ASA 8.x :在ASA上允许AnyConnect VPN客户端分割隧道配置示例

目录

简介
先决条件
要求
使用的组件
规则
背景信息
配置
网络图
使用 ASDM 6.0(2) 配置 ASA
ASA CLI 配置
使用 SVC 建立 SSL VPN 连接
验证
故障排除
相关信息

简介

本文档提供了有关如何允许Cisco AnyConnect VPN客户端在通过隧道连接到思科自适应安全设备(ASA)8.0.2时访问互联网的分步说明。此配置允许客户端通过SSL安全访问企业资源，同时使用分割隧道对互联网进行不安全访问。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- ASA 安全设备需要运行版本 8.x
- Cisco AnyConnect VPN Client 2.x**注意：**从思科软件下载（仅限注册客户）下载AnyConnect VPN客户端软件包(anyconnect-win*.pkg)(仅限注册客户)。 将 AnyConnect VPN Client 复制到 ASA 的闪存中以供远程用户计算机下载，以便建立与 ASA 的 SSL VPN 连接。有关 ASA 配置指南的详细信息，请参阅安装 AnyConnect 客户端部分。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行软件版本 8.0(2) 的 Cisco 5500 系列 ASA
- 用于 Windows 的 Cisco AnyConnect SSL VPN Client 版本 2.0.0343
- 运行 Microsoft Visa、Windows XP SP2 或 Windows 2000 Professional SP4 并且具有 Microsoft Installer 版本 3.1 的 PC
- Cisco 自适应安全设备管理器 (ASDM) 版本 6.0(2)

本文档中的信息都是基于特定实验室环境中的设备编写的。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。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

背景信息

Cisco AnyConnect VPN Client 为远程用户的安全设备提供了安全的 SSL 连接。如果以前未安装客户端，则远程用户可以在浏览器中输入已配置为接受 SSL VPN 连接的接口的 IP 地址。除非安全设备被配置为将 http:// requests 重定向到 https://，否则用户必须输入 https://<address> 形式的 URL。

输入 URL 后，浏览器将连接到此接口并显示登录屏幕。如果用户满足登录名和身份验证要求，并且安全设备将用户识别为需要客户端的用户，它将下载匹配远程计算机操作系统的客户端。下载完成后，客户端将自行安装并进行配置，建立一个安全 SSL 连接，并在连接终止时保留或卸载自身（根据安全设备配置）。

如果以前安装了客户端，则当用户验证身份时，安全设备将会检查客户端的版本，并根据需要升级客户端。

当客户端与安全设备协商 SSL VPN 连接时，它将使用传输层安全 (TLS) 以及可选的数据报传输层安全 (DTLS) 进行连接。使用 DTLS 可避免与某些 SSL 连接有关的延迟和带宽问题，并改进对数据包延迟敏感的实时应用程序的性能。

AnyConnect 客户端可以从安全设备下载，或者可以由系统管理员手动安装到远程 PC 上。有关如何手动安装客户端的详细信息，请参阅《Cisco AnyConnect VPN客户端管理员指南》。

安全设备将根据组策略或建立连接的用户的用户名属性下载客户端。您可以配置安全设备自动下载客户端，或者将其配置为提示远程用户选择是否下载客户端。在后一种情况下，如果用户不响应，您可以配置安全设备在超时时间后下载客户端或显示登录页。

