Exemple de configuration de client VPN AnyConnect (SSL) sur routeur IOS avec CCP

Contenu

Introduction

Ce document décrit comment installer un routeur de Cisco IOS® pour exécuter le VPN SSL sur un bâton avec le Cisco AnyConnect VPN Client utilisant le Cisco Configuration Professional (CCP). Cette configuration s'applique à un cas spécifique dans lequel le routeur n'autorise pas la transmission tunnel partagée et où les utilisateurs se connectent directement au routeur avant d'être autorisés à accéder à Internet.

Le technologie VPN SSL ou WebVPN est prise en charge sur les plate-formes de routeur IOS suivantes :

- 870, 1811, 1841, 2801, 2811, 2821, 2851
- 3725, 3745, 3825, 3845, 7200 et 7301

CCP est un outil de gestion des périphériques basé sur GUI vous permettant de configurer les routeurs d'accès basés sur Cisco IOS, y compris les routeurs à services intégrés Cisco, les routeurs de la gamme Cisco 7200 et le routeur Cisco 7301. CCP s'installe sur un PC et simplifie la configuration du routeur, de la sécurité, des communications unifiées, du réseau WAN sans fil ainsi que la configuration LAN de base, à l'aide d'assistants conviviaux basés sur GUI.

Les routeurs commandés avec CCP sont livrés avec Cisco Configuration Professional Express (CCP Express) installé dans la mémoire Flash du routeur. CCP Express est une version light de CCP. Vous pouvez utiliser CCP Express pour configurer les fonctions de sécurité de base sur les interfaces LAN et WAN du routeur. CCP Express est disponible dans la mémoire Flash du routeur.

Conditions préalables

Conditions requises

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

- Microsoft Windows 2000 ou XP ;
- Navigateur Web avec SUN JRE 1.4 (ou version ultérieure) ou navigateur contrôlé par ActiveX ;
- Privilèges administratifs locaux sur le client ;
- Routeur Cisco IOS avec image Advanced Security -12.4(20)T (ou version ultérieure) ;
- Cisco Configuration Professional 1.3

Si Cisco Configuration Professional n’est pas encore chargé sur votre ordinateur, vous pouvez obtenir une copie gratuite et installer le fichier .exe (cisco-config-pro-k9-pkg-1_3-en.zip) à partir de la section Téléchargement de logiciel. Pour obtenir des informations détaillées sur l’installation et la configuration de CCP, reportez-vous au Guide de démarrage rapide Cisco Configuration Professional.

Composants utilisés

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

- Routeur de la gamme Cisco IOS 1841 avec version logicielle 12.4(24)T
- Cisco Configuration Professional (CCP) +1.3
- Client VPN SSL Cisco AnyConnect version pour Windows 2.3.2016

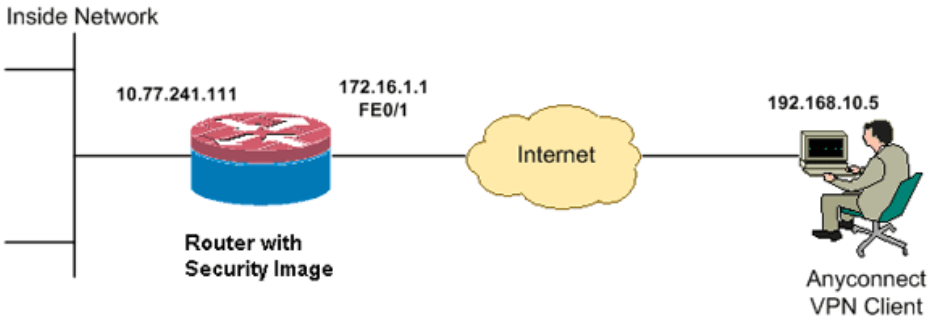
Remarque: Les informations contenues dans ce document ont été créées à partir des périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que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

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Tâches de préconfiguration

1. Vous devez configurer le routeur pour CCP.

   Les routeurs possédant la licence de sécurité appropriée ont déjà l’application CCP chargée en Flash. Pour obtenir et configurer le logiciel, reportez-vous au Guide de démarrage rapide Cisco Configuration Professional.
2. Téléchargez une copie du fichier Anyconnect VPN .pkg sur votre ordinateur de gestion.

Configurer Anyconnect VPN sur IOS

Cette section vous indique les étapes nécessaires pour configurer les fonctionnalités décrites dans ce document. Cet exemple de configuration utilise l’assistant CCP pour activer le fonctionnement de Anyconnect VPN sur le routeur IOS.

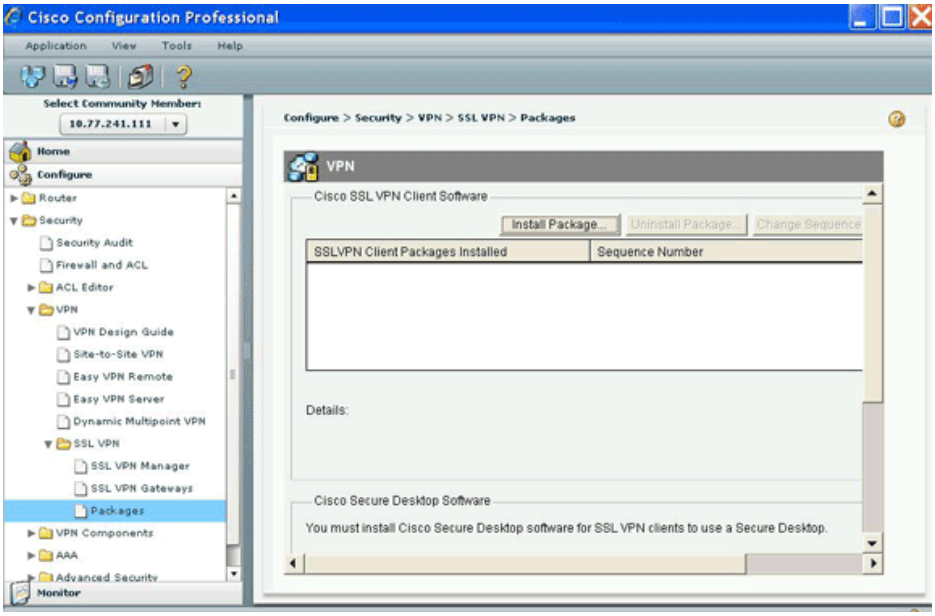
Exécutez ces étapes afin de configurer Anyconnect VPN sur le routeur Cisco IOS :

1. Installer et activer le logiciel Anyconnect VPN sur le routeur Cisco IOS
2. Configurer un contexte VPN SSL et une passerelle VPN SSL à l’aide de l’assistant CCP
3. Configurer la base de données utilisateur pour les utilisateurs d’Anyconnect VPN
4. Configurer les ressources à présenter aux utilisateurs

Étape 1. Installez et activez le logiciel Anyconnect VPN sur le routeur IOS

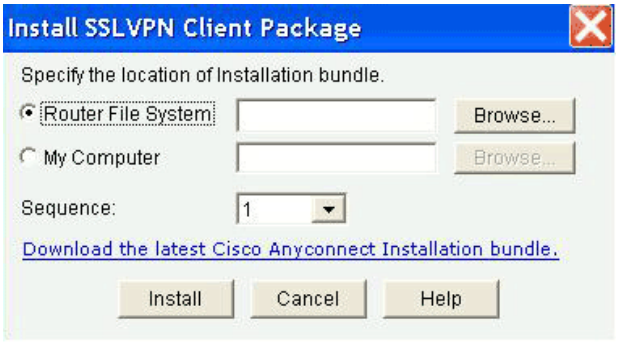
Pour installer et activer le logiciel Anyconnect VPN sur le routeur IOS, effectuez les étapes suivantes :

1. Ouvrez l’application CCP, accédez à **Configure > Security**, puis cliquez sur **VPN**.
2. Développez **SSLVPN**, puis sélectionnez **Packages**.



3. Dans le logiciel client Cisco SSLVPN, cliquez sur **Browse**.

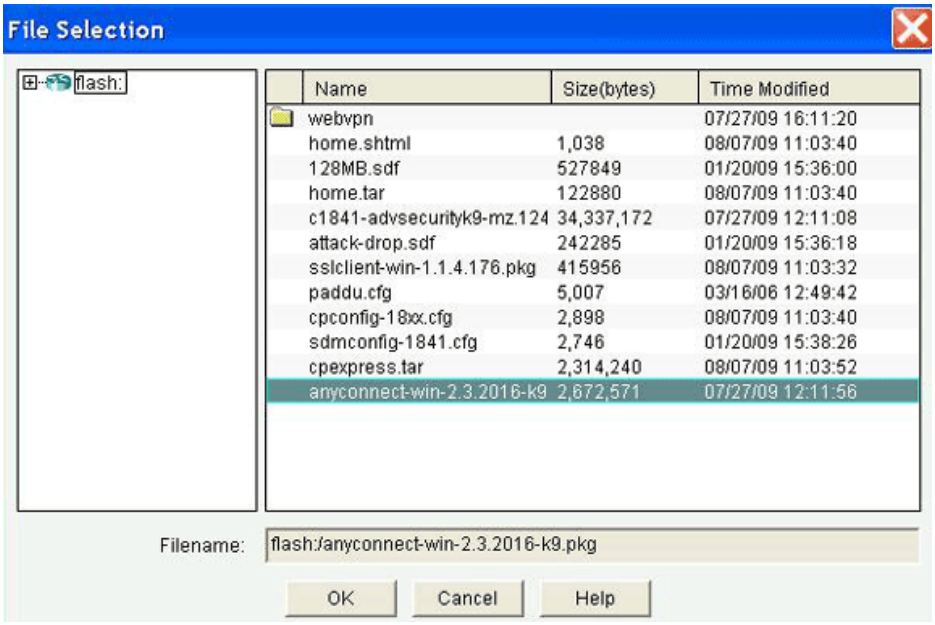
   La boîte de dialogue « Install SSL VPN Client Package » (Installer le package client VPN SSL) s'affiche.



