在IOS路由器上有CCP的AnyConnect VPN (SSL)客户端配置示例

内容

前言

本文描述如何设置Cisco IOS路由器执行在忠心于的SSL VPN使用Cisco Configuration Professional (CCP)的Cisco AnyConnect VPN客户。此设置适用于路由器不允许分割隧道的特定情况，且用户必须先直接连接到路由器，然后才可以访问 Internet。

以下 IOS 路由器平台支持 SSL VPN 或 WebVPN 技术：

- 870、1811、1841、2801、2811、2821、2851
- 3725、3745、3825、3845、7200 和 7301

CCP 是基于 GUI 的设备管理工具，可以配置基于 Cisco IOS 的接入路由器，包括 Cisco 集成多业务路由器、Cisco 7200 系列路由器和 Cisco 7301 路由器。CCP 安装在 PC 上，可以通过基于 GUI 且简单易用的向导简化路由器、安全、统一通信、无线、WAN 和 LAN 基本配置。

如果路由器和 CCP 一起订购，装货时 Cisco Configuration Professional Express (CCP Express) 将会安装到路由器闪存中。CCP Express 是 CCP 的轻量版本。您可以使用 CCP Express 在路由器的 LAN 和 WAN 接口上配置基本的安全功能。CCP Express 安装在路由器闪存中。

前提条件

需求

尝试进行此配置之前，请确保满足以下要求：

- Microsoft Windows 2000 或 XP
- 带 SUN JRE 1.4 或更高版本的 Web 浏览器，或者有 ActiveX 控制的浏览器
- 客户端的本地管理权限
- 安装了高级安全镜像 12.4(20)T 或更高版本的 Cisco IOS 路由器
- Cisco Configuration Professional 1.3

  如果尚未在计算机上加载 Cisco Configuration Professional，您可从软件下载获取该软件的免费副本，然后安装 .exe (cisco-config-pro-k9-pkg-1_3-en.zip) 文件。有关 CCP 安装和配置的详细信息，请参阅“Cisco Configuration Professional 快速入门指南”。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 软件版本为 12.4(24)T 的 Cisco IOS 系列 1841 路由器
- Cisco Configuration Professional (CCP) 1.3
- 用于 Windows 的 Cisco AnyConnect SSL VPN Client 版本 2.3.2016

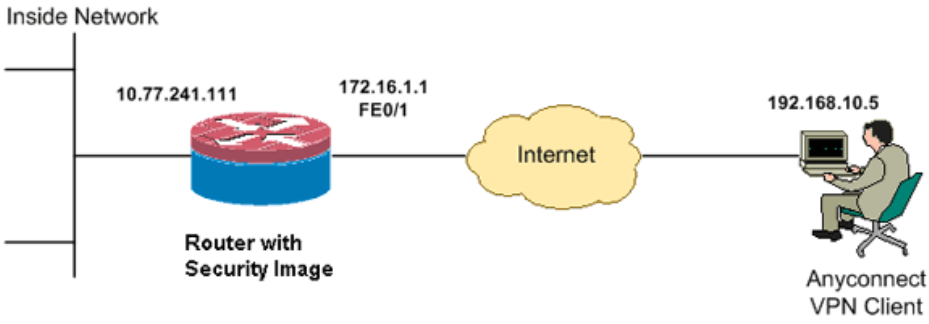
注意： 本文档中的信息在特定实验室环境设备上创建。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

惯例

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

网络图

本文档使用以下网络设置：



配置前的任务

1. 您必须为 CCP 配置路由器。

   具有相应安全捆绑许可证的路由器的闪存中已加载了 CCP 应用程序。要获得并配置该软件，请参阅“Cisco Configuration Professional 快速入门指南”。
2. 将 Anyconnect VPN .pkg 文件副本下载至管理 PC。

在 IOS 上配置 Anyconnect VPN

本部分提供有关配置本文档中所述功能的必要步骤。本配置示例使用 CCP 向导指导在 IOS 路由器上的 Anyconnect VPN 操作。

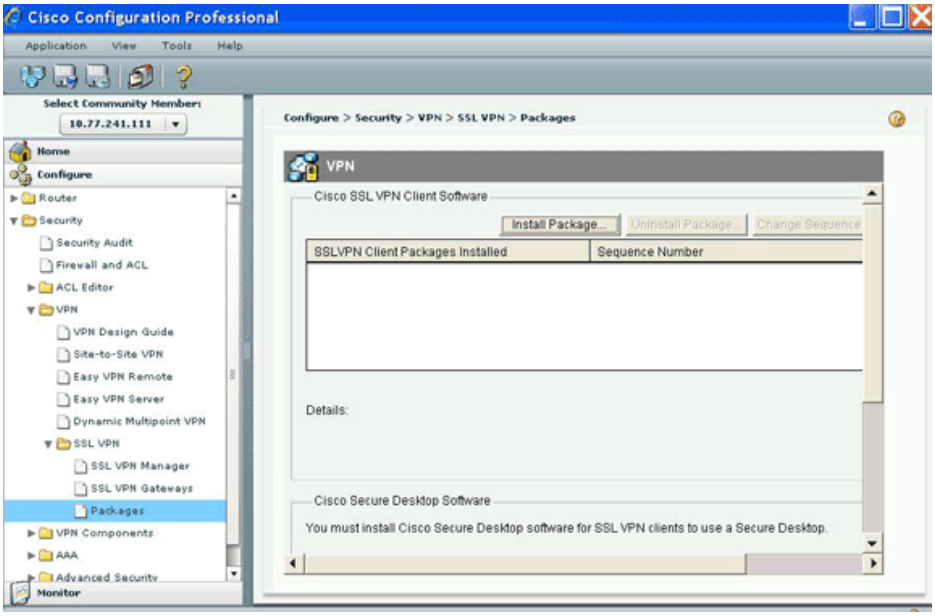
要在 Cisco IOS 路由器上配置 Anyconnect VPN，完成以下步骤：

1. 在 Cisco IOS 路由器上安装并启用 Anyconnect VPN 软件
2. 使用 CCP 向导配置 SSL VPN 上下文和 SSL VPN 网关
3. 配置 Anyconnect VPN 用户的用户数据库
4. 配置面向用户的资源

步骤 1. 在 IOS 路由器上安装并启用 Anyconnect VPN 软件

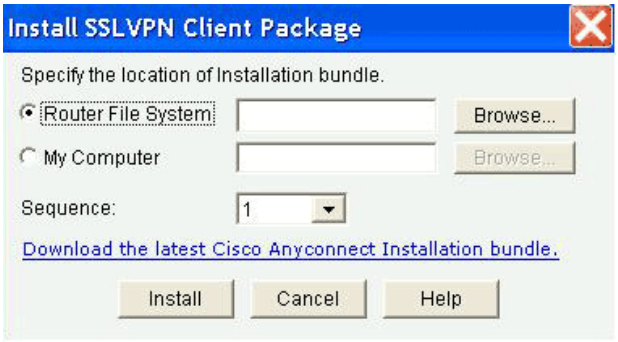
要在 IOS 路由器中安装并启用 Anyconnect VPN 软件，完成以下步骤：