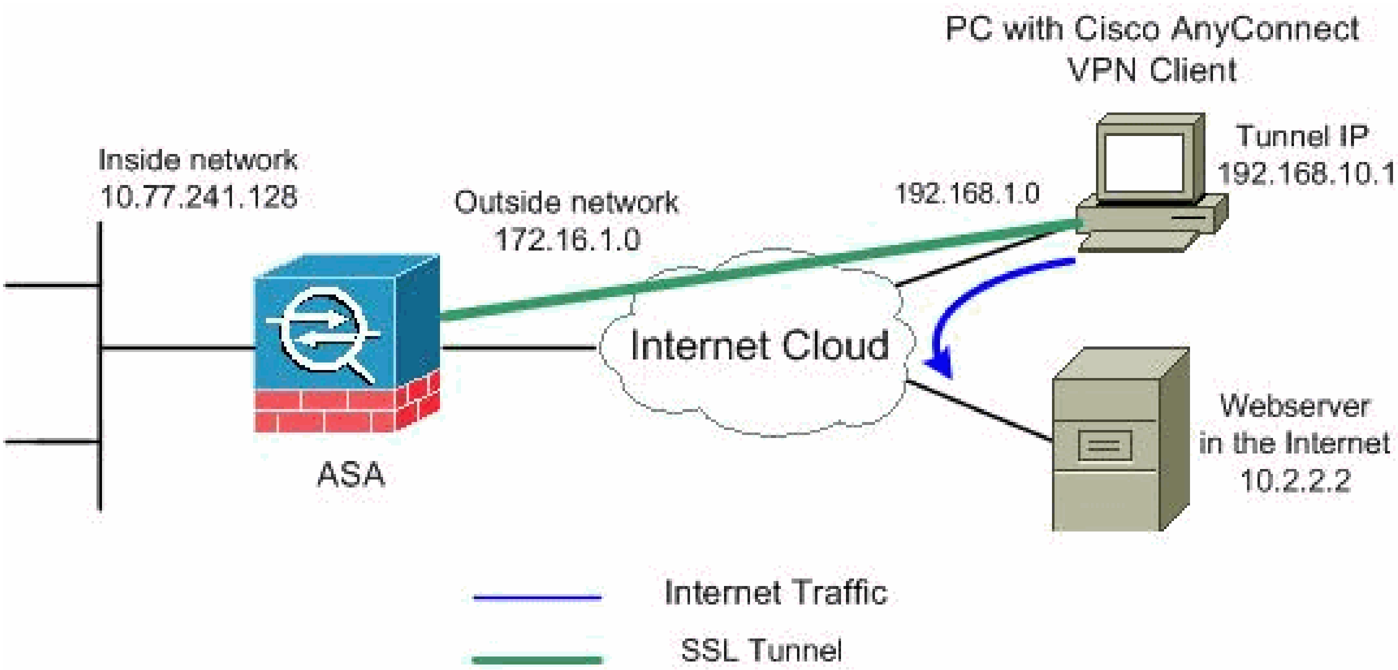
配置

本部分提供有关如何配置本文档所述功能的信息。

注意：使用命令查找工具(仅限注册客户)可获取有关本节中使用的命令的详细信息。

网络图

本文档使用以下网络设置：


PC with Cisco AnyConnect VPN Client
Tunnel IP 192.168.10.1
192.168.1.0
Inside network 10.77.241.128
Outside network 172.16.1.0
Internet Cloud
ASA
Webserver in the Internet 10.2.2.2
Internet Traffic
SSL Tunnel