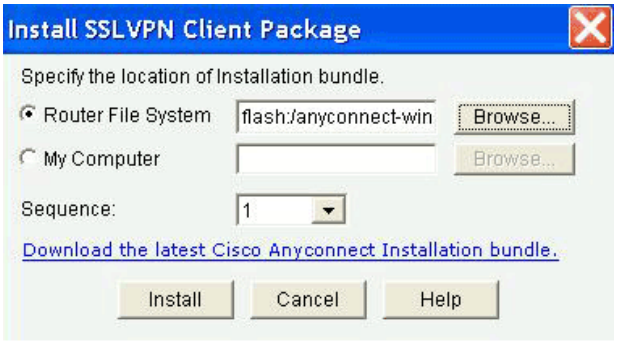
4. Spécifiez l'emplacement de l'image Cisco AnyConnect VPN Client.

   - Si l'image Cisco Anyconnect VPN se trouve dans la mémoire Flash du client, cliquez sur la case d'option **Router File System**, puis cliquez sur **Browse**.
   - Si l'image Cisco Anyconnect VPN Client ne se trouve pas dans la mémoire Flash du routeur, cliquez sur la boîte de dialogue **My Computer**, puis cliquez sur **Browse**.

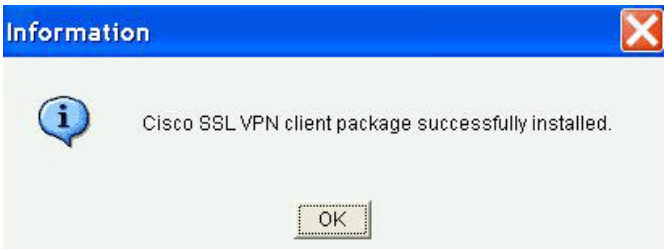
   La boîte de dialogue File Selection (Sélection de fichier) s'affiche.



5. Sélectionnez l'image client que vous souhaitez installer, puis cliquez sur **OK**.



6. Une fois que vous avez spécifié l'emplacement de l'image client, cliquez sur **Install**.
7. Cliquez sur **Yes**, puis cliquez sur **OK**.
8. Une fois l'image client correctement installée, le message suivant s'affiche :

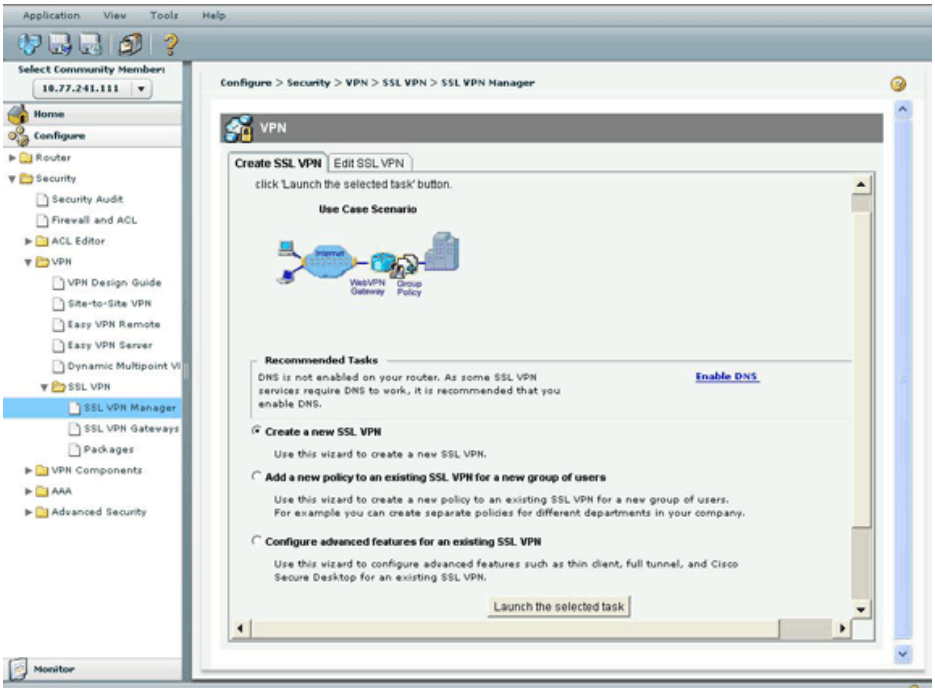


9. Cliquez sur **OK** pour continuer.

Étape 2. Configurez un contexte SSLVPN et la passerelle SSLVPN avec l'assistant CCP

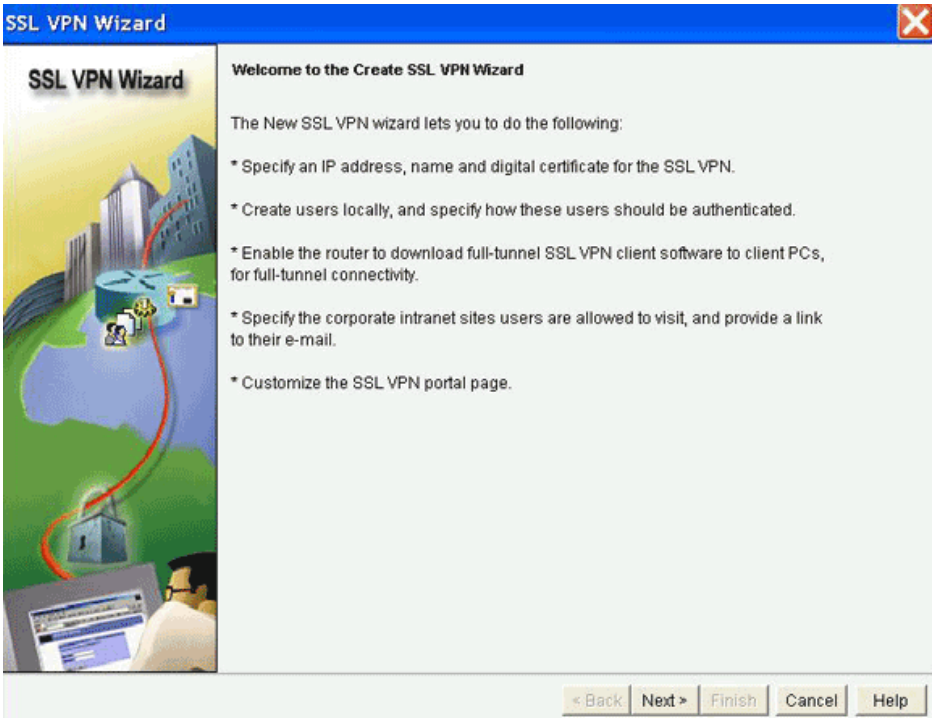
Exécutez les étapes suivantes pour configurer un contexte VPN SSL et une passerelle VPN SSL :

1. Accédez à **Configure > Security > VPN**, puis cliquez sur **SSL VPN**.
2. Cliquez sur **SSL VPN Manager** (Gestionnaire VPN SSL), puis cliquez sur l'onglet **Create SSL VPN** (Créer VPN SSL).

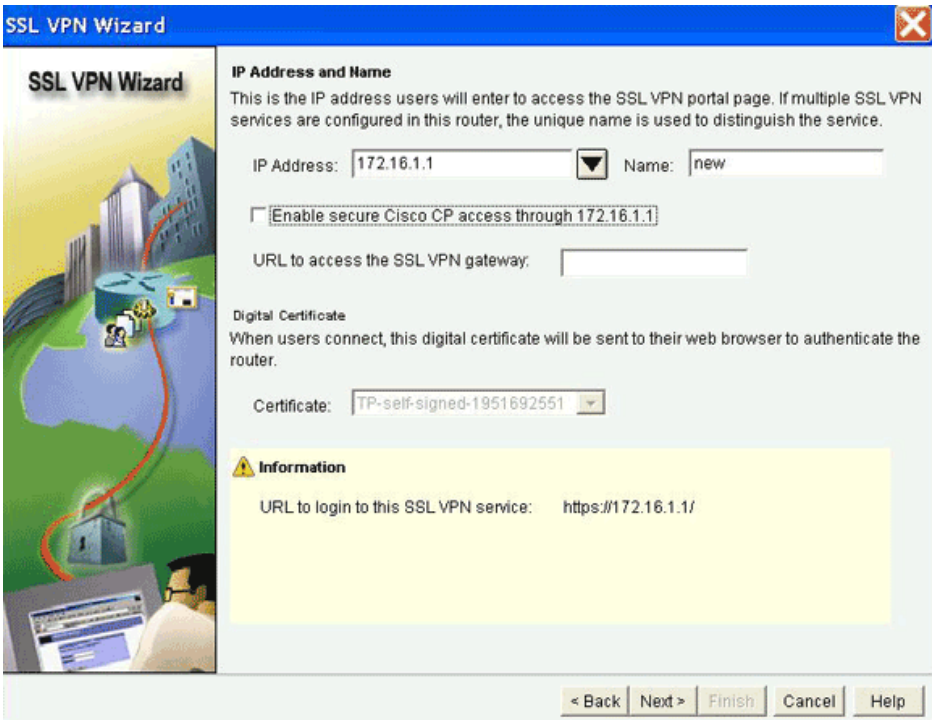


3. Cliquez sur la case d'option **Create a New SSL VPN**, puis cliquez sur **Launch the selected task**.

   La boîte de dialogue de l'Assistant VPN SSL s'affiche.