1. 打开 CCP 应用程序，选择 Configure > Security，然后单击 VPN。
2. 展开 SSLVPN，并选择 Packages。



3. 在 Cisco SSL VPN 客户端软件中，单击 Browse。

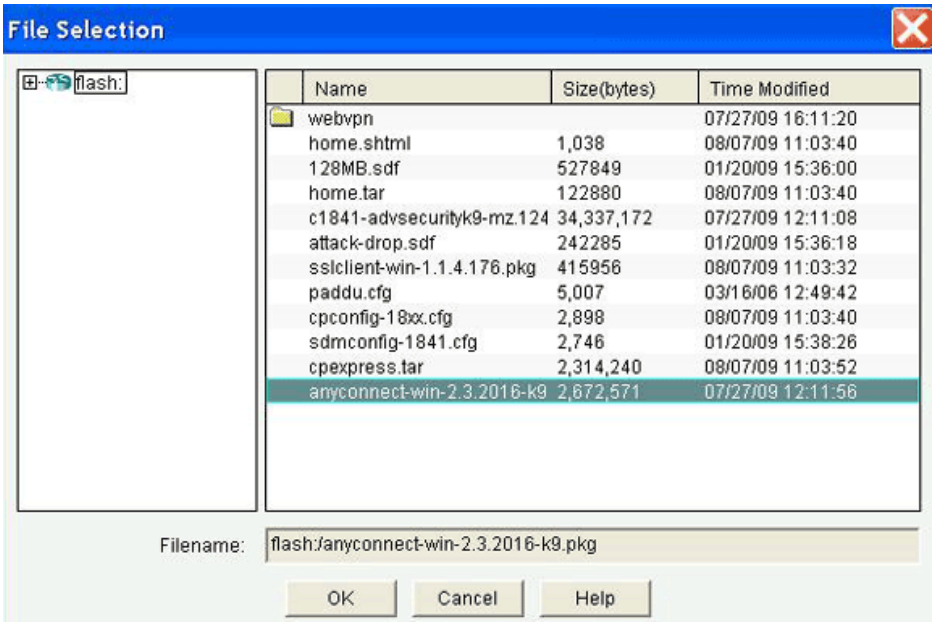
   此时将出现 Install SSL VPN Client Package 对话框。



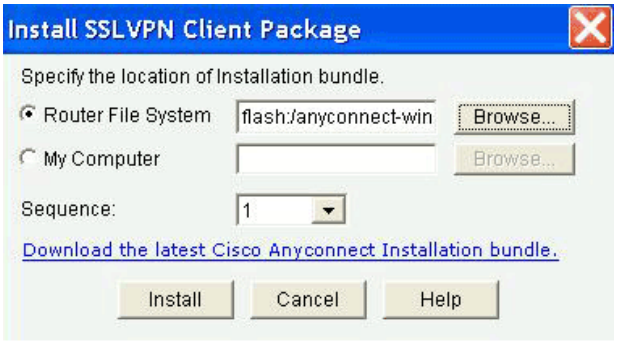
4. 指定 Cisco Anyconnect VPN 客户端镜像的位置。

   - 如果 Cisco Anyconnect VPN 客户端镜像在路由器闪存中，单击 Router File System 单选按钮对话框，然后单击 Browse。
   - 如果 Cisco Anyconnect VPN 客户端镜像不在路由器闪存中，单击 My Computer 单选对话框，然后单击 Browse。

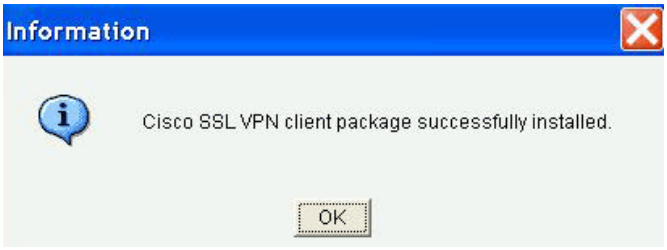
   此时将出现 File Selection 对话框。



5. 选择需要安装的客户端镜像，并单击 OK。



6. 指定客户端镜像的位置后，单击 Install。
7. 单击 Yes，然后单击 OK。
8. 客户端镜像成功安装后，您将收到以下消息：

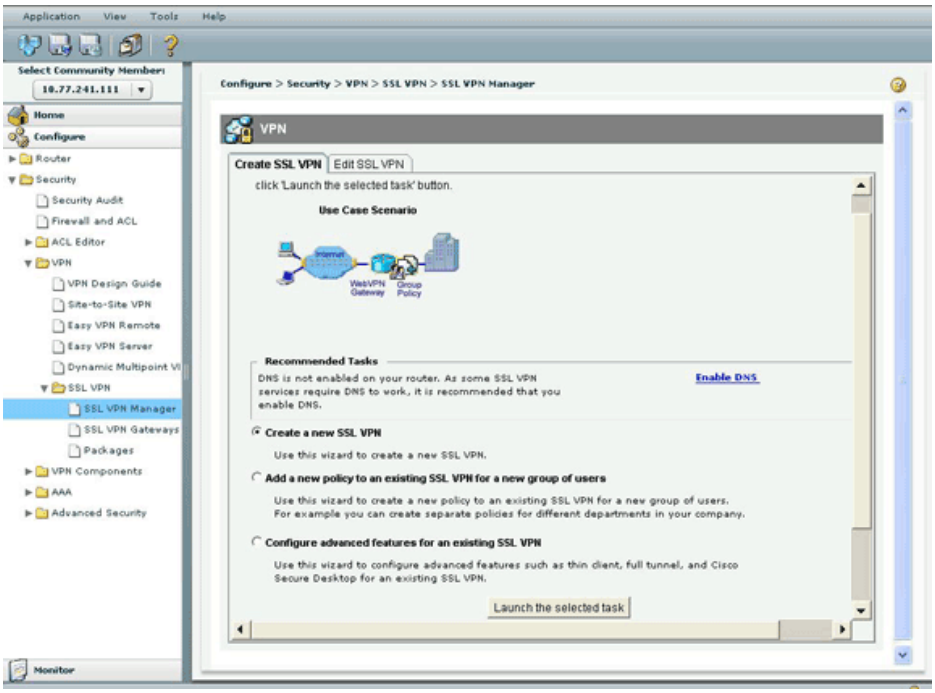


9. 单击 OK 继续。

步骤 2. 使用 CCP 向导配置 SSLVPN 上下文和 SSLVPN 网关

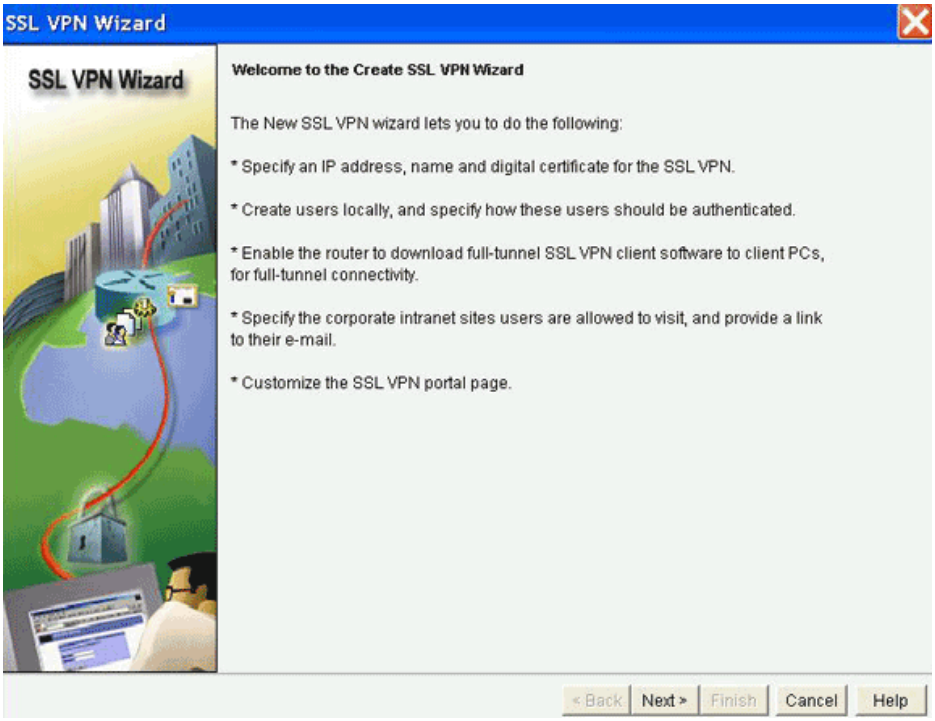
要配置 SSL VPN 上下文和 SSL VPN 网关，完成以下步骤：

1. 选择 Configure > Security > VPN，然后单击 SSL VPN。
2. 依次单击 SSL VPN Manager 和 Create SSL VPN 选项卡。