注意：此配置中使用的IP编址方案在Internet上不可合法路由。这些地址是在实验室环境中使用的 RFC 1918 地址。

使用 ASDM 6.0(2) 配置 ASA

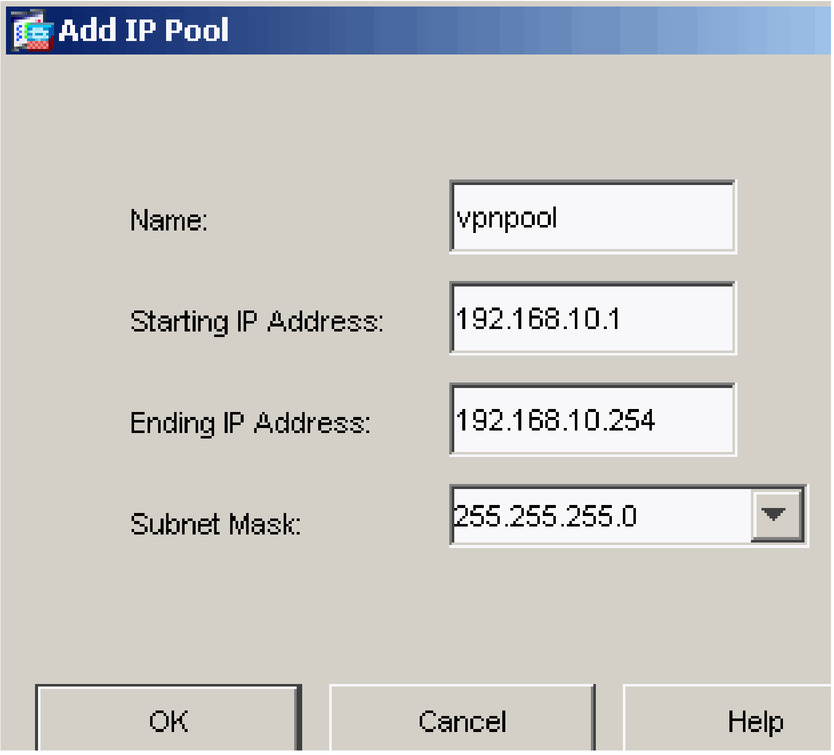
本文档假设基本配置（例如接口配置）已完成并且可以正常工作。

注意：请参阅允许ASDM的HTTPS访问，以便允许ASDM配置ASA。

注意：除非更改端口号，否则无法在同一ASA接口上启用WebVPN和ASDM。有关详细信息，请参阅在相同 ASA 接口上同时启用 Webvpn 和 ASDM。

要在 ASA 上为 SSL VPN 配置分割隧道，请执行以下步骤：

1. 选择 **Configuration > Remote Access VPN > Network (Client) Access > Address Management > Address Pools > Add 以创建 IP 地址池 vpnpool。**