4. Cliquez sur **Next** (Suivant).



5. Saisissez l’adresse IP de la nouvelle passerelle VPN SSL, puis saisissez un nom unique pour ce contexte VPN SSL.

   Vous pouvez créer différents contextes VPN SSL pour la même adresse IP (passerelle VPN SSL), cependant, chaque nom doit être unique. Cet exemple utilise l’adresse IP suivante : *https://172.16.1.1/*

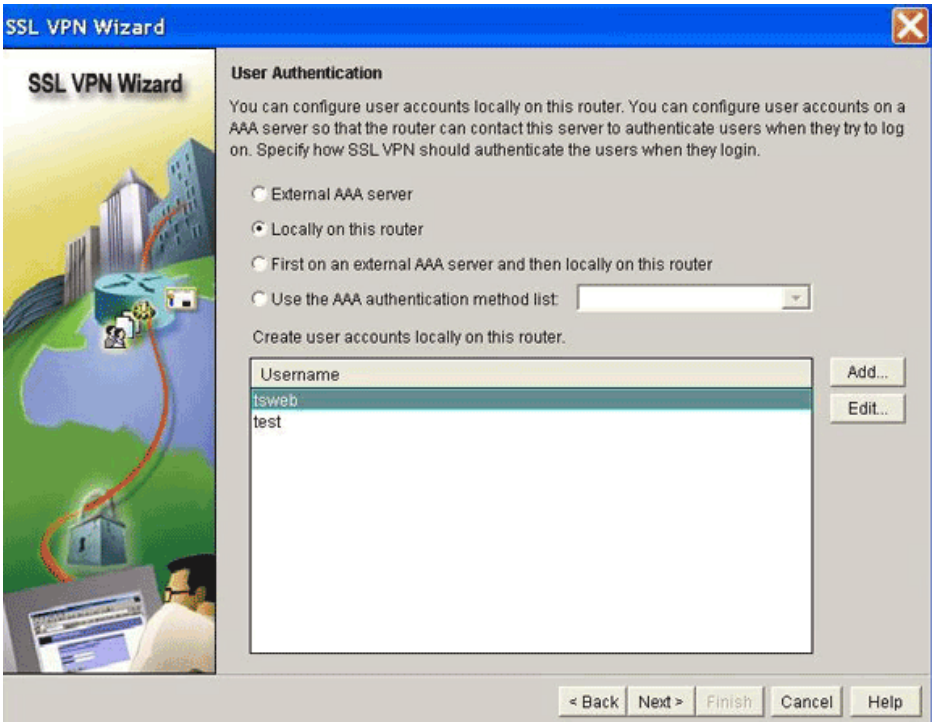
6. Cliquez sur **Next**, puis passez à l’Étape 3.

Étape 3. Configurez la base de données utilisateur pour des utilisateurs d'Anyconnect VPN

Pour l’authentification, vous pouvez utiliser un serveur AAA, des utilisateurs locaux ou les deux. Cet exemple de configuration utilise des utilisateurs créés localement pour l’identification.

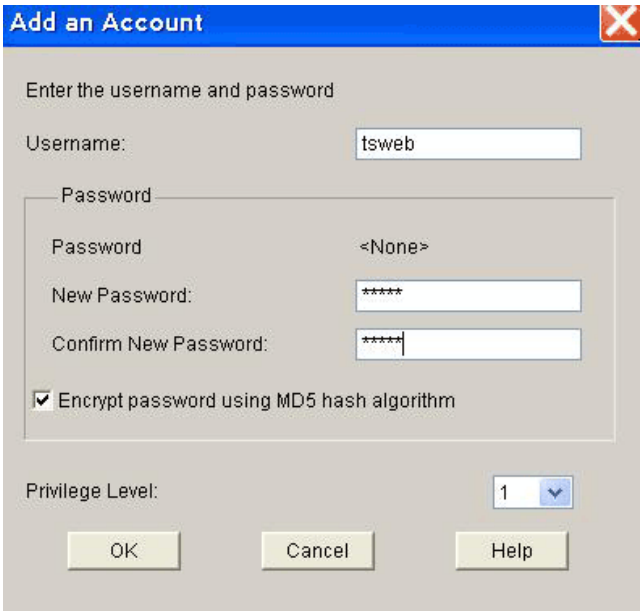
Effectuez les étapes suivantes pour configurer la base de données utilisateur pour les utilisateurs d’Anyconnect VPN :

1. Une fois que vous avez terminé l’Étape 2, cliquez sur la case d’option **Locally on this router** située dans la boîte de dialogue User Authentication de l’Assistant SSL VPN.



Cette boîte de dialogue vous permet d'ajouter des utilisateurs à la base de données locale.

2. Cliquez sur **Add**, puis saisissez les informations utilisateur.

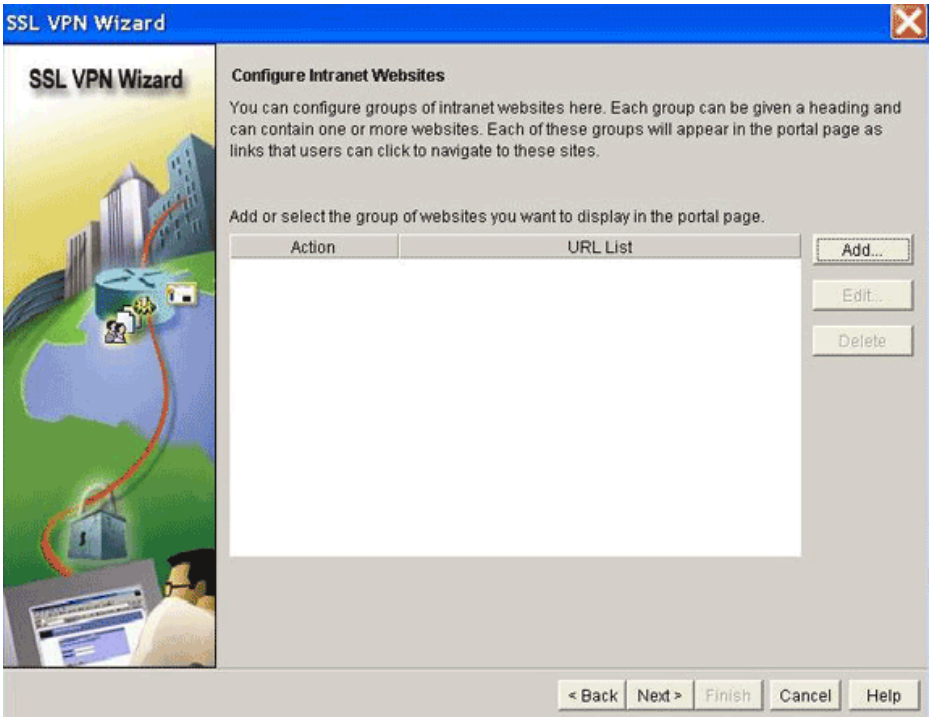


3. Cliquez sur **OK**, puis ajoutez des utilisateurs supplémentaires selon les besoins.
4. Après avoir ajouté les utilisateurs nécessaires, cliquez sur le bouton **Next**, puis passez à l'Étape 4.

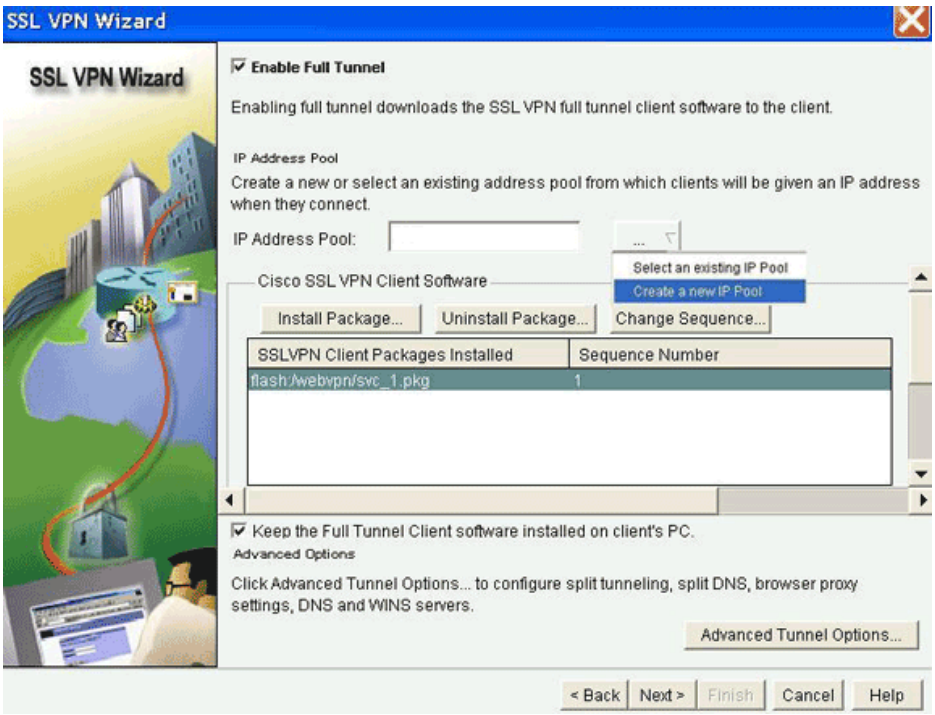
Étape 4. Configurez l'Anyconnect Full Tunnel

Exécutez les étapes suivantes pour configurer le tunnel complet Anyconnect ainsi que le pool d'adresses IP pour les utilisateurs :

1. Anyconnect offre un accès direct aux ressources Intranet d'entreprise ; il n'est donc pas nécessaire de configurer la liste d'URL. Cliquez sur le bouton **Next** situé dans la boîte de dialogue Configure Intranet Websites.



2. Vérifiez que la case **Enable Full Tunnel** est cochée.



3. Créez un pool d’adresses IP pouvant être utilisé par les clients de ce contexte VPN SSL.

   Le pool d’adresses doit correspondre aux adresses disponibles et routables sur votre Intranet.

4. Cliquez sur les ellipses (**..**) à côté du champ de groupe d'adresse IP, et choisissez **créent un nouveau pool d'IP**.

