase 1 pour permuter les paramètres de Sécurité requis pour transmettre réellement des données d'utilisateur. Les tunnels sécurisés utilisés en les deux phases d'IPsec sont basés sur les associations de sécurité (SAS) utilisées à chaque point final d'IPsec. SAS décrivent les paramètres de Sécurité, tels que le type d'authentification et le cryptage que les deux points d'extrémité acceptent d'utiliser.

Les paramètres de Sécurité permutés dans le Phase 2 sont utilisés pour créer un tunnel d'IPsec qui consécutivement est utilisé pour le transfert des données entre le client vpn et le serveur.

Référez-vous à la configuration d'IPSec pour plus d'informations sur IPsec et sa configuration.

Une fois qu'un tunnel VPN est établi entre le client vpn et le serveur, les *stratégies de sécurité définies au serveur VPN sont envoyées au client*. Ceci réduit des configurations requises au côté client.

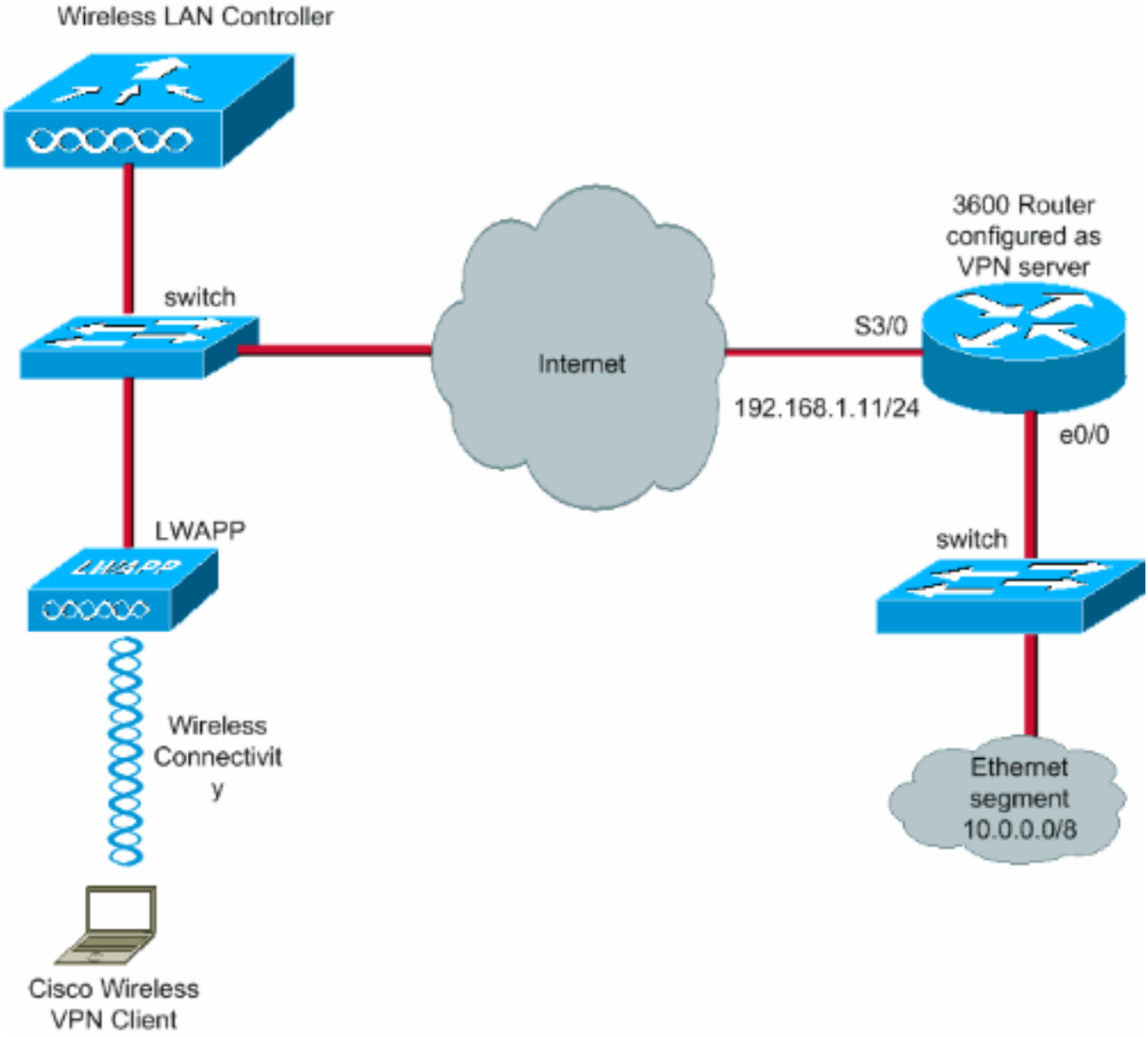
Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour trouver plus d'informations sur les commandes utilisées dans ce document.

Diagramme du réseau

Ce document utilise les configurations suivantes :

- Adresse IP d'interface de gestion du WLC — 172.16.1.10/16
- adresse IP d'interface d'AP-gestionnaire du WLC — 172.16.1.11/16
- Passerelle par défaut — 172.16.1.20/16**Remarque:** Dans un réseau vivant, cette passerelle par défaut devrait indiquer l'interface entrante du routeur immédiat qui connecte le WLC au reste du réseau et/ou à l'Internet.

- Adresse IP du serveur VPN s3/0 — 192.168.1.11/24**Remarque:** Cette adresse IP devrait indiquer l'interface qui termine le tunnel VPN sur le côté de serveur VPN. Dans cet exemple, s3/0 est l'interface qui termine le tunnel VPN au serveur VPN.
- Le segment de RÉSEAU LOCAL au serveur VPN utilise la plage d'adresses IP de 10.0.0.0/8.



Configurer

Dans un WLAN architecture centralisée, afin de permettre à un client vpn Sans fil tel qu'un ordinateur portable d'établir un tunnel VPN avec un serveur VPN, il est nécessaire que le client obtienne associé à un point d'accès léger (LAP) qui consécutivement les besoins d'être inscrit à un WLC. Ce document a le RECOUVREMENT comme déjà inscrit au WLC utilisant le processus de découverte local de diffusion de sous-réseau expliqué dans l'enregistrement léger AP (RECOUVREMENT) à un contrôleur LAN Sans fil (WLC).

L'étape suivante est de configurer le WLC pour le VPN.

Arrêt et intercommunication VPN

Avec la gamme Cisco 4000 WLCs plus tôt que la version 4, une caractéristique appelée l'arrêt d'IPsec VPN (support d'IPsec) est prise en charge. Cette caractéristique permet à ces contrôleurs

de terminer des sessions de client vpn directement sur le contrôleur. En résumé, cette caractéristique permet au contrôleur elle-même d'agir en tant que serveur VPN. Mais ceci exige d'un module de matériel distinct d'arrêt VPN d'être installé dans le contrôleur.