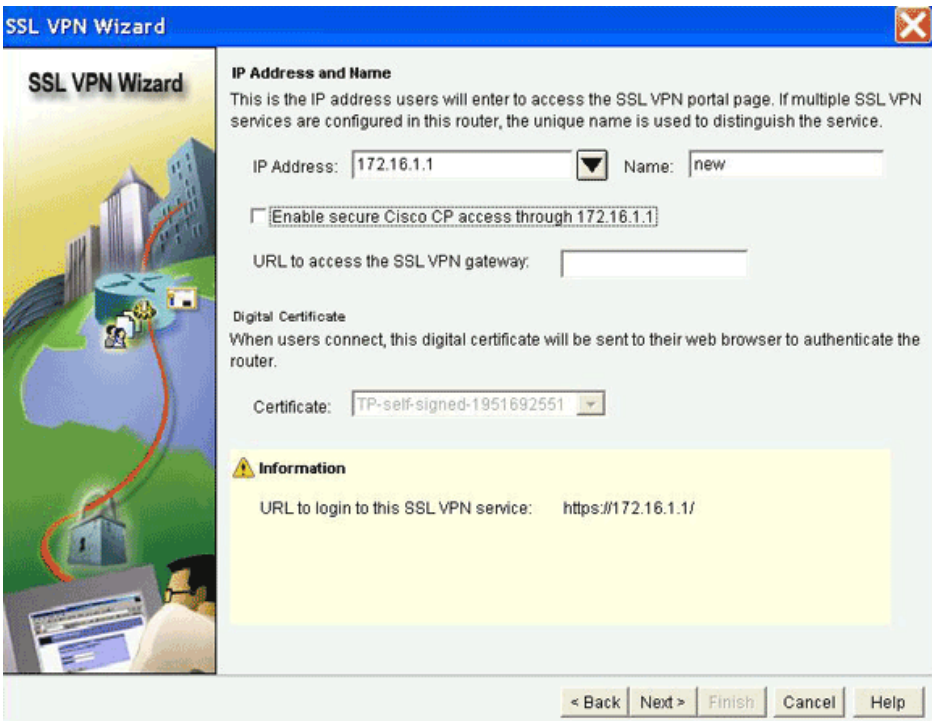


3. 选中 Create a New SSL VPN 单选按钮，然后单击 Launch the selected task。

   此时将出现 SSL VPN Wizard 对话框。



4. 单击 Next。



5. 输入新 SSL VPN 网关的 IP 地址，并为此 SSL VPN 上下文输入唯一名称。

   您可以为同一个 IP 地址（SSL VPN 网关）创建不同的 SSL VPN 上下文，但每个名称都必须唯一。本示例使用以下 IP 地址：https://172.16.1.1/

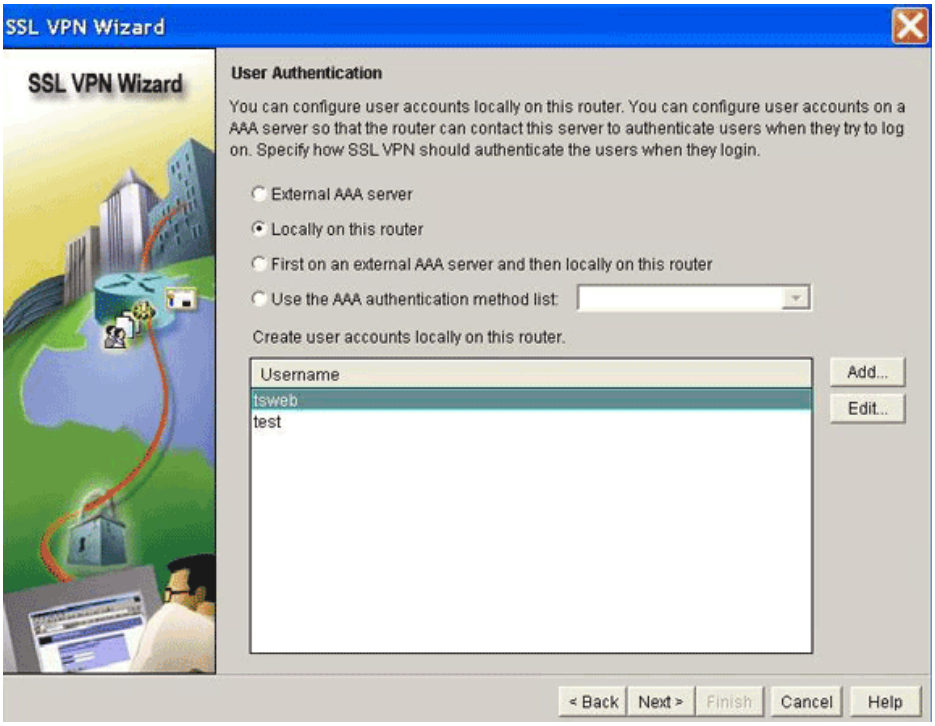
6. 单击 Next，继续进行步骤 3。

步骤 3. 配置 Anyconnect VPN 用户的用户数据库

您可以使用 AAA 服务器、本地用户或同时使用两者进行身份验证。本配置示例使用本地创建的用户进行身份验证。

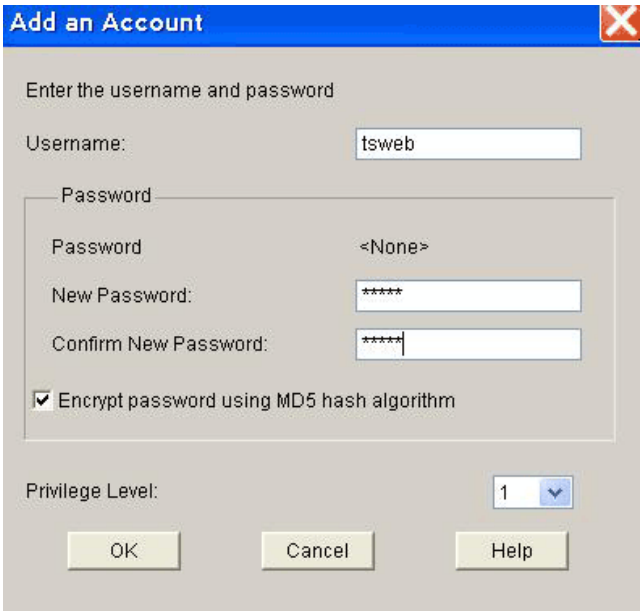
要配置 Anyconnect VPN 用户的用户数据库，完成以下步骤：

1. 完成步骤 2 后，单击 SSL VPN Wizard User Authentication 对话框中的 Locally on this router 单选按钮。