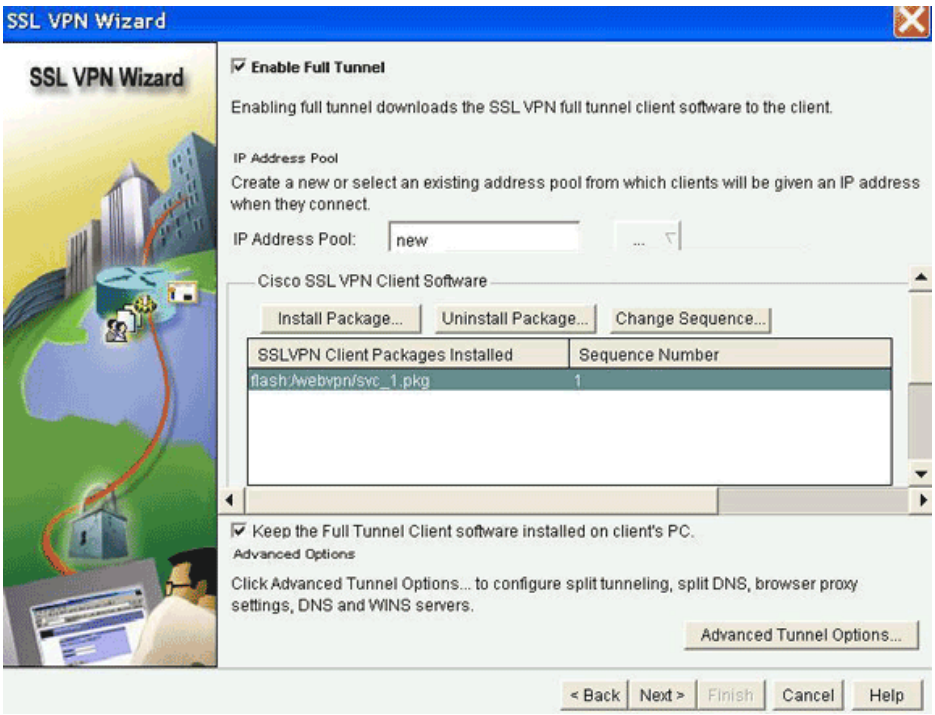
5. Dans la boîte de dialogue Add IP Local Pool, saisissez un nom pour le pool (par exemple, *nouveau*), puis cliquez sur **Add**.

6. Dans la boîte de dialogue Add IP address range, saisissez la plage de pool d'adresses pour les clients Anyconnect VPN, puis cliquez sur **OK**.

   Remarque: Pour les versions antérieures à **12.4(20)T**, le pool d'adresses IP doit se trouver dans la plage d'une interface directement connectée au routeur. Si vous voulez utiliser une plage différente de groupe, vous pouvez créer une adresse de bouclage associée avec votre nouveau groupe pour répondre à cette exigence.

7. Cliquez sur **OK**.

8. Assurez-vous que la case **Install Full Tunnel Client** est cochée.



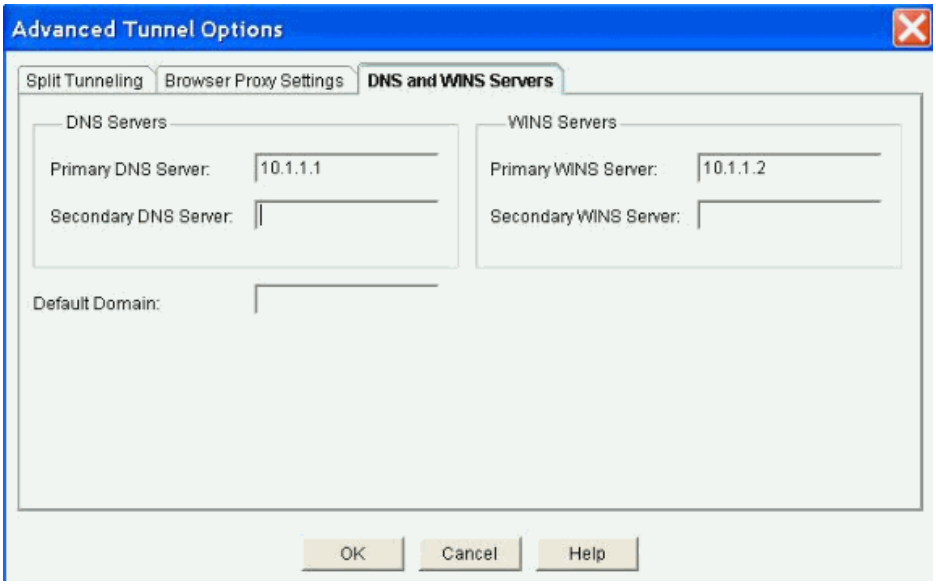
9. Configurez les options de tunnel avancées, notamment la transmission de tunnel partagée, le partage de DNS, les paramètres de proxy du navigateur ainsi que les serveurs DNS et WNS.

   Remarque: Cisco vous recommande de configurer au minimum les serveurs DNS et WINS.

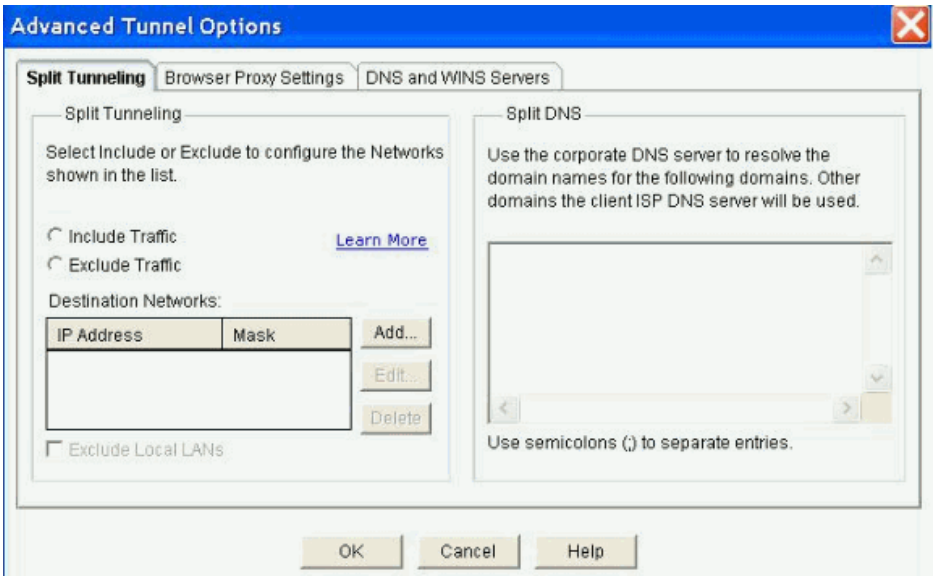
   Exécutez les étapes suivantes pour configurer les options de tunnel avancées :

   a. Cliquez sur le bouton **Advanced Tunnel Options** (Options de tunnel avancées).

   b. Cliquez sur l'onglet **DNS and WINS Servers**, puis saisissez les adresses IP principales des serveurs DNS et WINS.



c. Pour configurer la transmission tunnel partagée, cliquez sur l'onglet **Split Tunneling** (Transmission tunnel partagée).



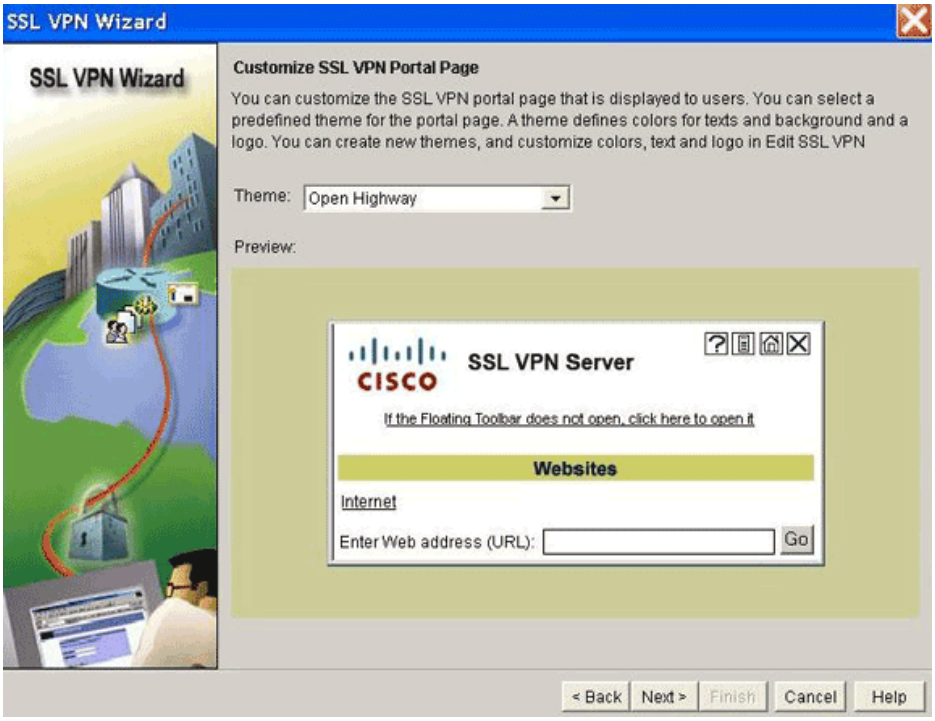
La possibilité de transmettre du trafic sécurisé comme du trafic non sécurité sur la même interface est connue sous le nom de transmission tunnel partagée. Pour la transmission tunnel partagée, vous devez spécifier exactement quel est le trafic sécurisé ainsi que sa destination afin que seul le trafic spécifié accède au tunnel alors que le reste du trafic est transmis non chiffré sur le réseau public (Internet).

Pour obtenir un exemple, reportez-vous à ASA 8.x : Exemple de configuration : Autoriser la transmission de tunnel partagée pour AnyConnect VPN Client sur ASA qui fournit des instructions pas à pas sur la méthode permettant d'autoriser les clients Cisco AnyConnect VPN à accéder à Internet alors qu'ils sont dirigés vers un appareil Cisco Adaptive Security Appliance (ASA) 8.0.2.