Ce support d'IPsec VPN n'est pas disponible dans :

- Gamme Cisco 2000 WLC
- Tout WLCs cette version 4.0 ou ultérieures de passage

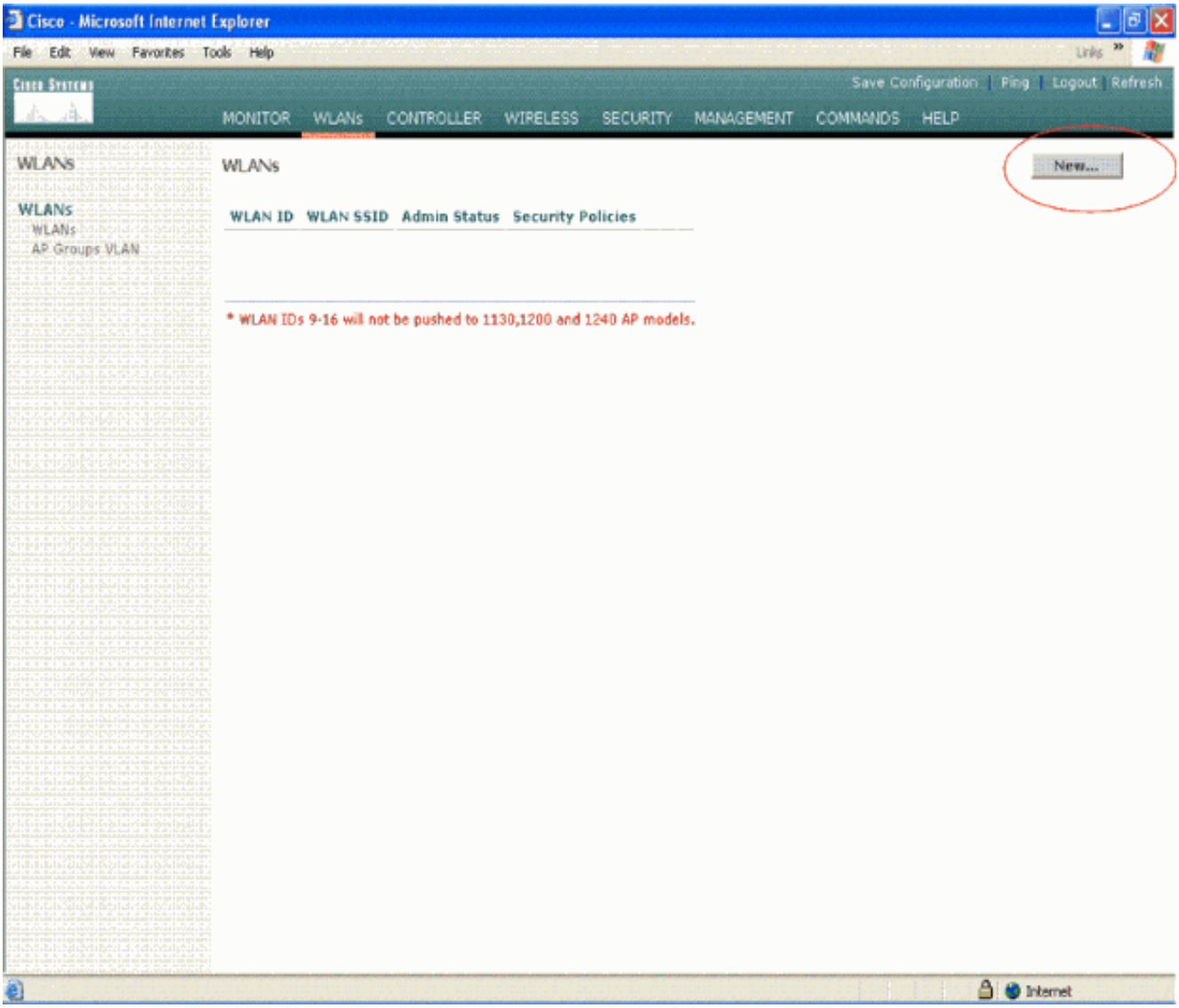
Par conséquent, la seule caractéristique VPN prise en charge dans les versions plus tard que 4.0 est intercommunication VPN. Cette caractéristique est également prise en charge dans la gamme Cisco 2000 WLC.

L'intercommunication VPN est une caractéristique qui permet à un client pour établir un tunnel seulement avec un serveur VPN spécifique. Ainsi, si vous devez accéder à sécurisé un serveur VPN configuré aussi bien qu'un serveur VPN différent ou un Internet, ce n'est pas possible avec l'intercommunication VPN activée sur le contrôleur. Sous de telles conditions requises, vous devez désactiver l'intercommunication VPN. Cependant, le WLC peut être configuré pour agir en tant que fonction émulation afin d'atteindre de plusieurs passerelles VPN quand un ACL approprié est créé et appliqué au WLAN correspondant. Ainsi, sous de tels scénarios où vous voulez atteindre de plusieurs passerelles VPN pour la Redondance, désactivez le relais VPN et créez un ACL qui permet l'accès aux passerelles VPN et vous appliquez l'ACL au WLAN.

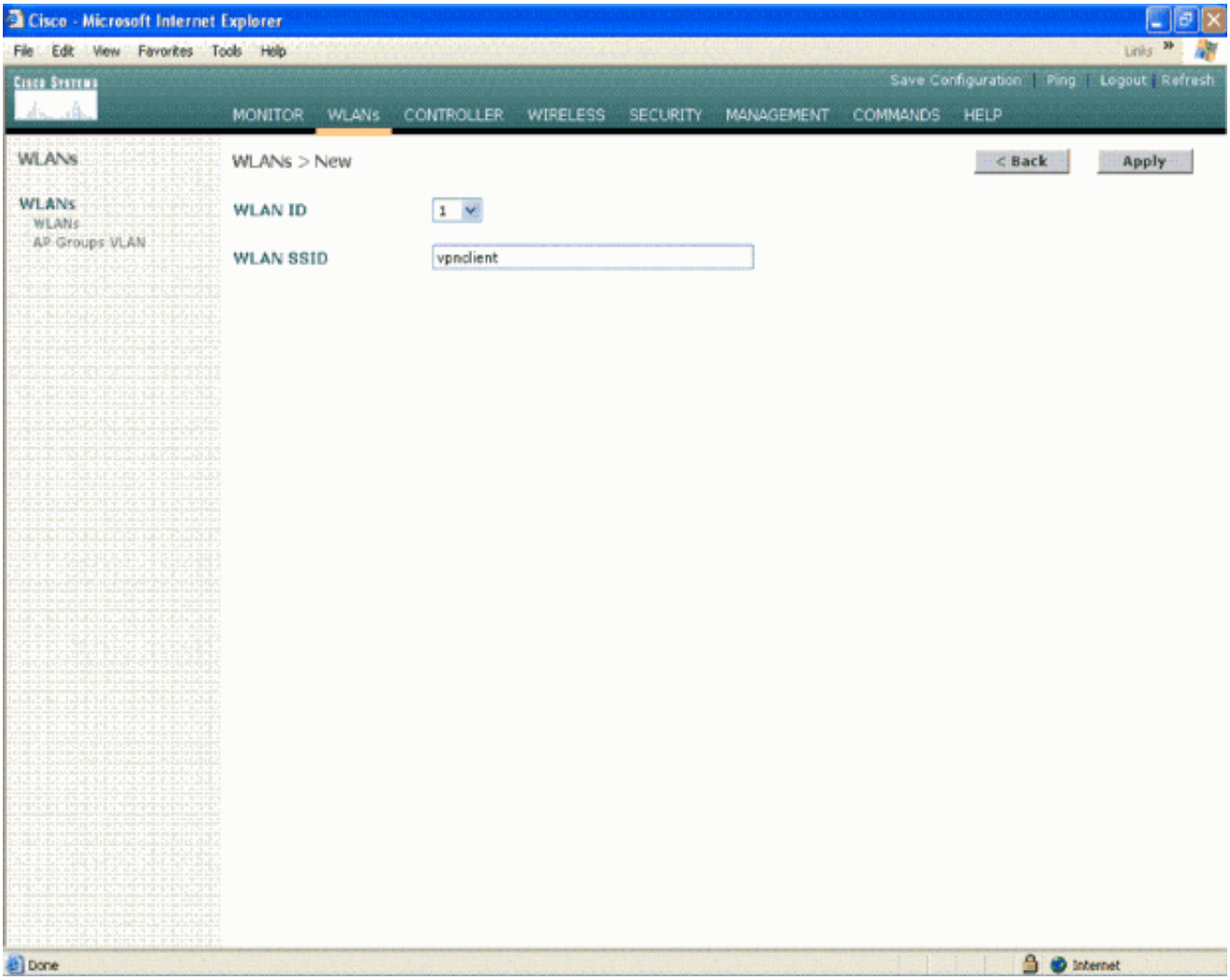
Configurez le WLC pour l'intercommunication VPN

Terminez-vous ces étapes afin de configurer l'intercommunication VPN.