可以使用此对话框向本地数据库添加用户。

2. 单击 Add，然后输入用户信息。

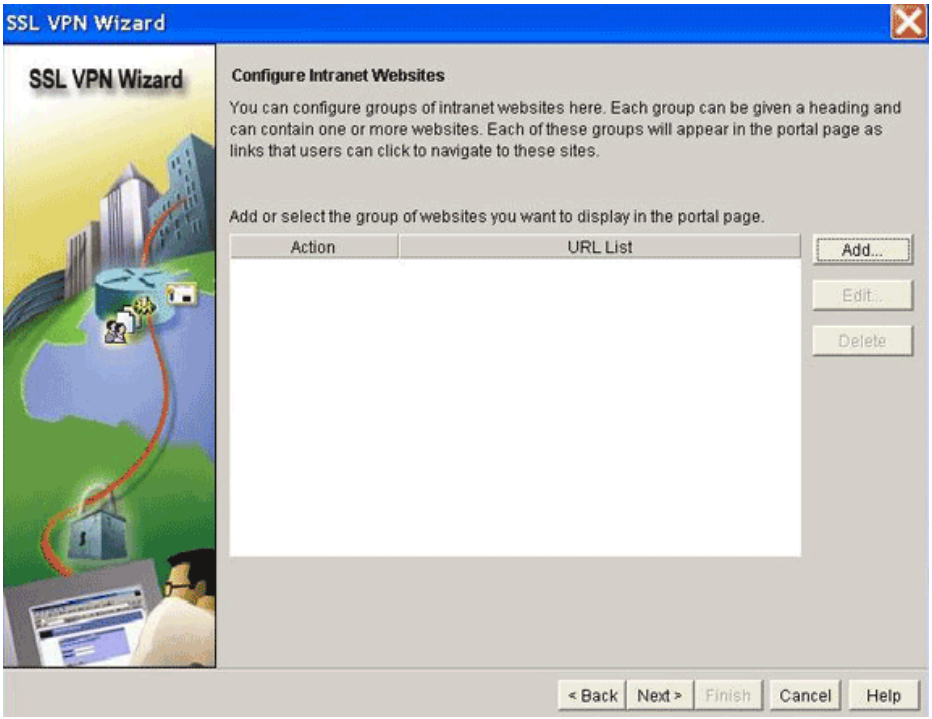


3. 单击 OK，并根据需要添加其他用户。
4. 添加所需用户后，单击 Next，继续进行步骤 4。

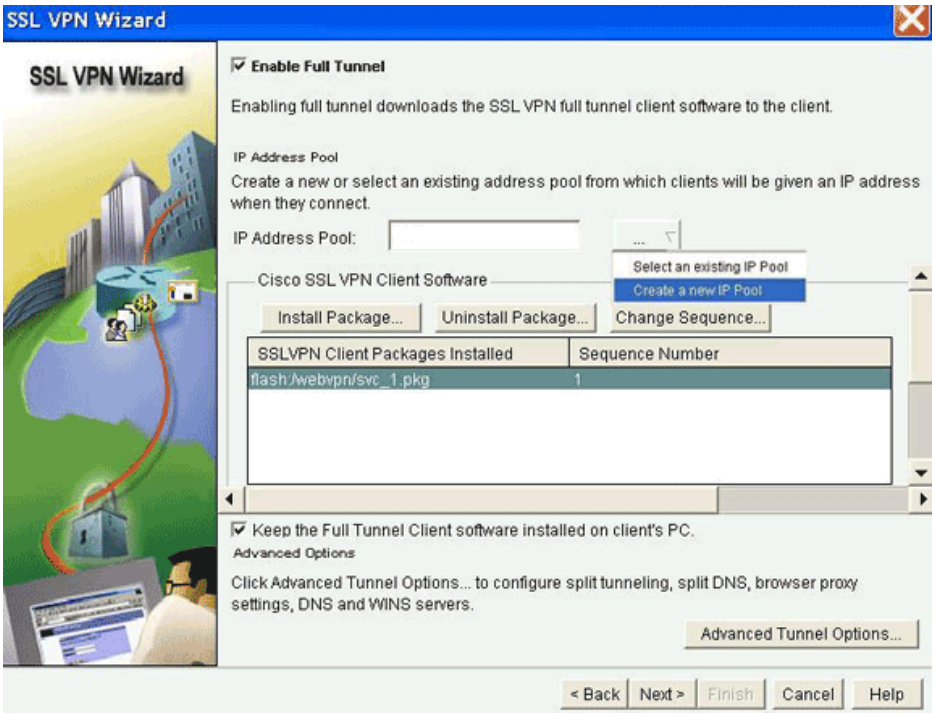
步骤 4. 配置 Anyconnect 全隧道

要配置用户的 Anyconnect 全隧道和 IP 地址池，完成以下步骤：

1. 由于 Anyconnect 可直接访问企业 Intranet 资源，所以不需要配置 URL 列表。单击 Configure Intranet Websites 对话框中的 Next 按钮。



2. 确认 Enable Full Tunnel 复选框已勾选。



3. 创建此 SSL VPN 上下文客户端可使用的 IP 地址池。

   地址池必须与 Intranet 上可用且可路由的地址相对应。

4. 点击椭圆(…)在IP地址旁边请缓冲字段，并且选择创建一个新的IP池。

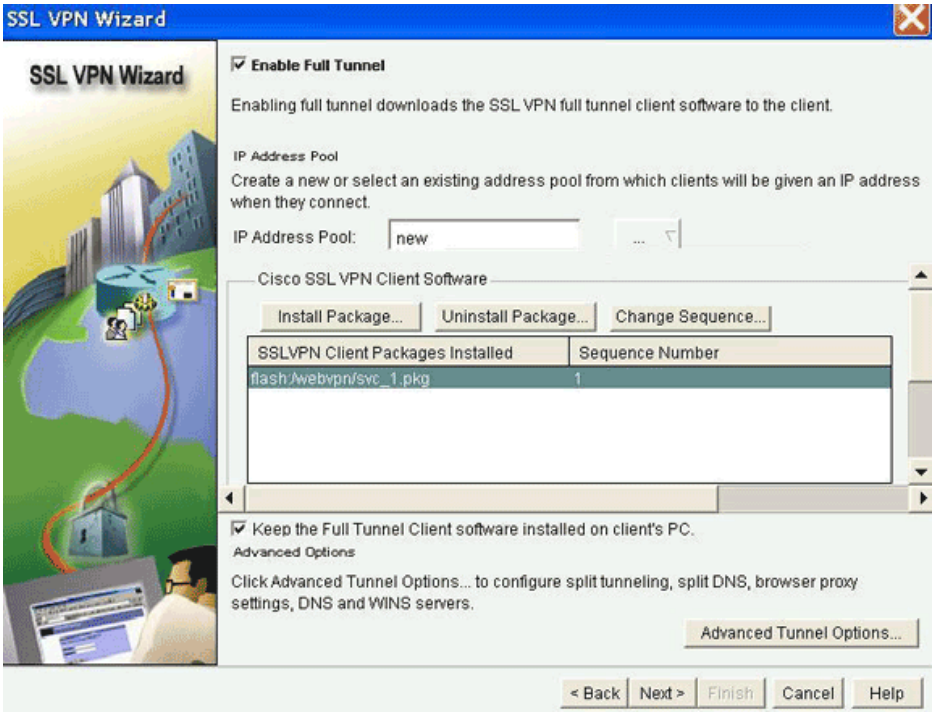
5. 在 Add IP Local Pool 对话框中，输入地址池的名称（例如，new），然后单击 Add。

6. 在 Add IP address range 对话框中，输入 Anyconnect VPN 客户端的地址池范围，然后单击 OK。

   注意： 在 12.4(20)T 之前的版本中，IP 地址池应包括直接连接至路由器的接口。如果要使用不同的池范围，可以创建与新池关联的环回地址，以满足该要求。

7. 单击 Ok。

8. 确保勾选 Install Full Tunnel Client 复选框。



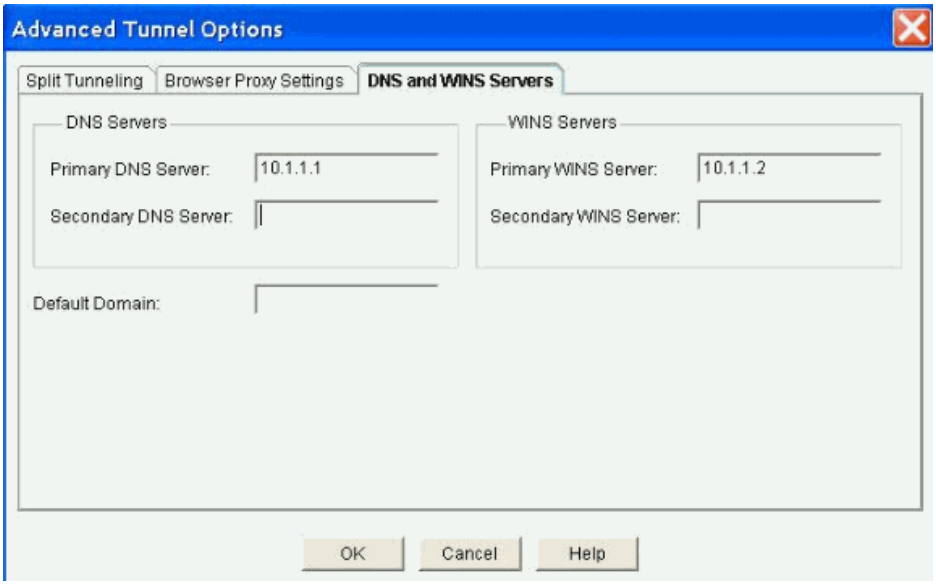
9. 配置高级隧道选项，如分割隧道、分割 DNS、浏览器代理设置以及 DNS 和 WNS 服务器等。