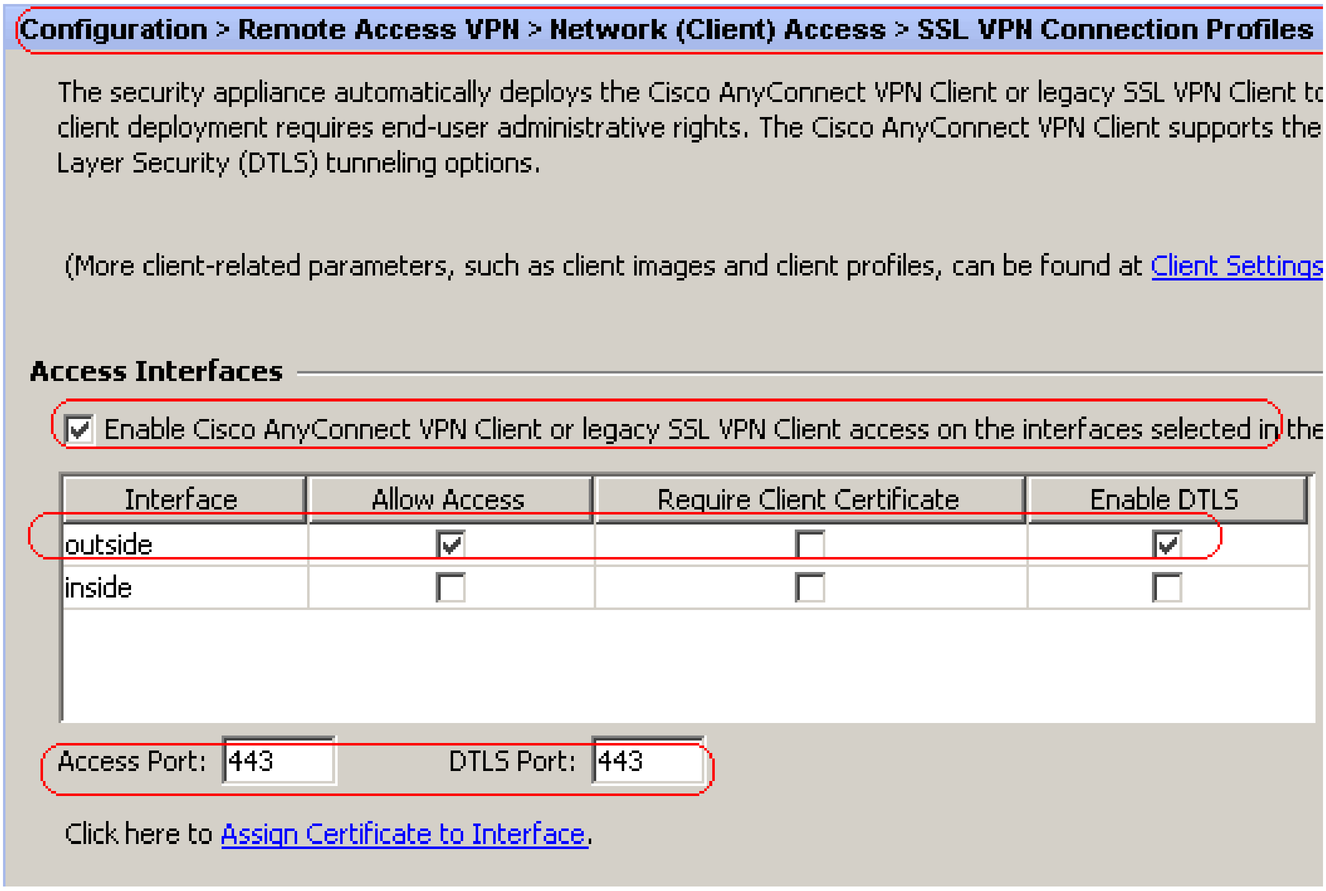
Name: vpnpool

Starting IP Address: 192.168.10.1

Ending IP Address: 192.168.10.254

Subnet Mask: 255.255.255.0

2. 单击 Apply。等效 CLI 配置：
3. 启用 Webvpn。选择 Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles，然后在 Access Interfaces 下选中外部接口的 Allow Access 和 Enable DTLS 复选框。此外，请选中 Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interface selected in the table below 复选框，以对外部接口启用 SSL VPN。



Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles

The security appliance automatically deploys the Cisco AnyConnect VPN Client or legacy SSL VPN Client to
client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports the
Layer Security (DTLS) tunneling options.

(More client-related parameters, such as client images and client profiles, can be found at Client Settings

Access Interfaces

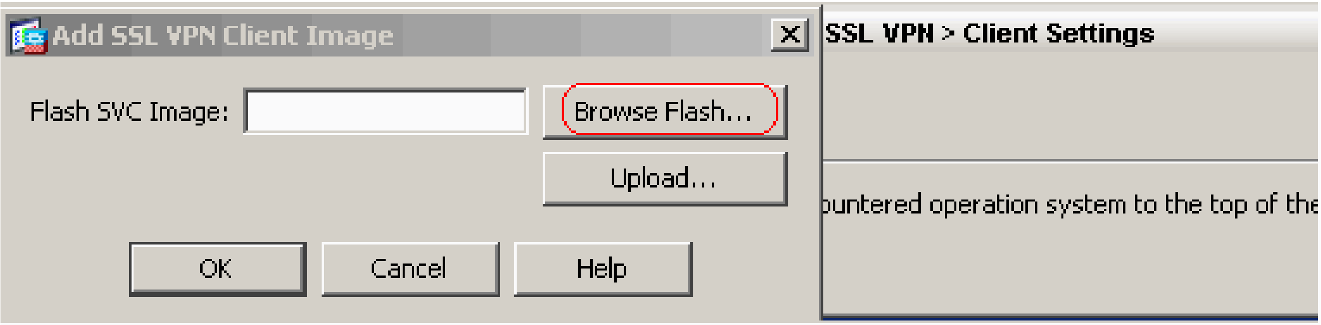
☑ Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interfaces selected in the