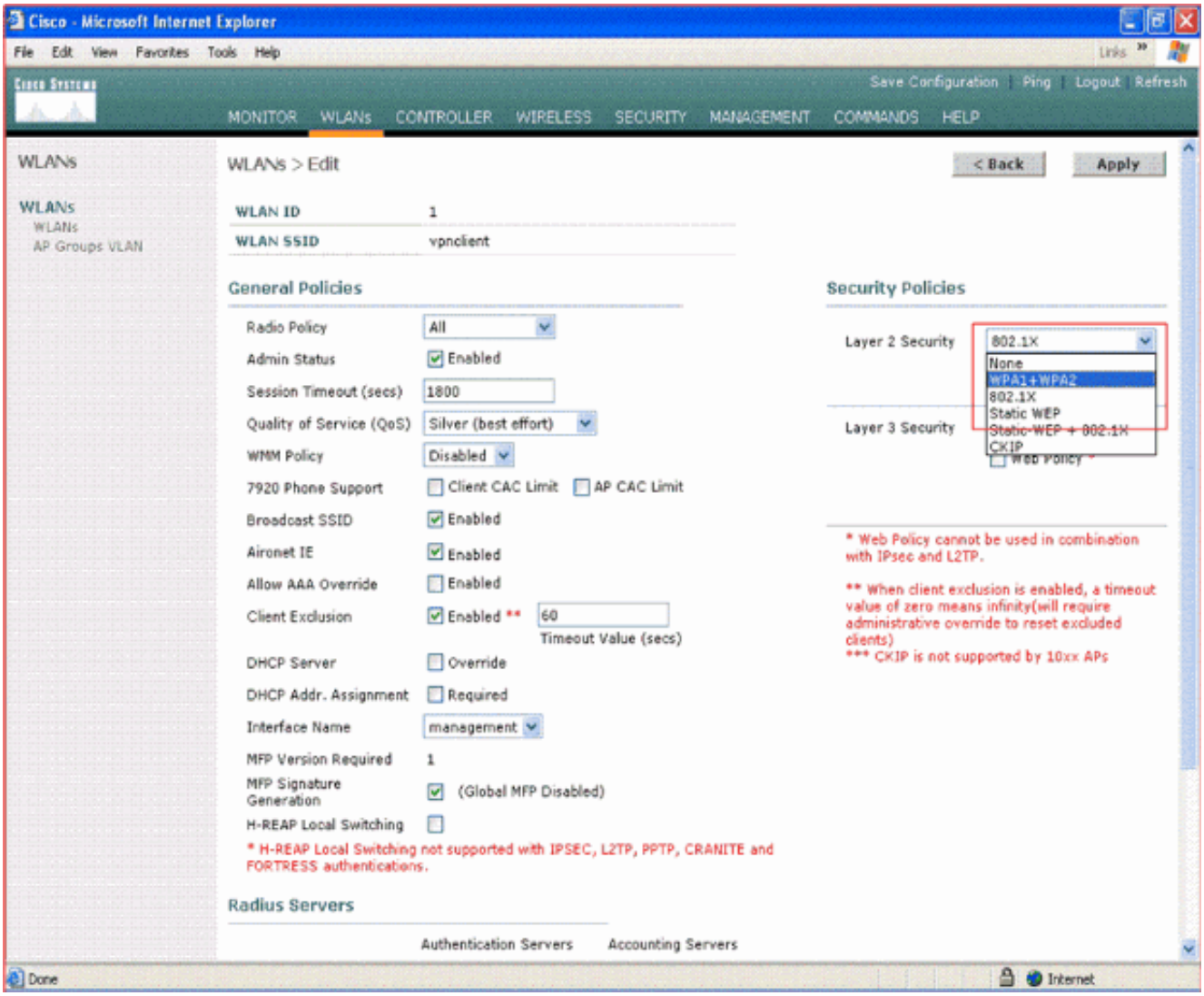
1. Du GUI WLC, clic **WLAN** afin d'aller aux WLAN la page.
2. Cliquez sur New afin de créer un nouveau WLAN.



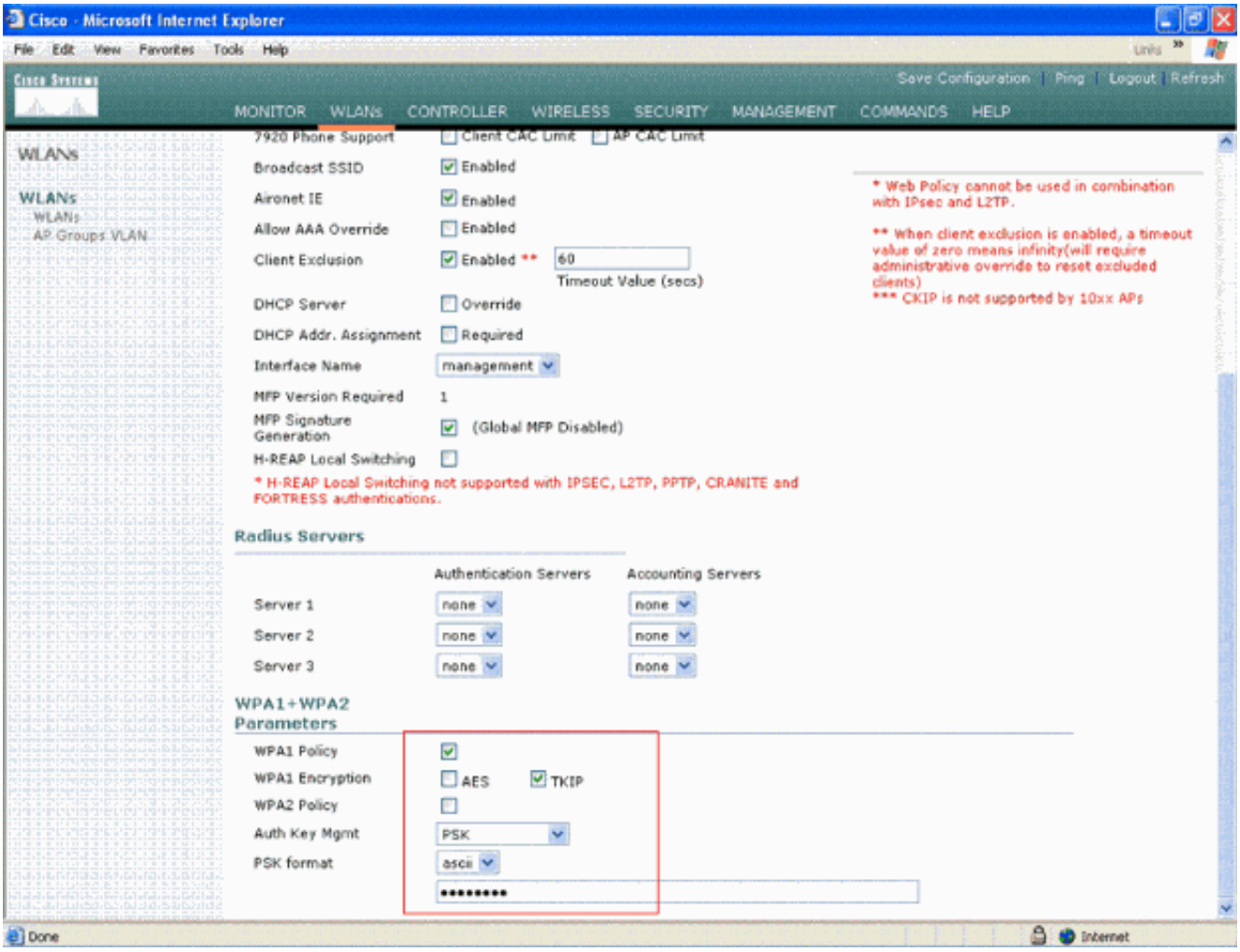
3. Le WLAN SSID est nommé comme **vpnclient** dans cet exemple. Cliquez sur **Apply**.