   注意： Cisco 建议至少配置 DNS 和 WINS 服务器。

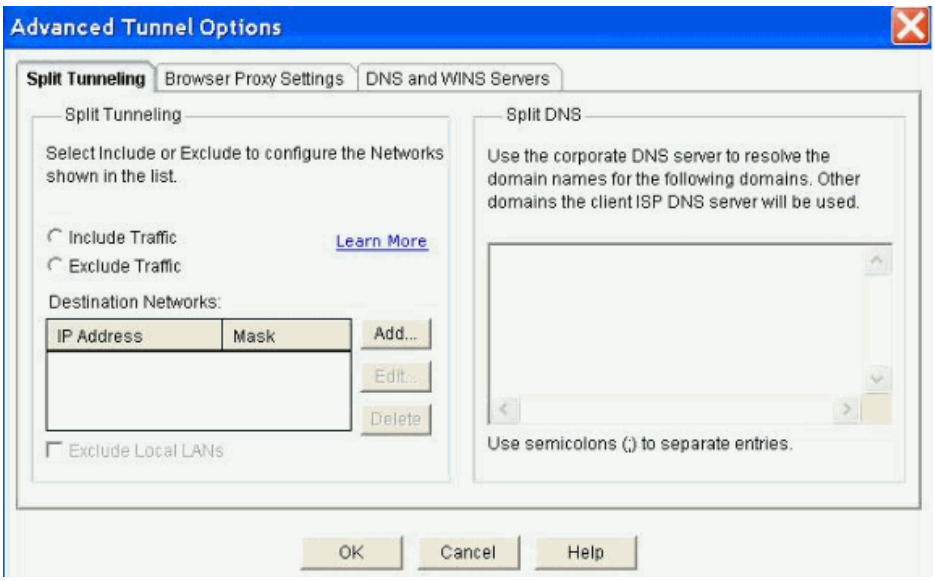
   要配置高级隧道选项，完成以下步骤：

   a. 单击 Advanced Tunnel Options 按钮。

   b. 单击 DNS and WINS Servers 选项卡，输入 DNS 和 WINS 的主 IP 地址。



c. 要配置分割隧道，单击 Split Tunneling 选项卡。



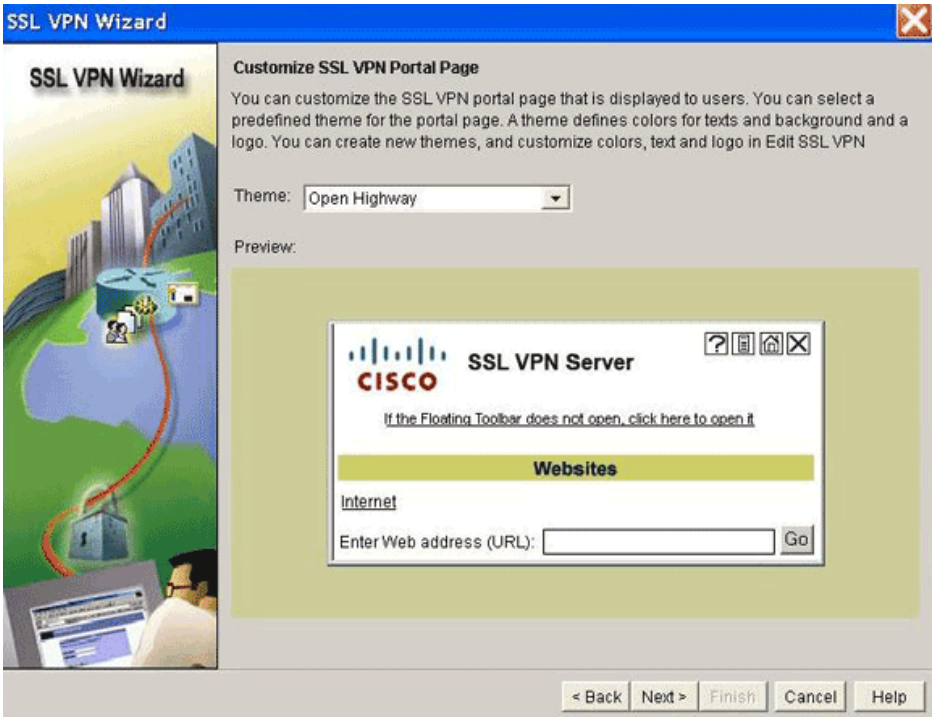
使用同一个接口同时传输安全数据流和非安全数据流的功能称为分割隧道。分割隧道要求明确指定哪个是安全数据流以及该数据流的目标是什么，这样只有指定的数据流进入隧道，而其余数据流则以未加密形式通过公共网络（Internet）进行传输。

例如，请参阅“ASA 8.x：在 ASA 上允许 VPN 客户端分割隧道的配置示例”，其中分步说明了 Cisco AnyConnect VPN 客户端在通过隧道连接至 Cisco 自适应安全设备（ASA）8.0.2 时如何实现 Internet 访问。