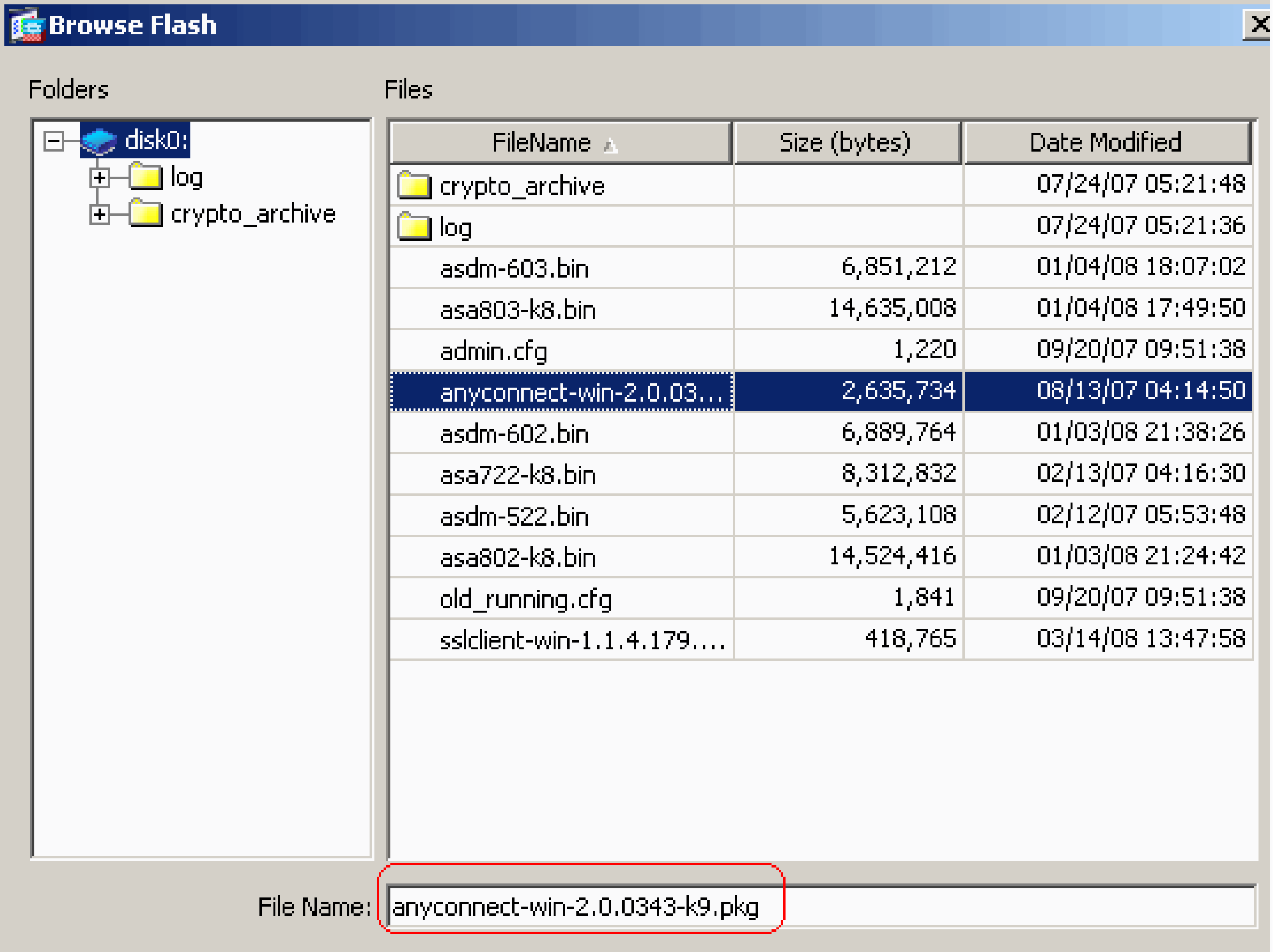
Interface	Allow Access	Require Client Certificate	Enable DTLS
outside	☑	□	☑
inside	□	□	□

Access Port: 443 DTLS Port: 443

Click here to Assign Certificate to Interface.