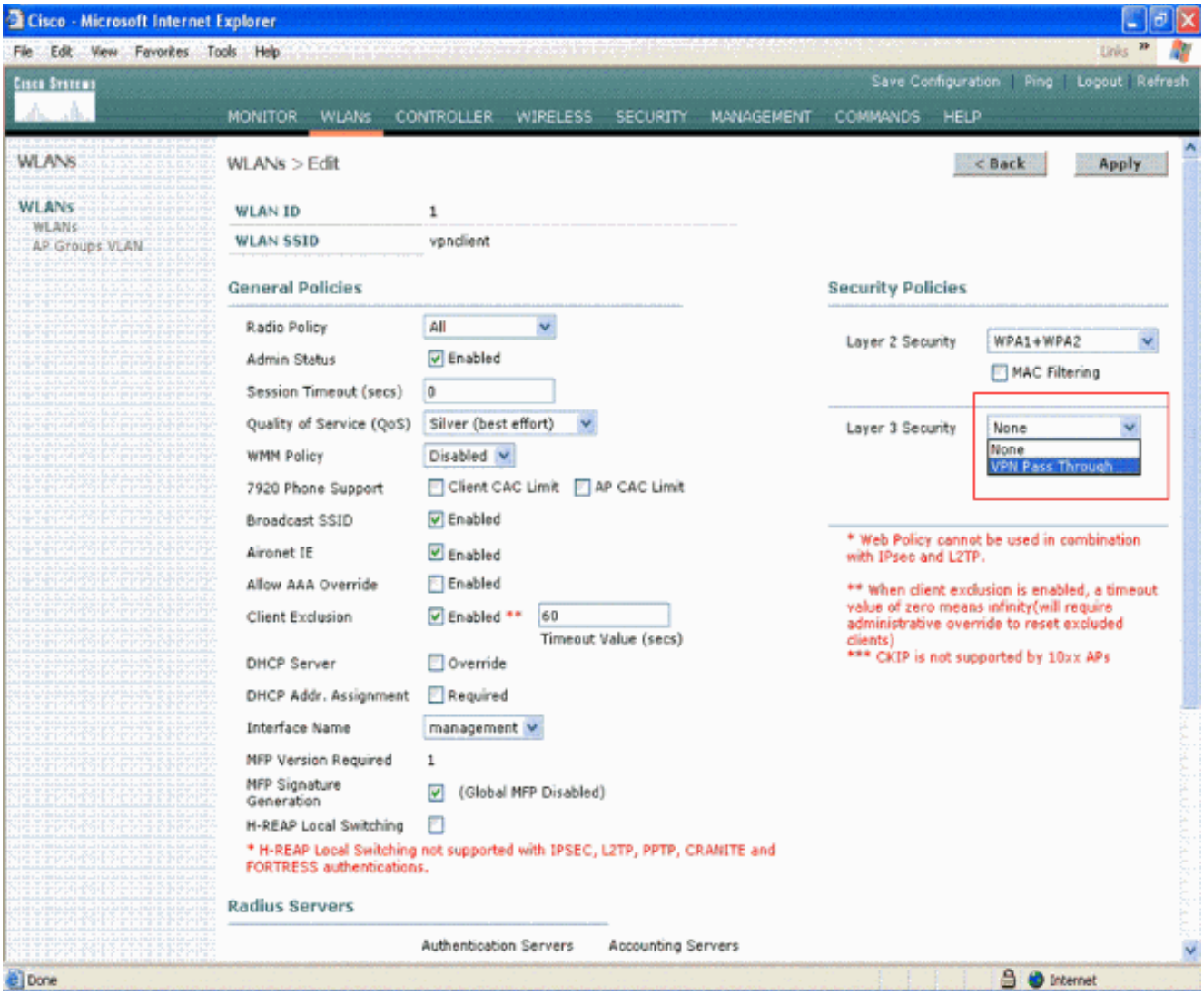
4. Configurez le SSID vpnclient avec le degré de sécurité de la couche 2. *C'est facultatif.*Cet exemple utilise **WPA1+WPA2** comme type de
Sécurité.



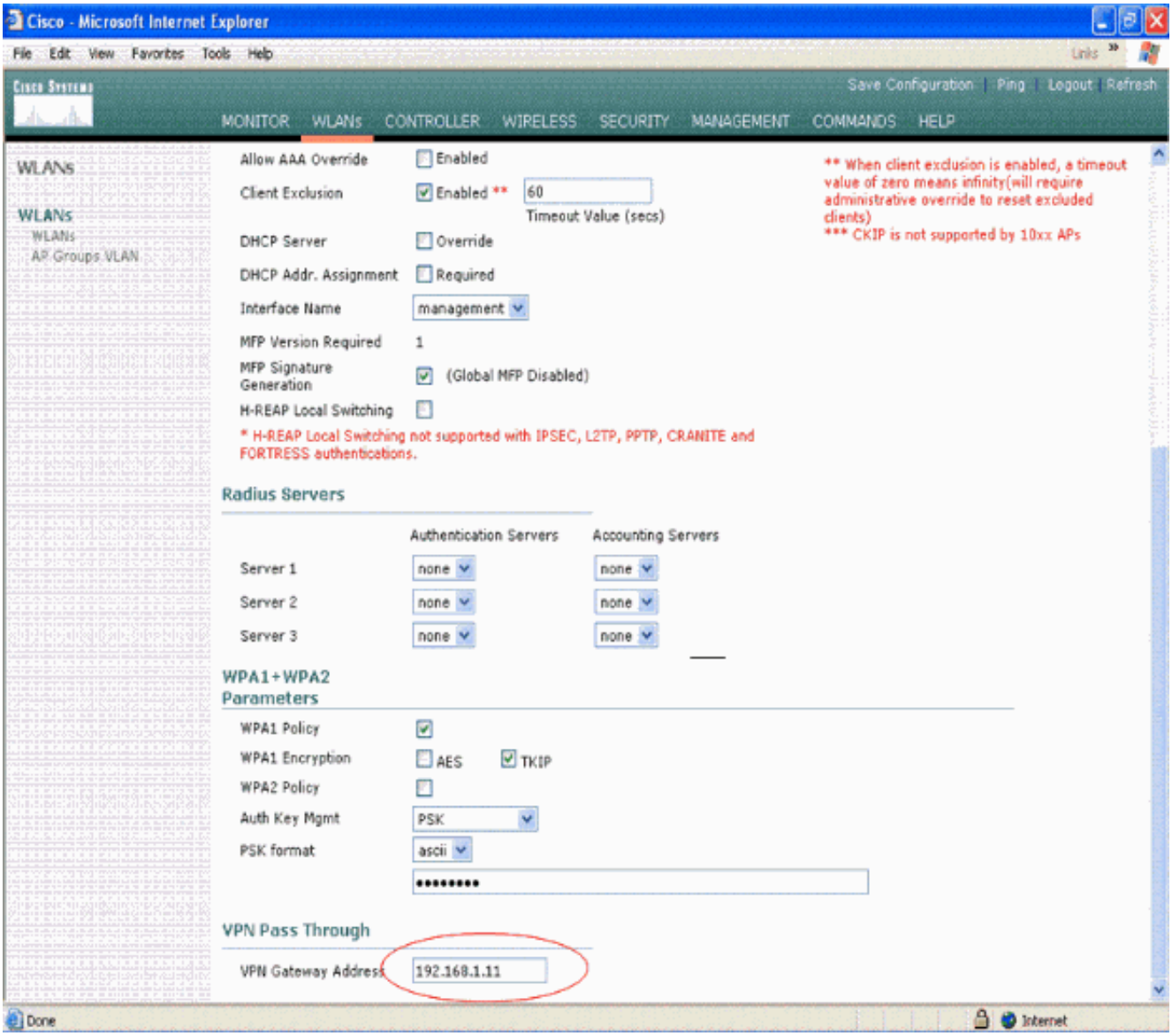
5. Configurez la stratégie WPA et le type de gestion des clés d'authentification à utiliser.Cet exemple utilise la **clé pré-partagée (PSK)** pour la gestion des clés d'authentification. Une fois que PSK est sélectionné, l'**ASCII** choisie comme format PSK et tapent la valeur PSK. Cette valeur devrait être identique dans la configuration SSID du client sans fil afin des clients qui appartiennent à ce SSID pour s'associer avec ce
WLAN.