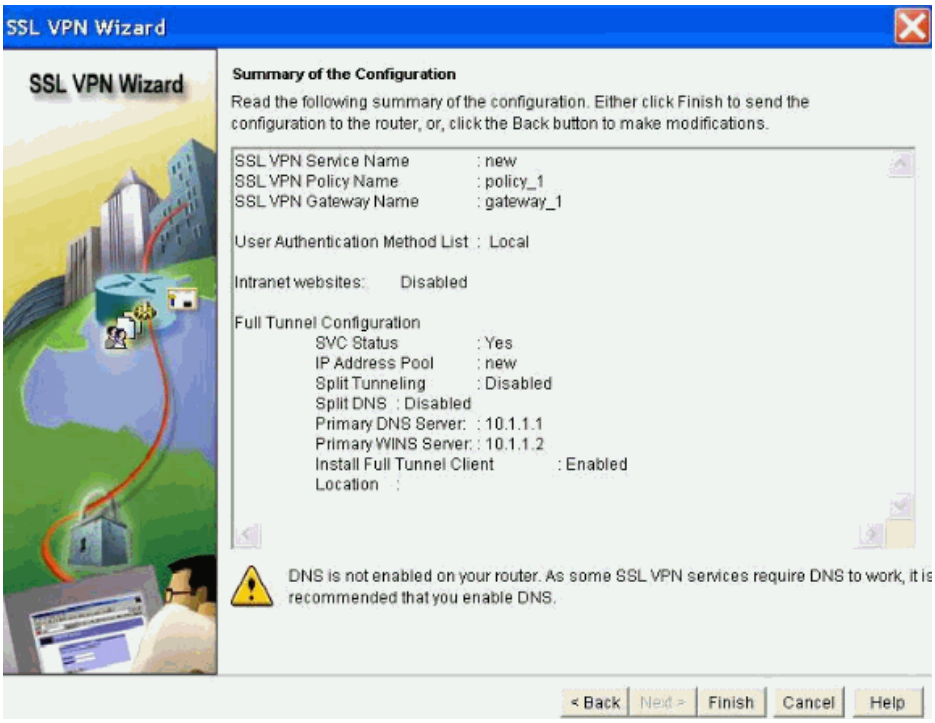
10. Après avoir configuré les options nécessaires, cliquez sur **Next**.

11. Personnaliser la page SSL VPN Portal ou sélectionner les valeurs par défaut.

L'option Customize SSL VPN Portal Page vous permet de personnaliser l'affichage de la page SSL VPN Portal pour vos clients.

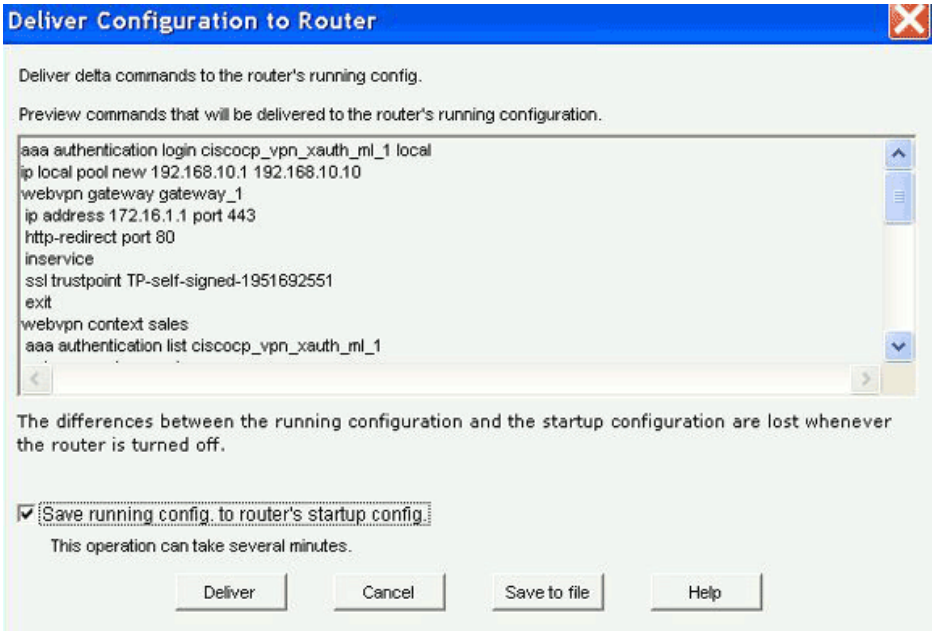


12. Après avoir personnalisé la page du portail VPN SSL, cliquez sur **Next**.
13. Cliquez sur **Finish** (Terminer).



14. Cliquez sur **Deliver** pour sauvegarder votre configuration, puis cliquez sur **OK**.

    L'Assistant VPN SSL soumet vos commandes au routeur.

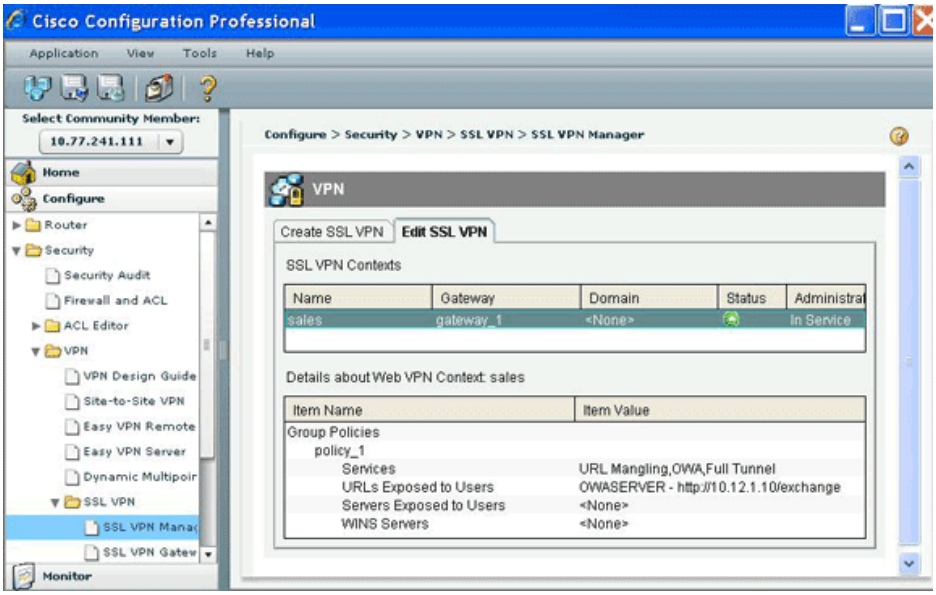


Remarque: Si vous recevez un message d'erreur, la licence VPN SSL peut être incorrecte.

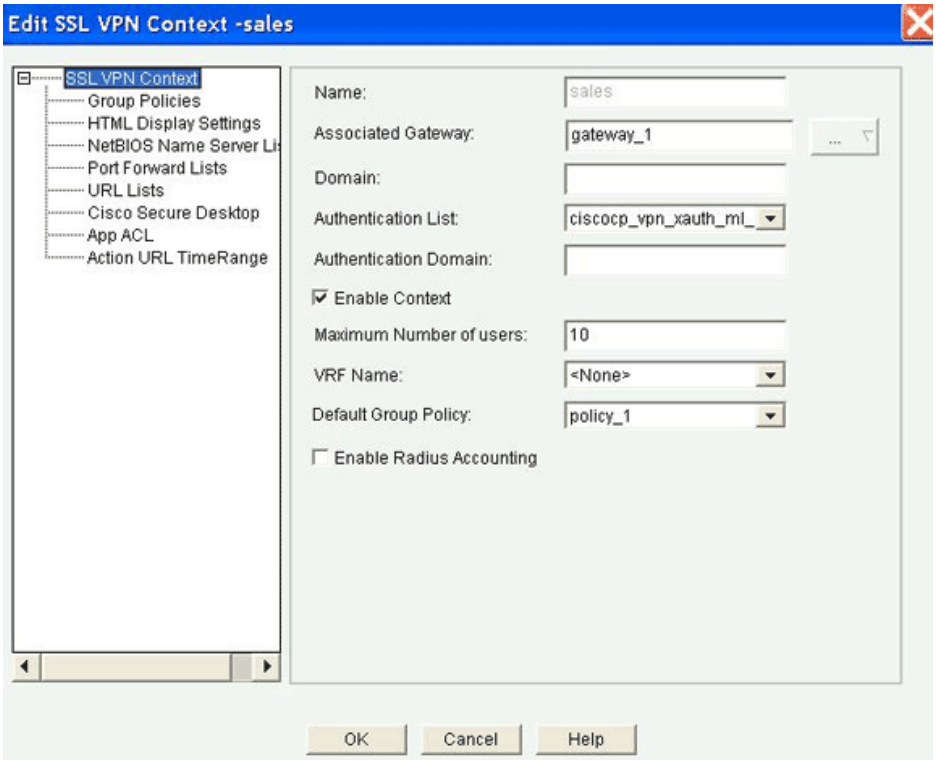
Pour corriger le problème de licence, exécutez les étapes suivantes :

a. Accédez à **Configure > Security > VPN**, puis cliquez sur **SSL VPN**.

b. Cliquez sur **SSL VPN Manager**, puis cliquez sur l'onglet **Edit SSL VPN** situé à droite.



c. Mettez le contexte que vous venez de créer en surbrillance, puis cliquez sur le bouton **Edit** (Modifier).



d. Dans le champ « Maximum Number of users » (Nombre maximal d'utilisateurs), saisissez le nombre correct d'utilisateurs de votre licence.

e. Cliquez sur **OK**, puis cliquez sur **Deliver**.

   Vos commandes sont enregistrées dans le fichier de configuration.