10. 完成必要选项配置后，单击 Next。

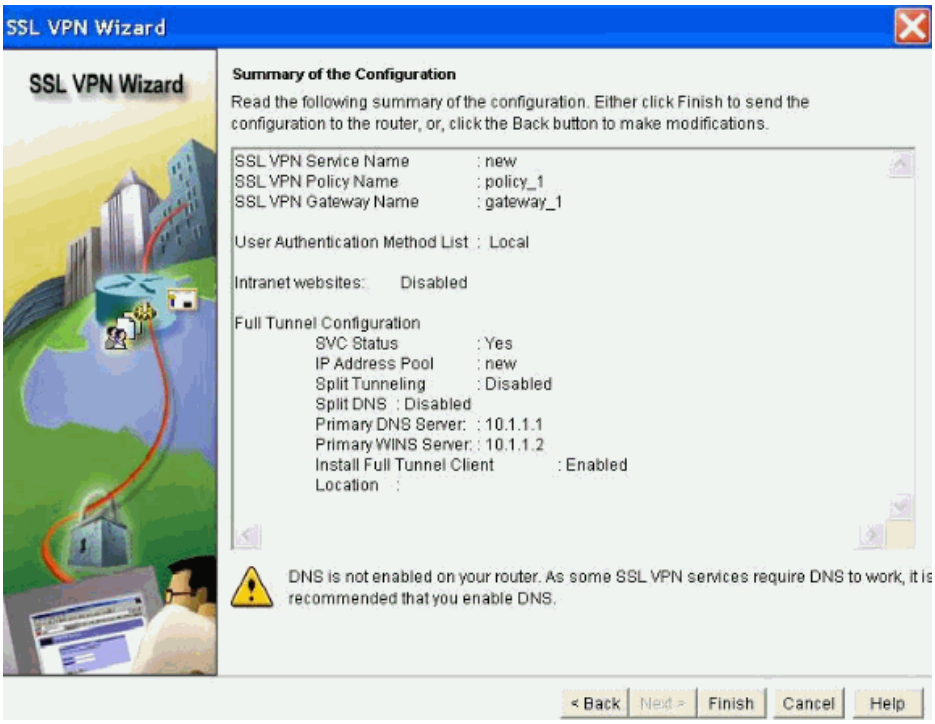
11. 自定义 SSL VPN 门户页或选择默认值。

通过 Customize SSL VPN Portal Page 可以自定义向客户显示 SSL VPN 门户页的方式。



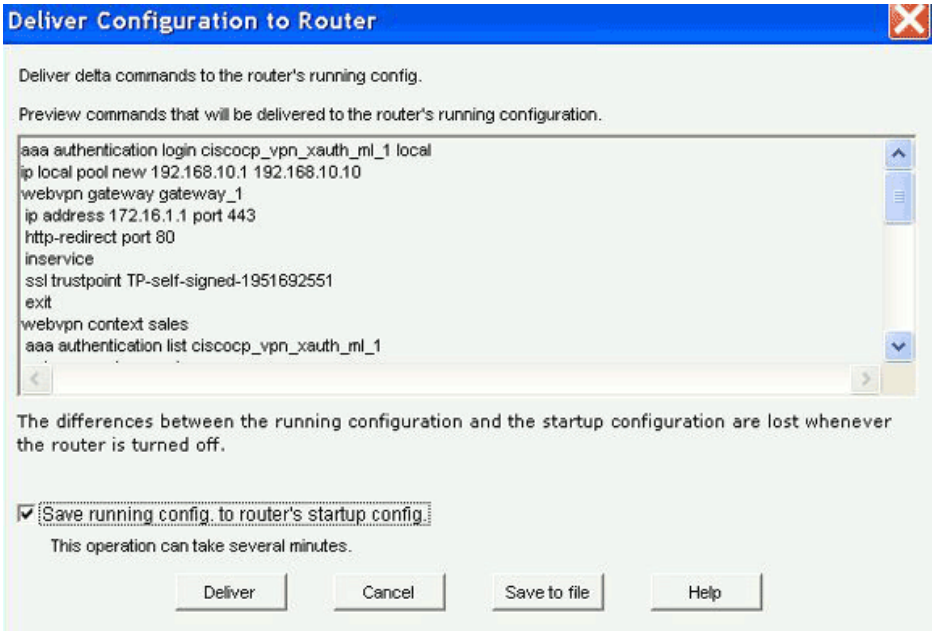
12. 完成自定义 SSL VPN 门户页后，单击 Next。

13. 单击 完成。



14. 单击 Deliver 保存配置，然后单击 OK。

SSL VPN 向导将浏览命令提交至路由器。

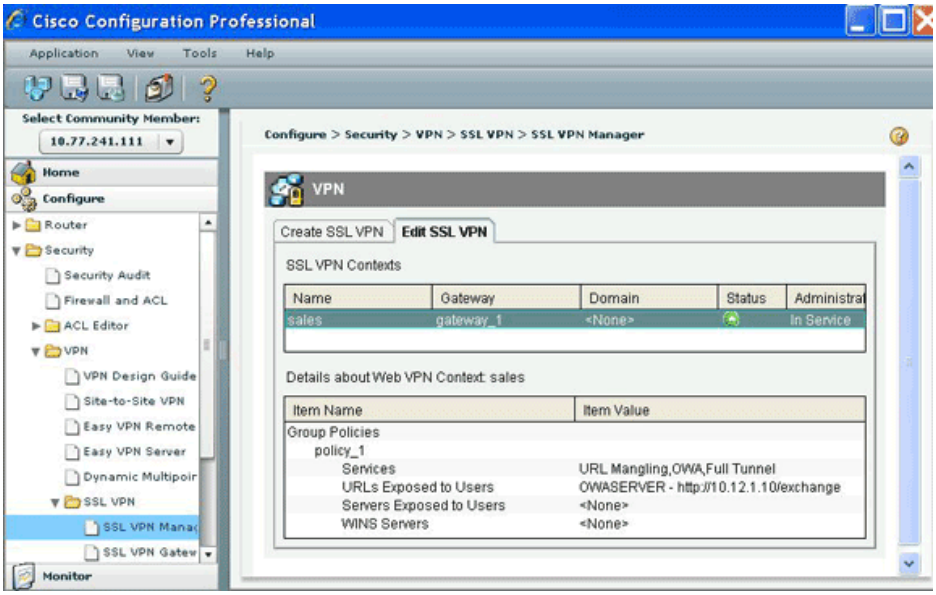


注意： 如果收到错误消息，则可能是 SSL VPN 许可证错误。

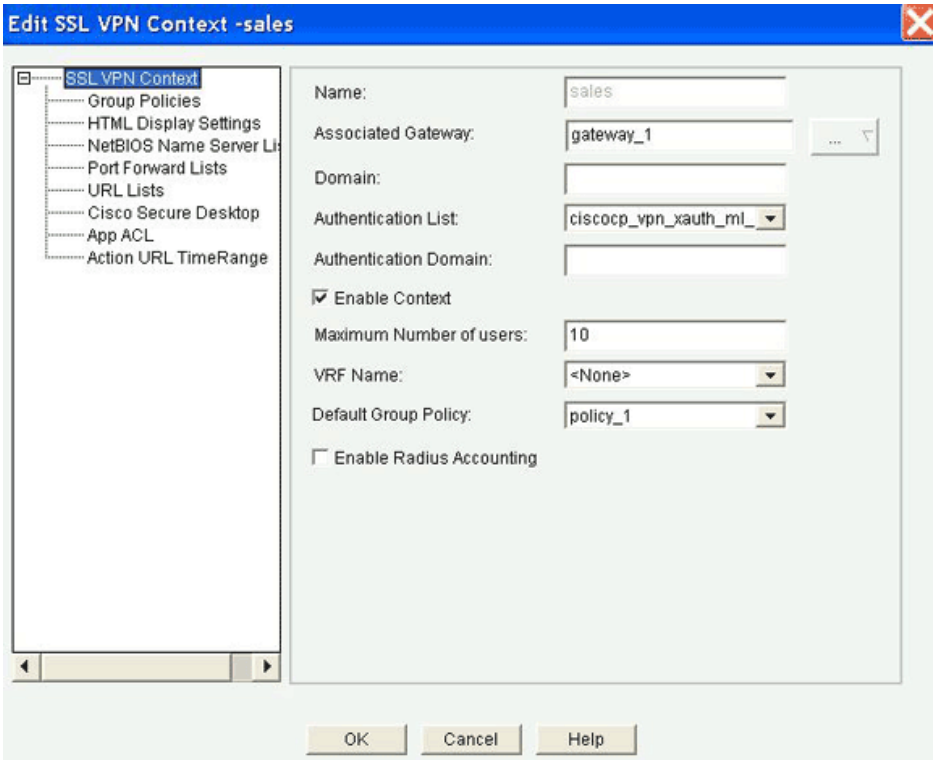
要解决许可证问题，完成以下步骤：

a. 选择 Configure > Security > VPN，然后单击 SSL VPN。

b. 单击 SSL VPN Manager，然后单击右侧 Edit SSL VPN 选项卡。



c. 突出显示新建的上下文，并单击 Edit button。