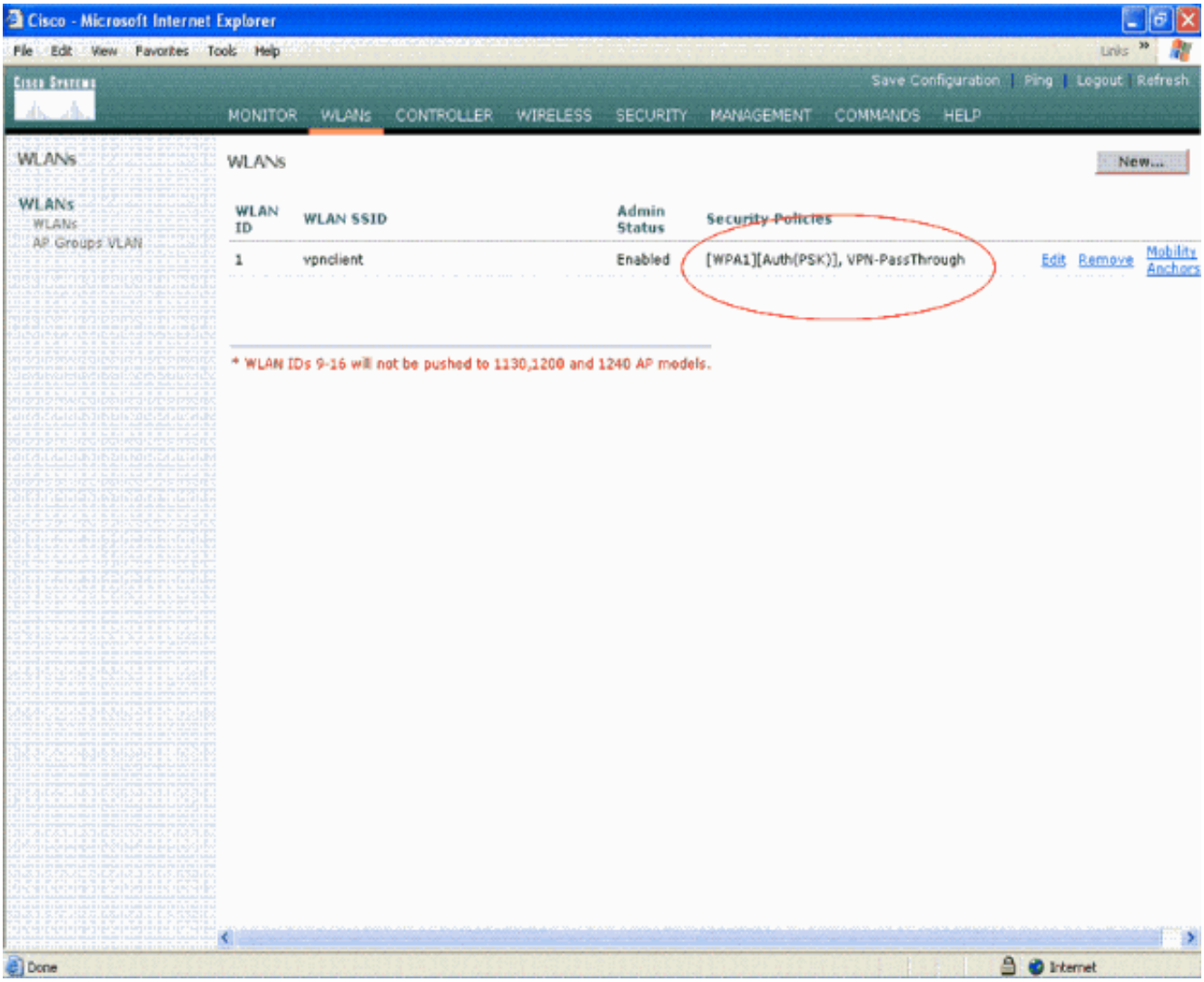
6. **Intercommunication** choisie **VPN** comme degré de sécurité de la couche 3. Voici l'exemple.



7. Une fois que l'intercommunication VPN est sélectionnée comme degré de sécurité de la couche 3, ajoutez le comme indiqué dans cet exemple d'adresse de passerelle VPN.Cette adresse de passerelle devrait être l'adresse IP de l'interface qui termine le tunnel VPN au côté serveur. Dans cet exemple, l'adresse IP de l'interface s3/0 (192.168.1.11/24) au serveur VPN est l'adresse de passerelle à
configurer.



8. Cliquez sur **Apply**. Le WLAN appelé *vpnclient* est maintenant configuré pour l'intercommunication
VPN.



Configuration de serveur VPN

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

Remarque: Pour la simplicité, cette configuration emploie le routage statique pour mettre à jour l'accessibilité par IP entre les points d'extrémité. Vous pouvez employer n'importe quel protocole de routage dynamique tel que le Protocole RIP (Routing Information Protocol), Protocole OSPF (Open Shortest Path First), et ainsi de suite pour mettre à jour l'accessibilité.

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

Remarque: Ce document suppose que l'utilisateur se rend compte de la façon 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 seulement l'authentification de groupe. Il n'utilise pas l'Individual User Authentication.