Configuration CLI

CCP crée les configurations de ligne de commande suivantes :

Routeur

```
Router#show run
Building configuration...

Current configuration : 4110 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
no logging buffered
enable password cisco
!
aaa new-model
!
!
aaa authentication login default local
aaa authentication login ciscocp_vpn_xauth_ml_1 local
aaa authorization exec default local
!
!
aaa session-id common
!
crypto pki trustpoint TP-self-signed-1951692551
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-1951692551
revocation-check none
rsakeypair TP-self-signed-1951692551
!
!
```

```
crypto pki certificate chain TP-self-signed-1951692551
certificate self-signed 02
 3082023E 308201A7 A0030201 02020102 300D0609 2A864886 F70D0101 04050030
 31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
 69666963 6174652D 31393531 36393235 3531301E 170D3039 30383037 31303538
 33345A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
 4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 39353136
 39323535 3130819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
 8100CD40 156E21C4 4F84401A F5674319 CC05B708 72A79C69 90997D30 6F556A37
 75FC53DA AB0B43AF 70E7DBC2 C9416C4B 009C3695 67C20847 4F0BC7B0 715F0518
 5E558DFC 13A20167 5D169C47 3BC083C9 A2B66790 79B83814 5008EBF6 169FA897
 6D955F46 2BDADBB0 5275F07E C124CCF3 64DD9CE1 1B6F5744 282E4EA5 A0840385
 5FD90203 010001A3 66306430 0F060355 1D130101 FF040530 030101FF 30110603
 551D1104 0A300882 06526F75 74657230 1F060355 1D230418 30168014 05F279A9
 C556AF46 C5F7A1F0 2ADD2D22 F75BF7B7 301D0603 551D0E04 16041405 F279A9C5
 56AF46C5 F7A1F02A DD2D22F7 5BF7B730 0D06092A 864886F7 0D010104 05000381
 81004886 D666121E 42862509 CA7FDACC 9C57C8BE EB6745FC 533A8C08 FEF2C007
 274374EE 803823FB 79CFD135 2B116544 88B5CFB1 B7BB03E2 F3D65A62 B0EE050A
 924D3168 98357A5B E1F15449 5C9C22D0 577FB036 A3D8BB08 5507C574 18F2F48F
 0694F21C 0983F254 6620FCD7 8E460D29 B09B87E8 ADC3D589 F4D74659 A5CEA30F 1A9C
       quit
dot11 syslog
ip source-route
!
!
!
!
ip cef
!
multilink bundle-name authenticated
!
!
!
username test privilege 15 password 0 test
username tsweb privilege 15 password 0 tsweb
!
!
!
archive
log config
 hidekeys
!
!
!
!
!
!
interface FastEthernet0/0
ip address 10.77.241.111 255.255.255.192
duplex auto
speed auto
!
interface FastEthernet0/1
description $ES_LAN$
ip address 172.16.1.1 255.255.255.0
ip virtual-reassembly
duplex auto
speed auto
!
interface FastEthernet0/1/0
!
interface FastEthernet0/1/1
!
interface FastEthernet0/1/2
!
interface FastEthernet0/1/3
!
interface ATM0/0/0
no ip address
shutdown
no atm ilmi-keepalive
!
interface Vlan1
no ip address
!
ip local pool new 192.168.10.1 192.168.10.10
ip forward-protocol nd
ip route 10.20.10.0 255.255.255.0 172.16.1.2
ip route 10.77.233.0 255.255.255.0 10.77.241.65
ip http server
ip http authentication local
ip http secure-server
!
!
```

```
!
!
!
!
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
password cisco
transport input telnet ssh
transport output telnet
!
scheduler allocate 20000 1000
!
webvpn gateway gateway_1
ip address 172.16.1.1 port 443
http-redirect port 80
ssl trustpoint TP-self-signed-1951692551
inservice
!
webvpn install svc flash:/webvpn/svc_1.pkg sequence 1
!
webvpn context sales
secondary-color white
title-color #CCCC66
text-color black
ssl authenticate verify all

!
!
policy group policy_1

  functions svc-enabled

  svc address-pool "new"
  svc dns-server primary 10.1.1.1
  svc wins-server primary 10.1.1.2
default-group-policy policy_1
aaa authentication list ciscocp_vpn_xauth_ml_1
gateway gateway_1
max-users 10
inservice
!
end
```

Établir la connexion AnyConnect VPN Client

Exécuter ces étapes pour établir une connexion AnyConnect VPN avec le routeur.

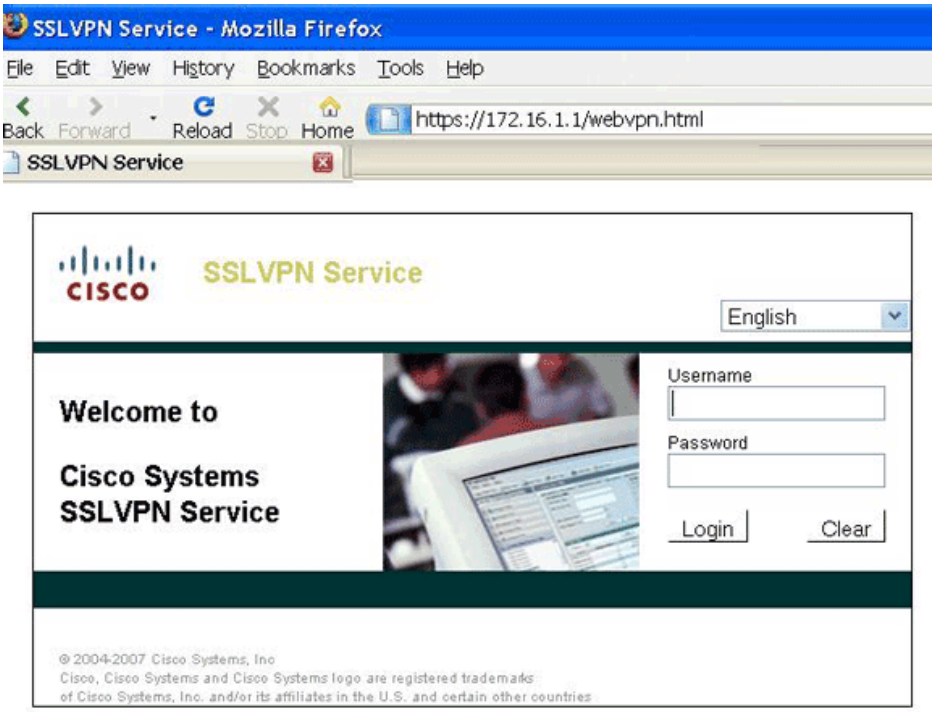
Remarque: Dans Internet Explorer, ajoutez un routeur à la liste des sites de confiance. Pour plus d'informations, reportez-vous à Ajout d'un appareil de sécurité/routeur à la liste des sites de confiance (IE).

1. Dans votre navigateur, saisissez l'URL ou l'adresse IP de l'interface WebVPN du routeur au format indiqué.

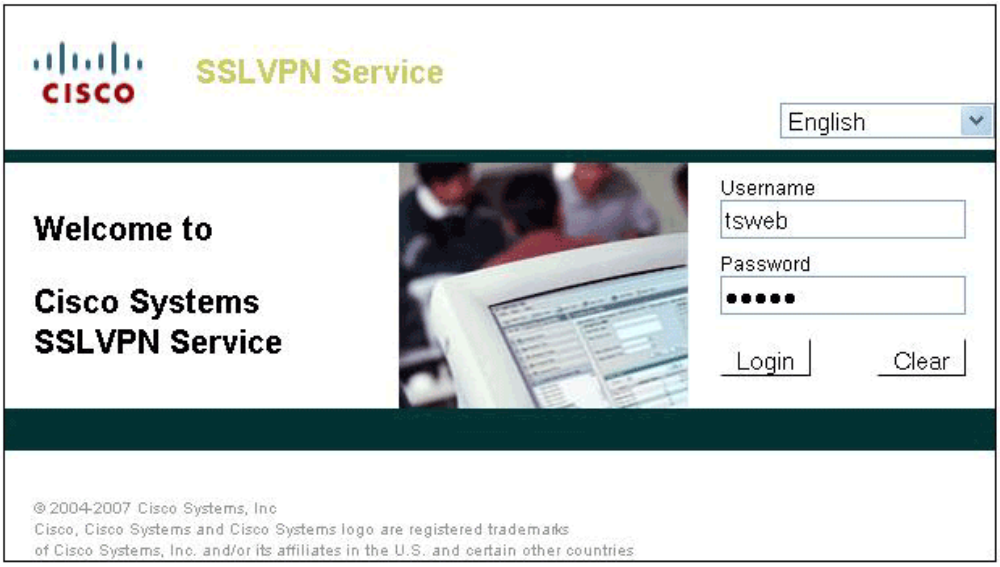
   ```
   https://<url>
   ```

   OU

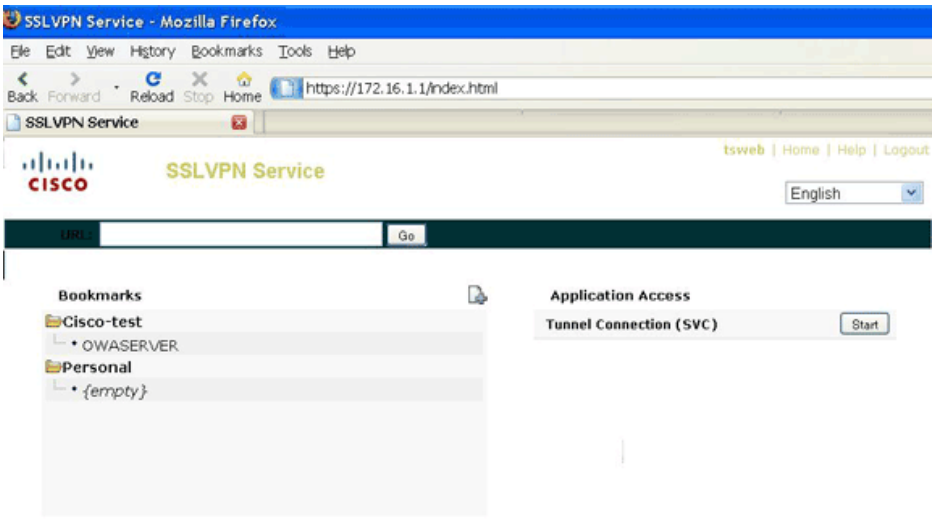
   ```
   https://<IP address of the Router WebVPN interface>
   ```



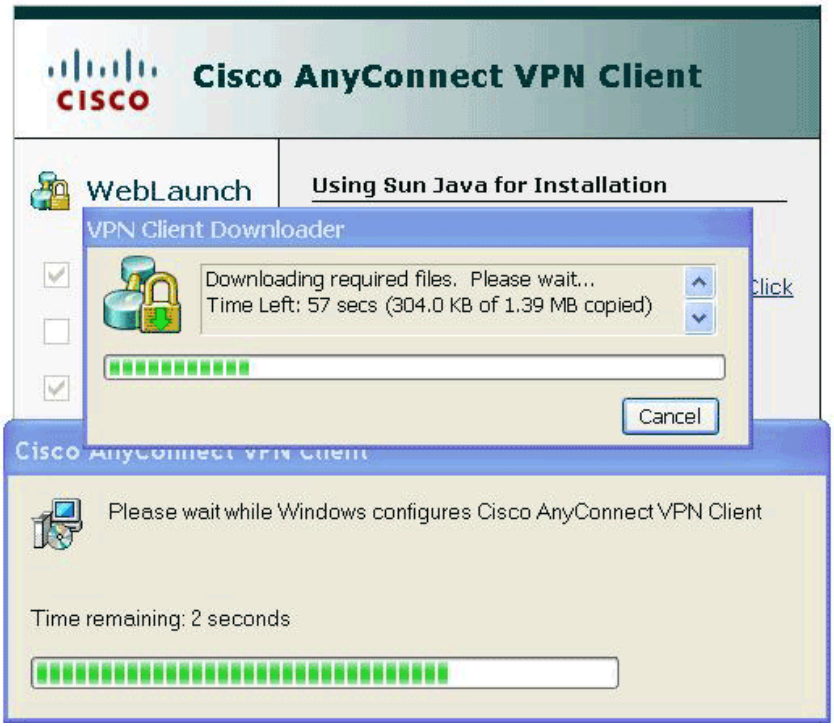
2. Saisissez votre nom d'utilisateur et votre mot de passe.