d. 在 Maximum Number of users 字段中，输入许可证允许的正确用户数。

e. 单击 OK，然后单击 Deliver。

您的命令已写入配置文件。

CLI 配置

CCP 创建以下命令行配置：

路由器

```
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
```

建立 AnyConnect VPN 客户端连接

要与路由器建立 AnyConnect VPN 连接，完成以下步骤。

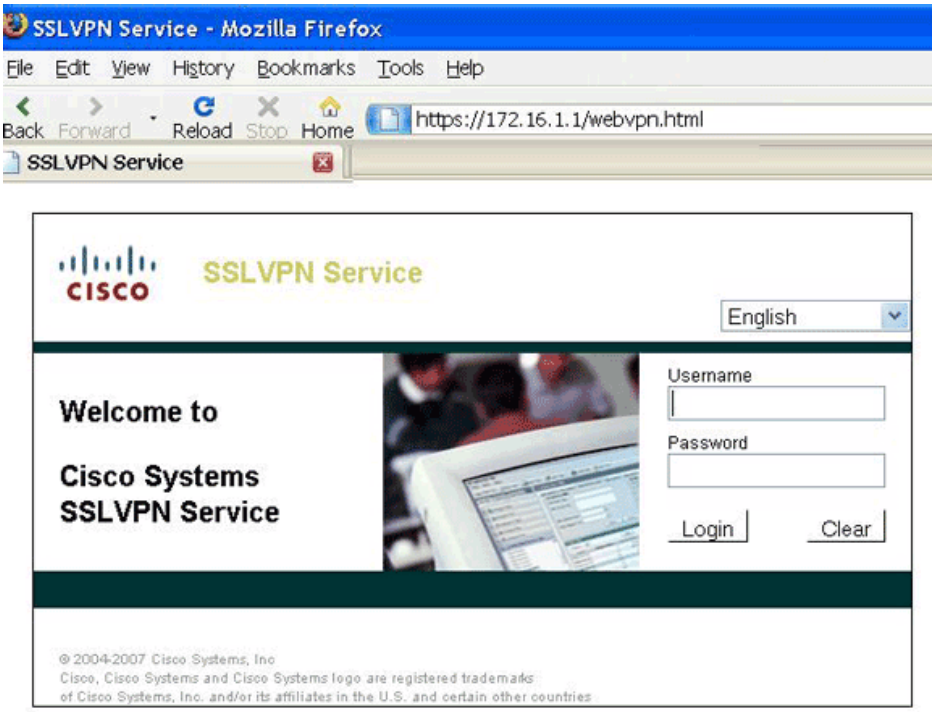
注意： 在 Internet Explorer 中，将路由器添加至受信任的站点列表。有关详细信息，请参考“将安全设备/路由器添加至受信任的站点列表 (IE)”。

1. 按如下格式在 Web 浏览器中输入路由器 WebVPN 接口的 URL 或 IP 地址。

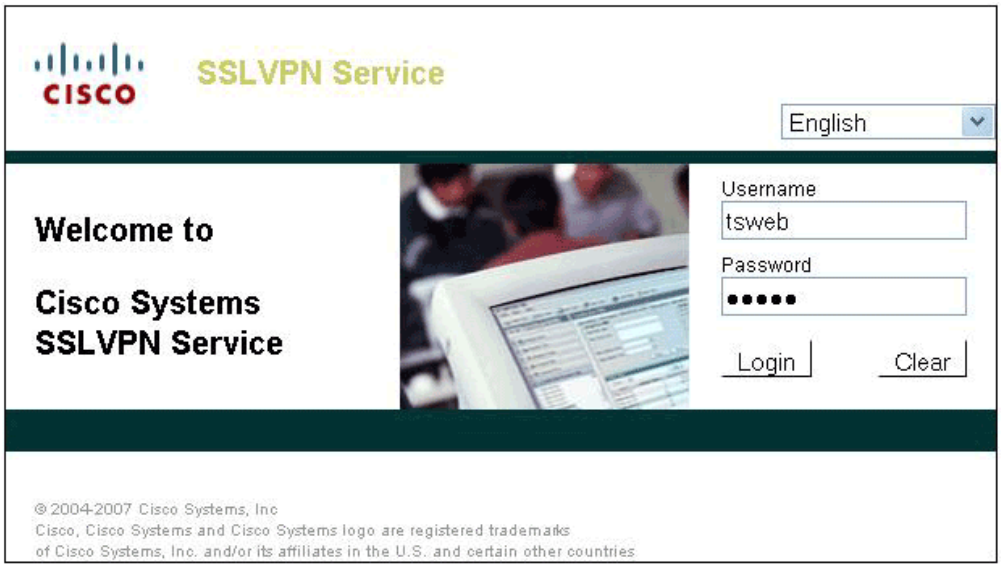
   ```
   https://<url>
   ```

   或者

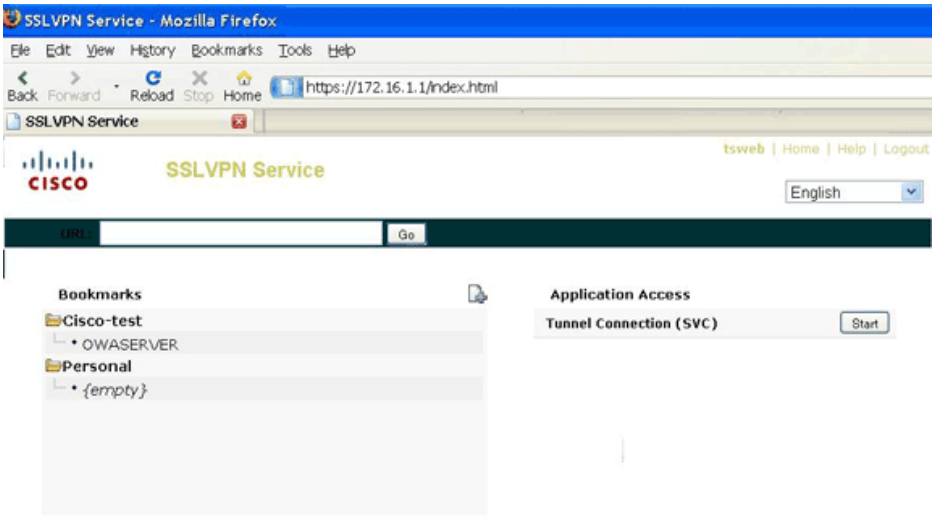
   ```
   https://<IP address of the Router WebVPN interface>
   ```