Configuration du client VPN

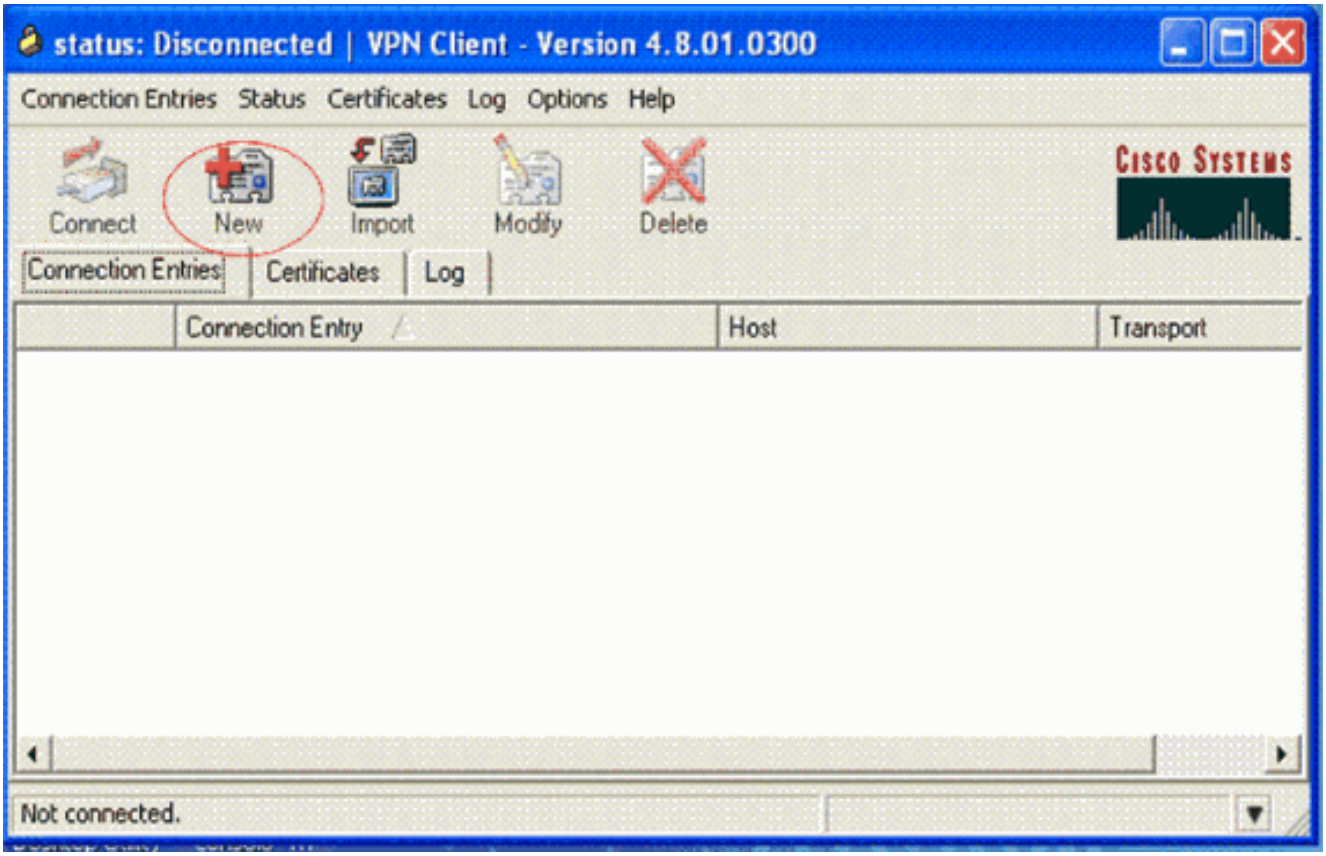
Un client vpn de logiciel peut être téléchargé du centre de logiciel de Cisco.com.

Remarque: Du logiciel de Cisco exige de vous d'ouvrir une session avec un nom d'utilisateur et mot de passe CCO.

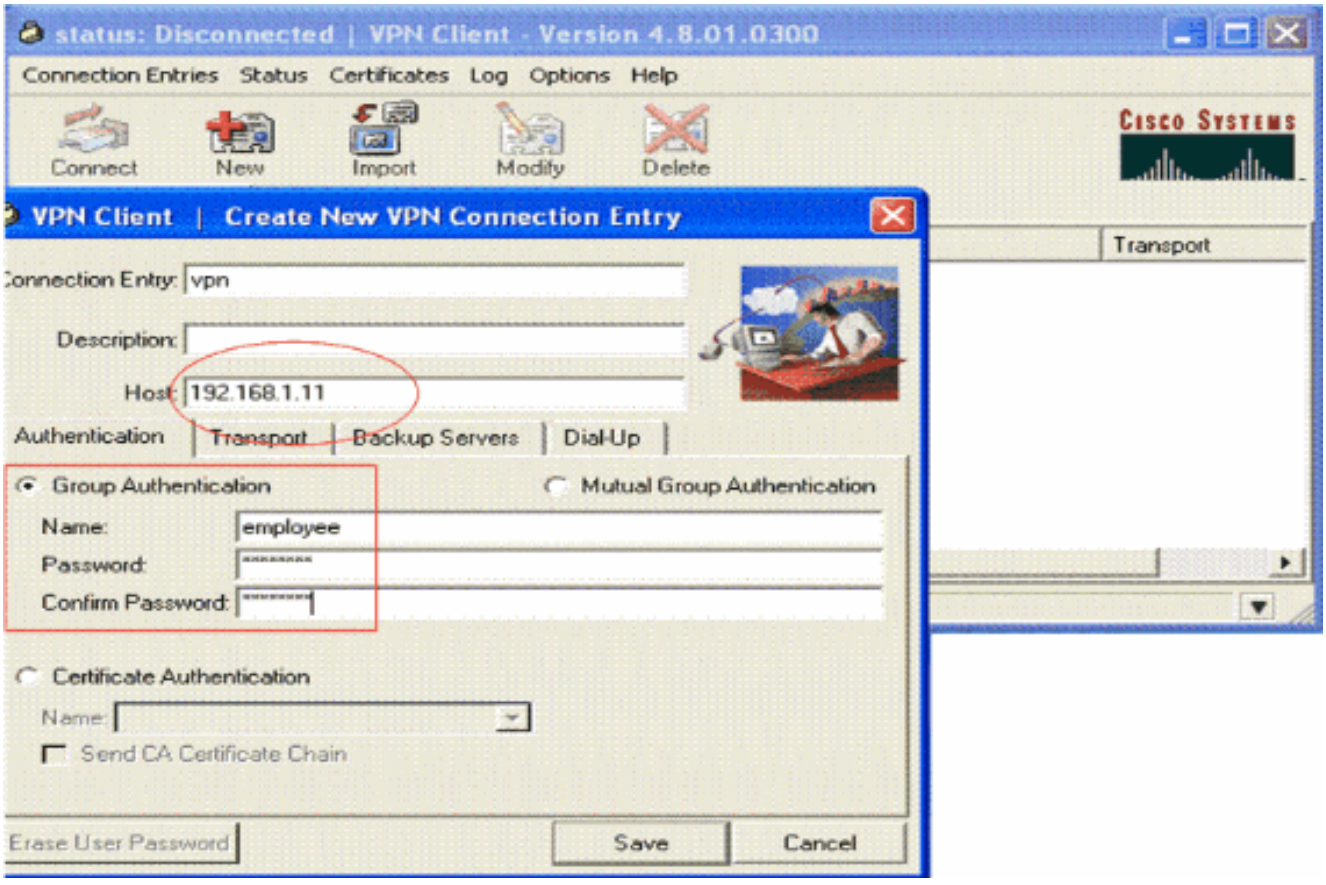
Exécutez les étapes suivantes afin de configurer le client VPN.

1. Formez votre client sans fil (ordinateur portable), choisissez le **début > les programmes > le client vpn de Cisco Systems > le client vpn** afin d'accéder au client vpn. C'est l'emplacement par défaut où le client vpn est installé.
2. Cliquez sur New afin de lancer la nouvelle fenêtre d'entrée de connexion VPN de

création.