3. Cliquez sur le bouton Start pour initialiser la connexion de tunnel Anyconnect VPN.



4. Cette fenêtre apparaît avant que la connexion VPN SSL ne soit établie.



Remarque: Le logiciel ActiveX doit être installé sur votre ordinateur avant de télécharger Anyconnect VPN.

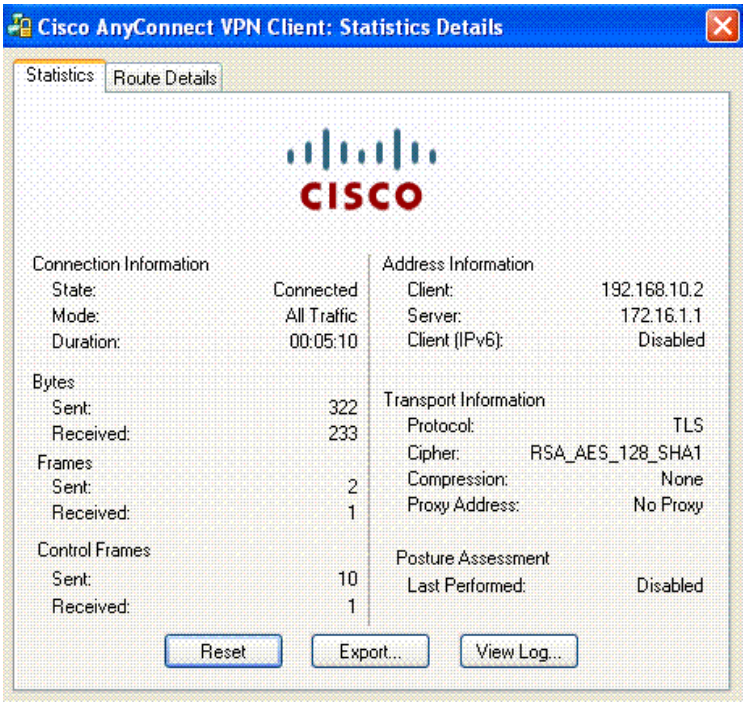
Le message Connection Established une fois le client connecté avec succès.

5. Une fois la connexion correctement établie, cliquez sur l'onglet **Statistics** (Statistiques).

L'onglet Statistics (Statistiques) affiche des informations relatives à la connexion SSL.

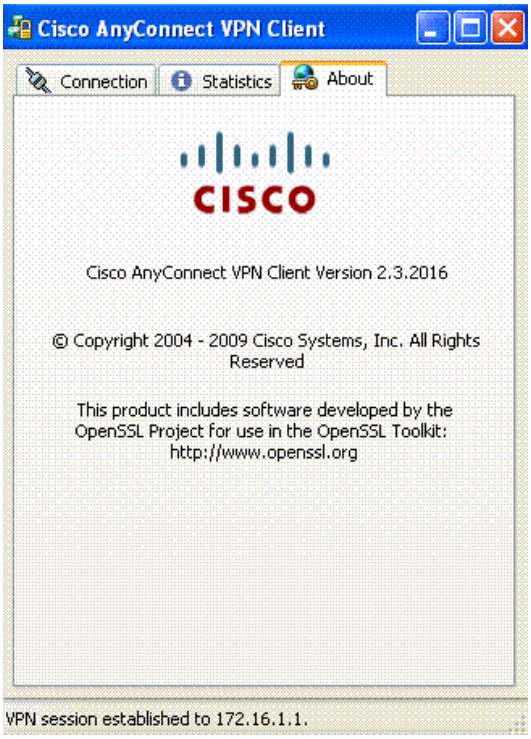
6. Cliquez sur **Details** (Détails).

   La boîte de dialogue Cisco AnyConnect VPN Client : La boîte de dialogue Statistics Detail s'affiche.



   La boîte de dialogue Statistics Details affiche les informations statistiques détaillées sur la connexion, notamment l'état et le mode du tunnel, la durée de la connexion, le nombre d'octets et de trames envoyés et reçus, les informations relatives à l'adresse, les informations relatives au transport ainsi que l'état d'évaluation de position Cisco Secure Desktop. Le bouton Reset de cet onglet permet de réinitialiser les statistiques de transmission. Le bouton « Export » (Exporter) vous permet d'exporter les statistiques, l'interface et la table de routage actuelles dans un fichier texte. Le client AnyConnect vous invite à saisir un nom et à sélectionner un emplacement pour le fichier texte. Le nom par défaut est *AnyConnect-ExportedStats.txt* et l'emplacement par défaut se trouve sur le bureau.
7. Dans la boîte de dialogue Cisco AnyConnect VPN Client, cliquez sur l'onglet **About** (À propos).

   Cet onglet affiche les informations relatives à la version de Cisco AnyConnect VPN Client.



Vérifiez

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

Commandes

Plusieurs commandes **show** sont associées au WebVPN. Vous pouvez exécuter ces commandes dans l'interface de ligne de commande (CLI) afin d'afficher les statistiques et autres informations. Pour obtenir des informations détaillées à propos des commandes **show**, reportez-vous à Vérification de la configuration de WebVPN.

Remarque: 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** .

- ```
  Router#show webvpn session context all
  WebVPN context name: sales
  Client_Login_Name  Client_IP_Address  No_of_Connections  Created  Last_Used
  test               10.20.10.2                3         00:03:10  00:02:56
  ```
- ```
  Router#show webvpn session user test context sales
  WebVPN user name = test ; IP address = 10.20.10.2 ; context = sales
     No of connections: 0
     Created 00:26:05, Last-used 00:25:24
     User Policy Parameters
       Group name = policy_1
     Group Policy Parameters
       url list name = "webserver"
       idle timeout = 2100 sec
       session timeout = Disabled
       functions =
                 mask-urls
                 svc-enabled

       citrix disabled
       address pool name = "new"
       dpd client timeout = 300 sec
       dpd gateway timeout = 300 sec
       keepalive interval = 30 sec
       SSLVPN Full Tunnel mtu size = 1406 bytes
       keep sslvpn client installed = enabled
       rekey interval = 3600 sec
       rekey method =
       lease duration = 43200 sec
  ```
- ```
  Router#show webvpn stats
  User session statistics:
     Active user sessions     : 1          AAA pending reqs         : 0
     Peak user sessions       : 2          Peak time                : 00:00:52
     Active user TCP conns    : 0          Terminated user sessions : 2
     Session alloc failures   : 0          Authentication failures  : 1
     VPN session timeout      : 0          VPN idle timeout         : 0
  ```
  ```

```
   User cleared VPN sessions: 0          Exceeded ctx user limit  : 0
   Exceeded total user limit: 0
   Client process rcvd pkts : 108        Server process rcvd pkts : 0
   Client process sent pkts : 589        Server process sent pkts : 0
   Client CEF received pkts : 76         Server CEF received pkts : 0
   Client CEF rcv punt pkts : 0          Server CEF rcv punt pkts : 0
   Client CEF sent pkts     : 0          Server CEF sent pkts     : 0
   Client CEF sent punt pkts: 0          Server CEF sent punt pkts: 0

   SSLVPN appl bufs inuse   : 0          SSLVPN eng  bufs inuse   : 0
   Active server TCP conns  : 0

Mangling statistics:
   Relative urls            : 0          Absolute urls            : 0
   Non-http(s) absolute urls: 0          Non-standard path urls   : 0
   Interesting tags         : 0          Uninteresting tags       : 0
   Interesting attributes   : 0          Uninteresting attributes : 0
   Embedded script statement: 0          Embedded style statement : 0
   Inline scripts           : 0          Inline styles            : 0
   HTML comments            : 0          HTTP/1.0 requests        : 0
   HTTP/1.1 requests        : 9          Unknown HTTP version     : 0
   GET requests             : 9          POST requests            : 0
   CONNECT requests         : 0          Other request methods    : 0
   Through requests         : 0          Gateway requests         : 9
   Pipelined requests       : 0          Req with header size >1K : 0
   Processed req hdr bytes  : 2475       Processed req body bytes : 0
   HTTP/1.0 responses       : 0          HTTP/1.1 responses       : 0
   HTML responses           : 0          CSS responses            : 0
   XML responses            : 0          JS responses             : 0
   Other content type resp  : 0          Chunked encoding resp    : 0
   Resp with encoded content: 0          Resp with content length : 0
   Close after response     : 0          Resp with header size >1K: 0
   Processed resp hdr size  : 0          Processed resp body bytes: 0
   Backend https response   : 0          Chunked encoding requests: 0

HTTP Authentication stats :
   Successful NTLM Auth     : 0          Failed NTLM Auth         : 0
   Successful Basic Auth    : 0          Failed Basic Auth        : 0
   Unsupported Auth         : 0          Unsup Basic HTTP Method  : 0
   NTLM srv kp alive disabld: 0          NTLM Negotiation Error   : 0
   Oversize NTLM Type3 cred : 0          Internal Error           : 0
   Num 401 responses        : 0          Num non-401 responses    : 0
   Num Basic forms served   : 0          Num NTLM forms served    : 0
   Num Basic Auth sent      : 0          Num NTLM Auth sent       : 0