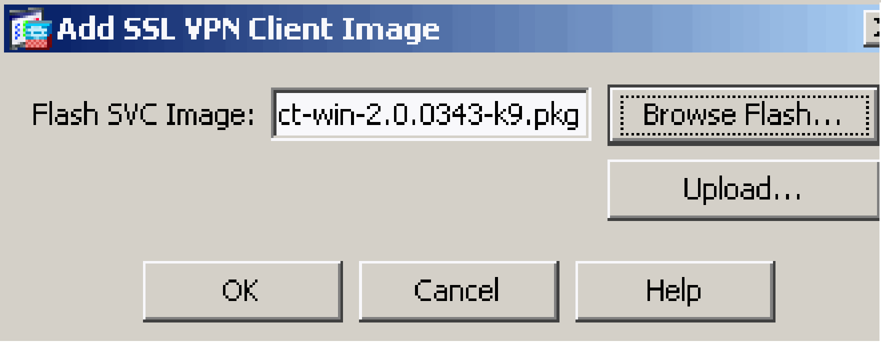
单击 Apply。选择 Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings > Add，以便从 ASA 闪存中添加 Cisco AnyConnect VPN Client 映像，如下所示。





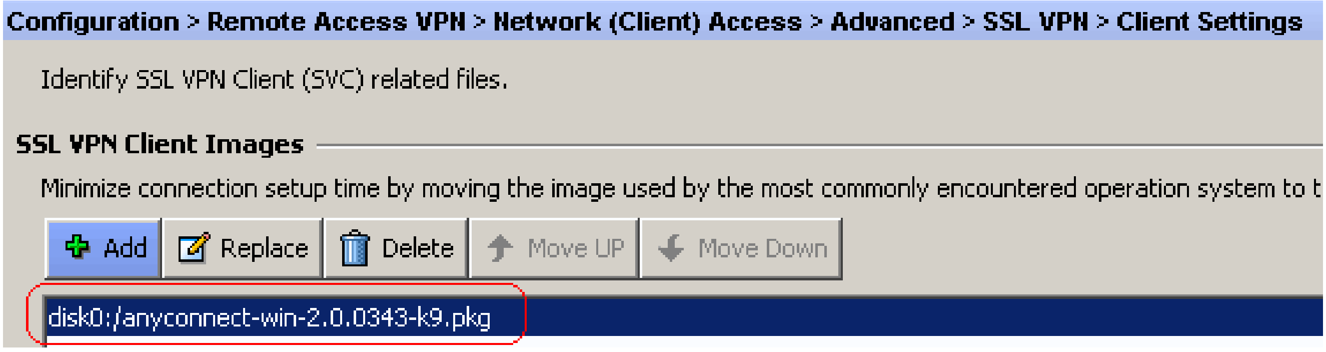
FileName	Size (bytes)	Date Modified
crypto_archive		07/24/07 05:21:48
log		07/24/07 05:21:36
asdm-603.bin	6,851,212	01/04/08 18:07:02
asa803-k8.bin	14,635,008	01/04/08 17:49:50
admin.cfg	1,220	09/20/07 09:51:38
anyconnect-win-2.0.03...	2,635,734	08/13/07 04:14:50
asdm-602.bin	6,889,764	01/03/08 21:38:26
asa722-k8.bin	8,312,832	02/13/07 04:16:30
asdm-522.bin	5,623,108	02/12/07 05:53:48
asa802-k8.bin	14,524,416	01/03/08 21:24:42
old_running.cfg	1,841	09/20/07 09:51:38
sslclient-win-1.1.4.179....	418,765	03/14/08 13:47:58

File Name: anyconnect-win-2.0.0343-k9.pkg



Flash SVC Image: ct-win-2.0.0343-k9.pkg

Click **OK.** 单击 **Add**。



Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings

Identify SSL VPN Client (SVC) related files.