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



Remarque: Le nom et le mot de passe configuré de groupe ici devraient être identique que celui configuré dans le serveur VPN. Cet exemple utilise l'*employé* et le mot de passe

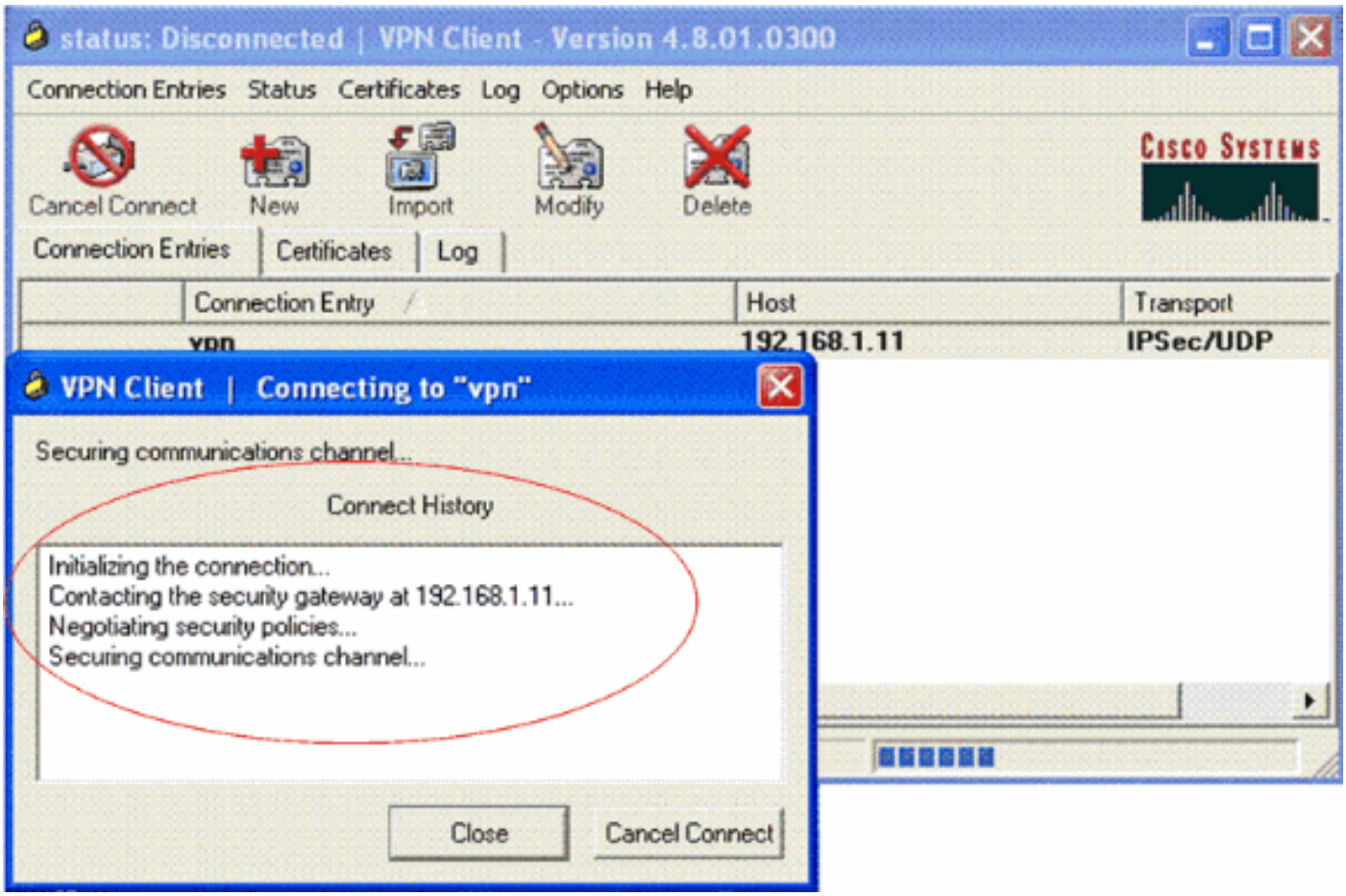
cisco123 de nom.

Vérifier

Afin de vérifier cette configuration, configurez le SSID **vpnclient** dans le client sans fil avec les mêmes paramètres de Sécurité configurés dans le WLC et associez le client à ce WLAN. Il y a plusieurs documents qui expliquent comment configurer un client sans fil avec un nouveau profil.

Une fois que le client sans fil est associé, allez au client vpn et cliquez sur en fonction la connexion que vous avez configurée. Cliquez sur alors **se connectent de la** fenêtre principale de client vpn.

Vous pouvez des paramètres voir de Phase 1 et de Phase 2 Sécurité négociés entre le client et le serveur.



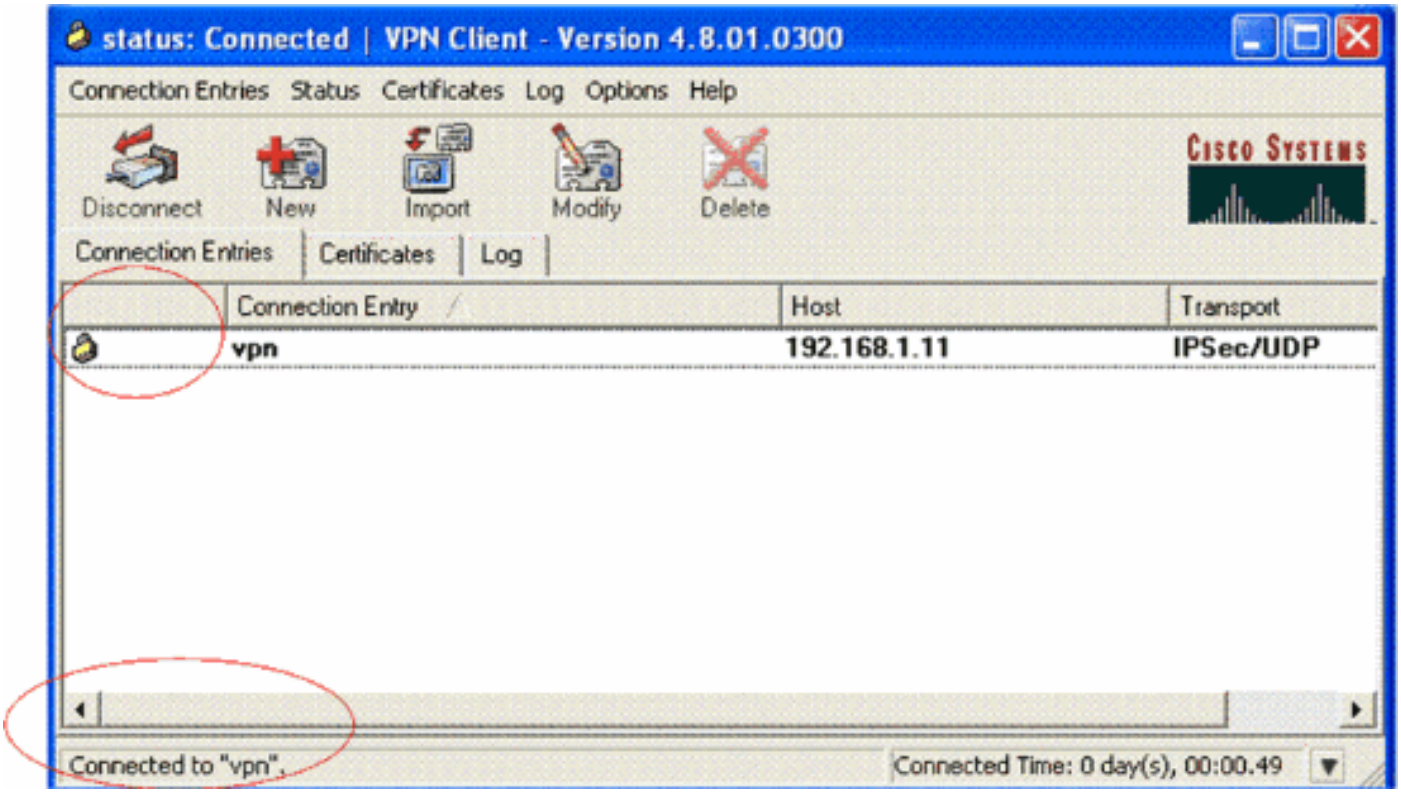
Remarque: Afin d'établir ce tunnel VPN, le client vpn et le serveur devraient avoir l'accessibilité par IP entre eux. Si le client vpn ne peut pas entrer en contact avec la passerelle de sécurité (serveur VPN), alors le tunnel n'est pas établi et une case vigilante est affichée au côté client avec ce message :

```
vpnrouter#show running-config

Building configuration...

Current configuration : 1623 bytes
!
version 12.4
```