CIFS statistics:
 SMB related Per Context:
   TCP VC's                 : 0          UDP VC's                 : 0
   Active VC's              : 0          Active Contexts          : 0
   Aborted Conns            : 0
 NetBIOS related Per Context:
   Name Queries             : 0          Name Replies             : 0
   NB DGM Requests          : 0          NB DGM Replies           : 0
   NB TCP Connect Fails     : 0          NB Name Resolution Fails : 0
 SMB related Global:
   Sessions in use          : 0          Mbufs in use             : 0
   Mbuf Chains in use       : 0          Active VC's              : 0
   Active Contexts          : 0          Browse Errors            : 0
   Empty Browser List       : 0          NetServEnum Errors       : 0
   Empty Server List        : 0          NBNS Config Errors       : 0
   NetShareEnum Errors      : 0
 HTTP related Per Context:
   Requests                 : 0          Request Bytes RX         : 0
   Request Packets RX       : 0          Response Bytes TX        : 26286
   Response Packets TX      : 33         Active Connections       : 0
   Active CIFS context      : 0          Requests Dropped         : 0
 HTTP related Global:
   Server User data         : 0          CIFS User data           : 0
   Net Handles              : 0          Active CIFS context      : 0
   Authentication Fails     : 0          Operations Aborted       : 0
   Timers Expired           : 0          Pending Close            : 0
   Net Handles Pending SMB  : 0          File Open Fails          : 0
   Browse Network Ops       : 0          Browse Network Fails     : 0
   Browse Domain Ops        : 0          Browse Domain Fails      : 0
   Browse Server Ops        : 0          Browse Server Fails      : 0
   Browse Share Ops         : 0          Browse Share Fails       : 0
   Browse Dir Ops           : 0          Browse Network Fails     : 0
   File Read Ops            : 0          File Read Fails          : 0
   File Write Ops           : 0          File Write Fails         : 0
   Folder Create Ops        : 0          Folder Create Fails      : 0
   File Delete Ops          : 0          File Delete Fails        : 0
   File Rename Ops          : 0          File Rename Fails        : 0
   URL List Access OK       : 0          URL List Access Fails    : 0
```

```
Socket statistics:
   Sockets in use          : 1          Sock Usr Blocks in use   : 1
   Sock Data Buffers in use : 0         Sock Buf desc in use     : 0
   Select timers in use     : 1         Sock Select Timeouts     : 0
   Sock Tx Blocked          : 0         Sock Tx Unblocked        : 0
   Sock Rx Blocked          : 0         Sock Rx Unblocked        : 0
   Sock UDP Connects        : 0         Sock UDP Disconnects     : 0
   Sock Premature Close     : 0         Sock Pipe Errors         : 12
   Sock Select Timeout Errs : 0

Port Forward statistics:
 Client                                Server
   proc pkts               : 0         proc pkts                : 0
   proc bytes              : 0         proc bytes               : 0
   cef pkts                : 0         cef pkts                 : 0
   cef bytes               : 0         cef bytes                : 0

WEBVPN Citrix statistics:

              Server                   Client
 Packets in  : 0                       0
 Packets out : 0                       0
 Bytes in    : 0                       0
 Bytes out   : 0                       0

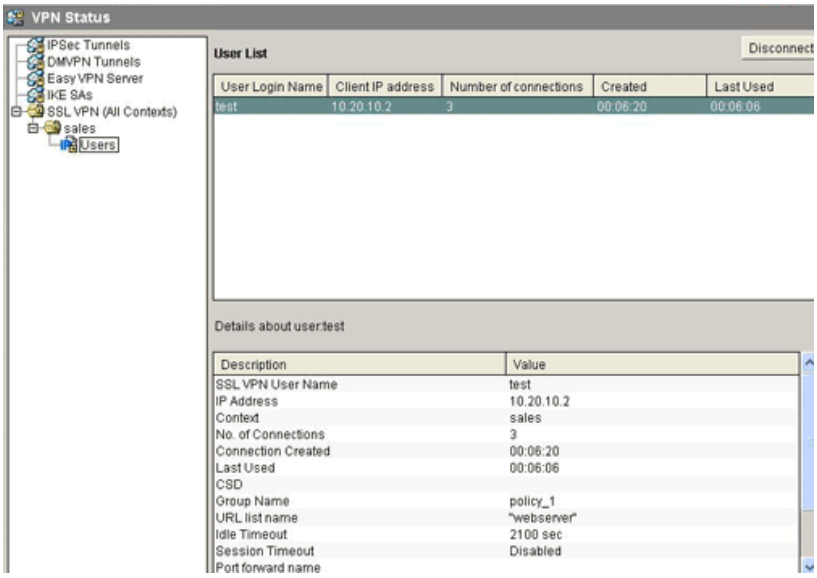
ACL statistics:
   Permit web request       : 0         Deny web request         : 0
   Permit cifs request      : 0         Deny cifs request        : 0
   Permit without ACL       : 0         Deny without match ACL   : 0
   Permit with match ACL    : 0         Deny with match ACL      : 0

Single Sign On statistics:
   Auth Requests            : 0         Pending Auth Requests    : 0
   Successful Requests      : 0         Failed Requests          : 0
   Retranmissions           : 0         DNS Errors               : 0
   Connection Errors        : 0         Request Timeouts         : 0
   Unknown Responses        : 0

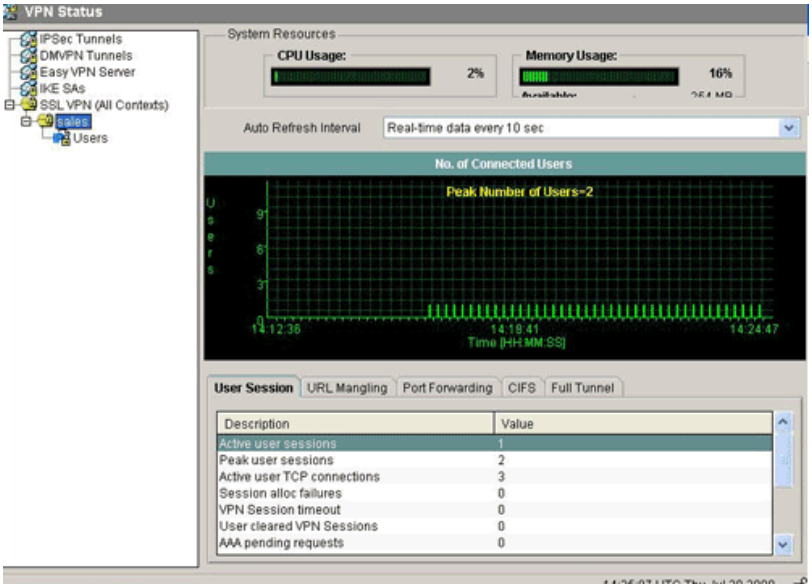
URL-rewrite splitter statistics:
   Direct access request    : 0         Redirect request         : 0
   Internal request         : 0

Tunnel Statistics:
   Active connections       : 0
   Peak connections         : 1         Peak time                : 00:34:51
   Connect succeed          : 3         Connect failed           : 0
   Reconnect succeed        : 0         Reconnect failed         : 0
   DPD timeout              : 0
 Client                                Server
   in  CSTP frames          : 32        out IP pkts              : 5
   in  CSTP data            : 5
   in  CSTP control         : 27
   in  CSTP bytes           : 1176      out IP bytes             : 805
   out CSTP frames          : 4         in  IP pkts              : 0
   out CSTP data            : 0
   out CSTP control         : 4
   out CSTP bytes           : 32        in  IP bytes             : 0
   cef in CSTP data frames  : 0         cef out forwarded pkts   : 0
   cef in CSTP data bytes   : 0         cef out forwarded bytes  : 0
   cef out CSTP data frames : 0         cef in forwarded pkts    : 0
   cef out CSTP data bytes  : 0         cef in forwarded bytes   : 0
```

- Dans CCP, sélectionnez **Monitoring > Security > VPN Status > SSL VPN > Users** pour afficher la liste d’utilisateurs VPN SSL actuels dans le routeur.



- Sélectionnez **Monitoring > Security > VPN Status > SSL VPN > Sales** pour afficher les informations relatives à la session VPN SSL actuelle dans le routeur.



Dépannez

Utilisez cette section pour dépanner votre configuration.

Problème de connectivité SSL

Problème : Les clients VPN SSL ne peuvent pas se connecter au routeur.

Solution : Un nombre insuffisant d'adresses IP dans le pool d'adresses IP peut être à l'origine du problème. Pour résoudre ce problème, augmentez le nombre d'adresses IP dans le pool d'adresses IP du routeur.

Pour plus d'informations sur le dépannage d'AnyConnect VPN Client, reportez-vous à FAQ sur AnyConnect VPN Client.

Erreur : SSLVPN Package SSL-VPN-Client : installed Error: Disque

Problème : Vous recevez cette erreur lorsque vous installez un package SVC sur un routeur : `SSLVPN Package SSL-VPN-Client : installed Error: Disque`.

Solution : Un reformatage de la mémoire Flash peut résoudre cette erreur.

Dépannage des commandes

Plusieurs commandes **clear** sont associées à WebVPN. Pour obtenir des informations détaillées à propos de ces commandes, reportez-vous à Utilisation des commandes Clear WebVPN.

Plusieurs commandes **debug** sont associées à WebVPN. Pour obtenir des informations détaillées à propos de ces commandes, reportez-vous à Utilisation des commandes Debug WebVPN.

Remarque: L’utilisation des commandes **debug** peut avoir un impact négatif sur votre périphérique Cisco. Avant d'utiliser les commandes **debug**, référez-vous à la section **Informations importantes sur les commandes Debug**.

Informations connexes

- **Client VPN AnyConnect - Forum Aux Questions**
- **Guide de l’administrateur Cisco AnyConnect VPN Client, Version 2.3**
- **VPN SSL - WebVPN**
- **Exemple de configuration d'un VPN SSL sans client (WebVPN) sur Cisco IOS avec SDM**
- **Exemple de configuration de VPN SSL (WebVPN) client léger sur IOS avec SDM**
- **Exemples et notes techniques de configuration**

Date du fichier PDF généré: 30 juillet 2013

http://www.cisco.com/cisco/web/support/CA/fr/109/1098/1098197_ssl-ios-00.html