2. 输入您的用户名和密码。



3. 单击 Start 按钮启动 Anyconnect VPN 隧道连接。



4. 在 SSL VPN 连接建立之前，将会出现以下窗口。

注意： 下载 Anyconnect 前，计算机上必须已安装 ActiveX 软件。

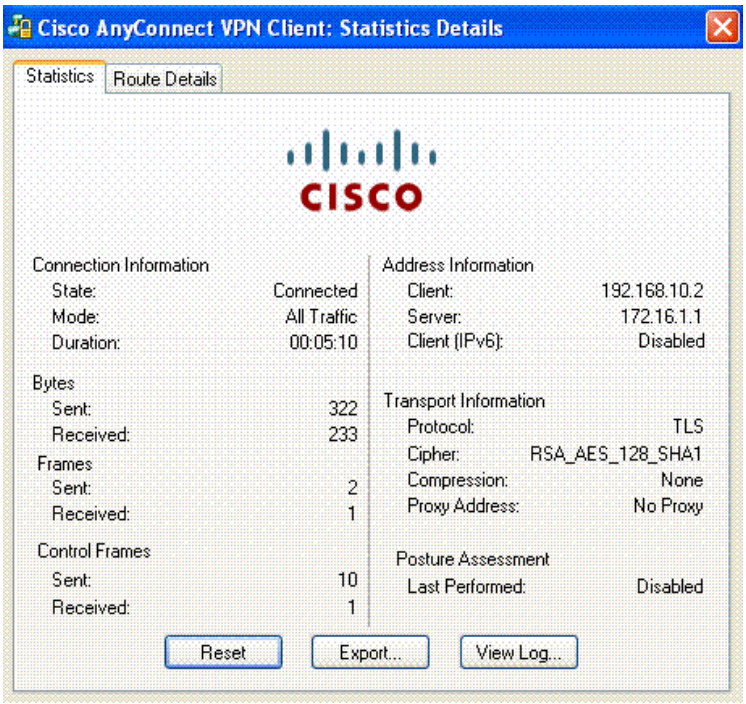
客户端成功连接后，会显示 Connection Established 消息。

5. 成功建立连接后，单击 Statistics 选项卡。

   Statistics 选项卡将显示关于 SSL 连接的信息。

6. 单击 Details。

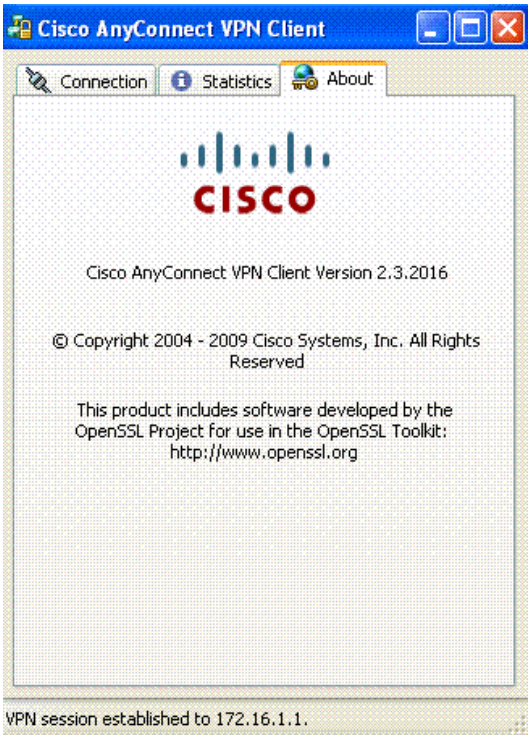
   此时将出现 Cisco AnyConnect VPN Client:Statistics Detail 对话框。



   Statistics Details 对话框显示详细的连接统计信息，包括隧道状态和模式、连接持续时间、发送和接收的字节数和帧数、地址信息、传输信息以及 Cisco Secure Desktop 状态评估状态。通过该选项卡上的 Reset 按钮可重置传输统计数据。使用 Export 按钮可将当前的统计数据、接口和路由表导出至文本文件。AnyConnect 客户端将提示您输入文本文件的名称和位置。默认名称是 AnyConnect-ExportedStats.txt，默认位置是桌面。

7. 在 Cisco AnyConnect VPN Client 对话框中，单击 About 选项卡。

   该选项卡显示了 Cisco AnyConnect VPN 客户端的版本信息。



验证

使用本部分可确认配置能否正常运行。

命令

有若干 show 命令与 WebVPN 关联。可以在命令行界面 (CLI) 上执行这些命令以显示统计信息和其他信息。有关 show 命令的详细信息，请参阅验证 WebVPN 配置。

注意： 命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

- ```
  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

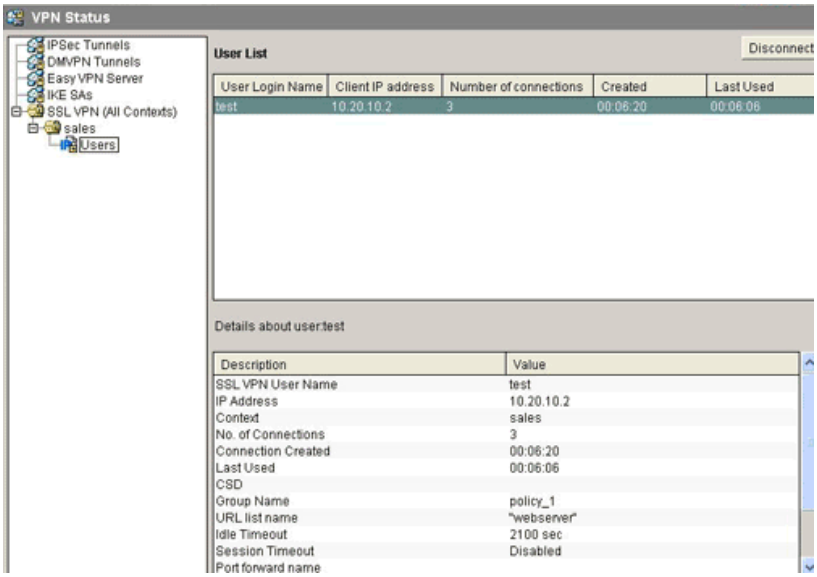
ACL statistics:
   Permit web request       : 0          Deny web request         : 0
   Permit cifs request      : 0          Deny cifs request        : 0
   Permit without ACL       : 0          Deny without match ACL   : 0
   Permit with match ACL    : 0          Deny with match ACL      : 0

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

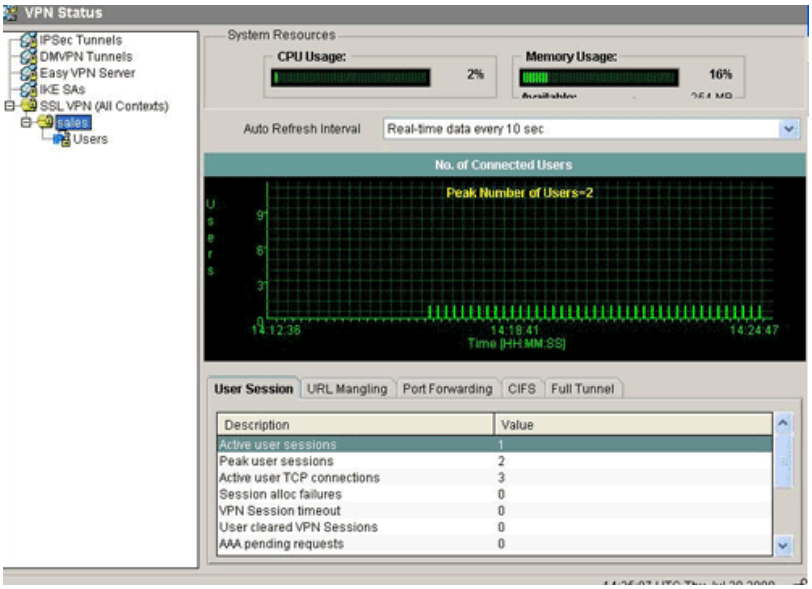
URL-rewrite splitter statistics:
   Direct access request    : 0          Redirect request         : 0
   Internal request         : 0

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
```

- 在 CCP 中，选择 Monitoring > Security > VPN Status > SSL VPN > Users，查看路由器中的当前 SSL VPN 用户列表。



- 选择 Monitoring > Security > VPN Status > SSL VPN > Sales，查看路由器中的当前 SSL VPN 会话信息。



排除故障

使用本部分可排除配置故障。

SSL 连接问题

问题：SSL VPN 客户端无法连接路由器。

解决方案：导致该问题的原因可能是 IP 地址池中的地址不足。可增加路由器 IP 地址池中的地址数，以解决该问题。

有关 AnyConnect VPN 客户端问题故障排除的详细信息，请参阅“AnyConnect VPN 客户端常见问题解答”。

Error:SSLVPN Package SSL-VPN-Client :installed Error:磁盘

问题：在路由器上安装 SVC 程序包时，可能会收到以下错误消息：SSLVPN Package SSL-VPN-Client :installed Error:磁盘。

解决方案：该错误可通过重新格式化闪存解决。

故障排除命令

有若干 clear 命令与 WebVPN 关联。有关这些命令的详细信息，请参阅“使用 WebVPN Clear 命令”。

有若干 debug 命令与 WebVPN 关联。有关这些命令的详细信息，请参阅使用 WebVPN Debug 命令。

注意： 使用 debug 命令可能会对 Cisco 设备造成负面影响。使用 debug 命令之前，请参阅有关 Debug 命令的重要信息。

相关信息

- AnyConnect VPN 客户端常见问题
- Cisco AnyConnect VPN 客户端管理员指南 2.3 版
- SSL VPN - WebVPN
- 有 SDM 的 Cisco IOS 的无客户端 SSL VPN (WebVPN) 配置示例
- 使用 SDM 的瘦客户端 SSL VPN (WebVPN) IOS 配置示例
- 配置示例和技术说明

文件创建日期：2013 年 8 月 5 日