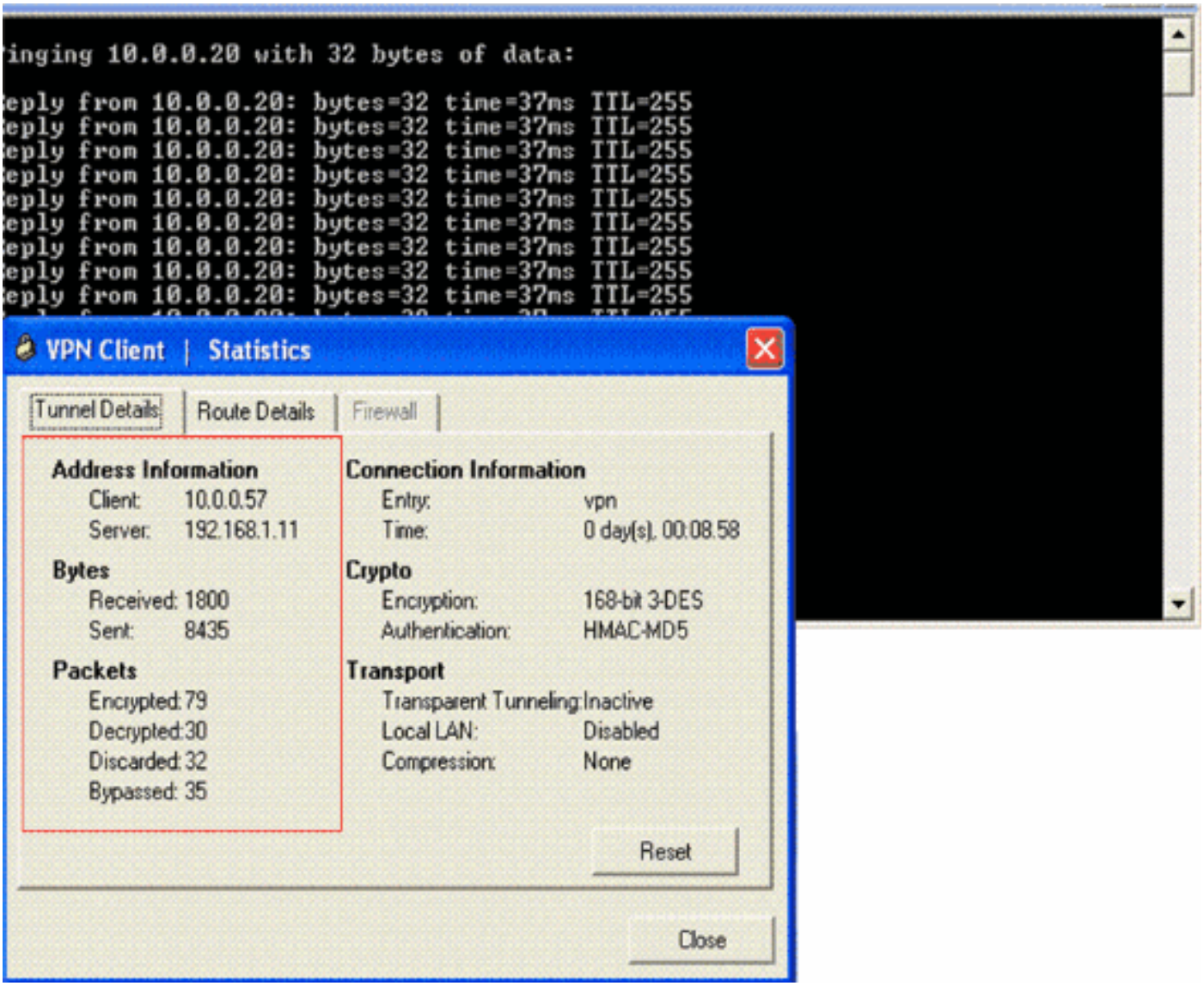
```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname vpnrouter
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
!
aaa authorization network employee local
!
aaa session-id common
!
resource policy
!
memory-size iomem 10
!
!
ip 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
```

Afin de s'assurer qu'un tunnel VPN est correctement établi entre le client et serveur, vous pouvez trouver une icône de verrouillage qui est créée à côté du client vpn établi. La barre d'état indique également **connecté au « vpn »**. Voici un exemple.



En outre, assurez-vous que vous pouvez transmettre avec succès des données au segment de RÉSEAU LOCAL au côté serveur du client vpn et vice-versa. Du menu principal de client vpn, choisissez le **Status > Statistics**. Là vous pouvez trouver les statistiques des paquets chiffrés et déchiffrés qui sont traversés le tunnel.



Dans ce tir d'écran, vous pouvez voir l'adresse du client comme 10.0.0.57. C'est l'adresse que le serveur VPN assigne au client de son groupe localement configuré après négociation réussie de Phase 1. Une fois que le tunnel est établi, le serveur VPN ajoute automatiquement une artère à cette adresse IP assignée DHCP dans sa table de routage.

Vous pouvez également voir le nombre de paquets chiffrés augmentant tandis que les données sont transférées du client vers le serveur et le nombre de paquets déchiffrés augmentant pendant un transfert des données inverse.

Remarque: Puisque le WLC est configuré pour l'intercommunication VPN, il permet au client d'accéder à seulement le segment lié à la passerelle VPN (ici, c'est serveur VPN de 192.168.1.11) configurée pour l'intercommunication. Ceci filtre tout autre trafic.

Vous pouvez vérifier ceci en configurant un autre serveur VPN avec la même configuration et configurer une nouvelle entrée de connexion pour ce serveur VPN au client vpn. Maintenant, quand vous essayez d'établir un tunnel avec ce serveur VPN, il n'est pas réussi. C'est parce que le WLC filtre ce trafic et permet un tunnel seulement à l'adresse de passerelle VPN configurée pour l'intercommunication VPN.

Vous pouvez également vérifier la configuration du 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: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

Ces **commandes show** utilisées dans le serveur VPN pourraient également être utiles pour vous aider à vérifier l'état de tunnel.

- L'ordre de **show crypto session** est utilisé de vérifier l'état de tunnel. Voici un exemple de sortie de 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
```

- **Le show crypto isakmp policy** est utilisé pour visualiser les paramètres configurés de Phase 1.

Dépanner

Le débogage et les **commandes show** expliqués dans la section de vérifier peuvent également être utilisés pour dépanner.

- debug crypto isakmp
- debug crypto ipsec
- **show crypto session**

- La commande de **debug crypto isakmp au** serveur VPN affiche le procédé entier de négociation de Phase 1 entre le client et le serveur. Voici un exemple d'une négociation réussie de 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 de **debug crypto ipsec au** serveur VPN affiche la négociation IPSec de Phase 1 et la création réussies 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
- Sécurité des réseaux de configuration d'IPSec
- Solution Cisco Easy VPN Q&A
- 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