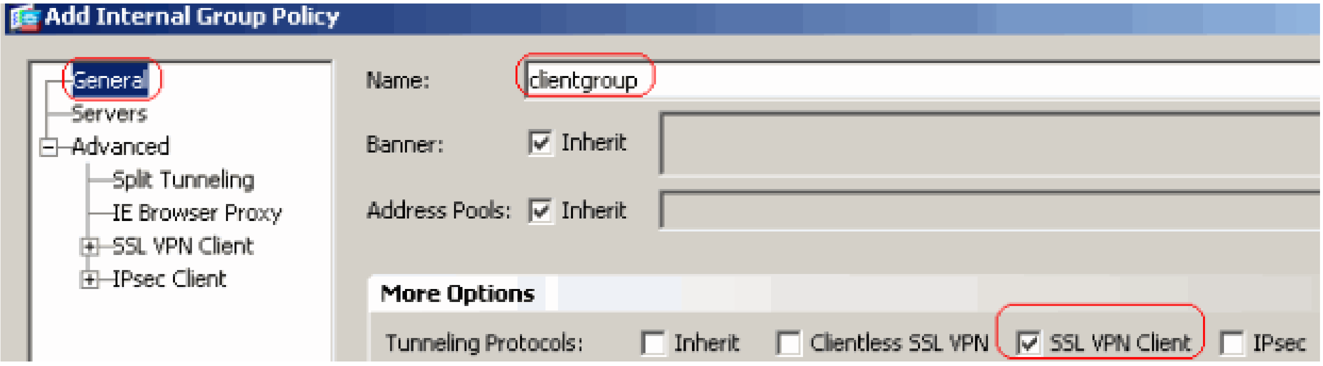
SSL VPN Client Images

Minimize connection setup time by moving the image used by the most commonly encountered operation system to t

disk0:/anyconnect-win-2.0.0343-k9.pkg

等效 CLI 配置：

4. 配置组策略。选择 **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** 以创建内部组策略 **clientgroup**。在 **General** 选项卡下，选中 **SSL VPN Client** 复选框以启用 WebVPN 作为隧道协议。



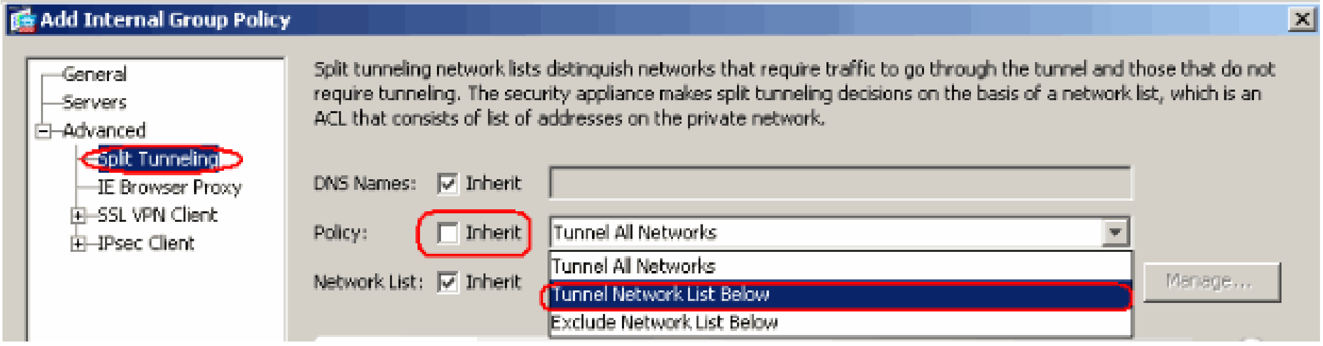
Name: clientgroup

Banner: ☑ Inherit

Address Pools: ☑ Inherit

Tunneling Protocols: □ Inherit □ Clientless SSL VPN ☑ SSL VPN Client □ IPsec

在 **Advanced > Split Tunneling** 选项卡中，取消选中 **Split Tunnel Policy** 的 **Inherit** 复选框，并从下拉列表中选择 **Tunnel Network List Below**。



Split tunneling network lists distinguish networks that require traffic to go through the tunnel and those that do not require tunneling. The security appliance makes split tunneling decisions on the basis of a network list, which is an ACL that consists of list of addresses on the private network.

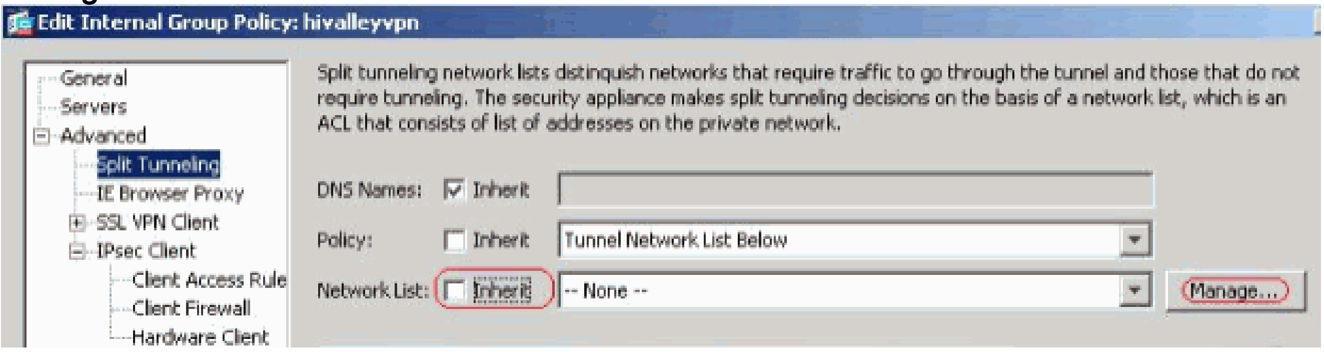
DNS Names: ☑ Inherit

Policy: □ Inherit Tunnel All Networks

- Tunnel All Networks
- Tunnel Network List Below
- Exclude Network List Below

Network List: ☑ Inherit

取消选中 Split Tunnel Network List 的 **Inherit** 复选框，然后单击 **Manage** 以启动 **ACL Manager**。



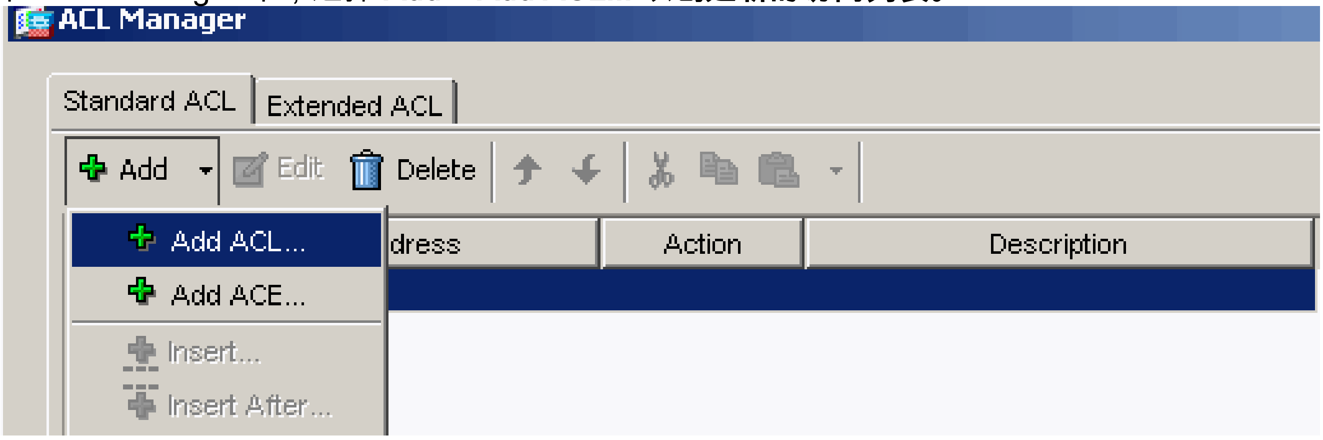
Split tunneling network lists distinguish networks that require traffic to go through the tunnel and those that do not require tunneling. The security appliance makes split tunneling decisions on the basis of a network list, which is an ACL that consists of list of addresses on the private network.

DNS Names: ☑ Inherit

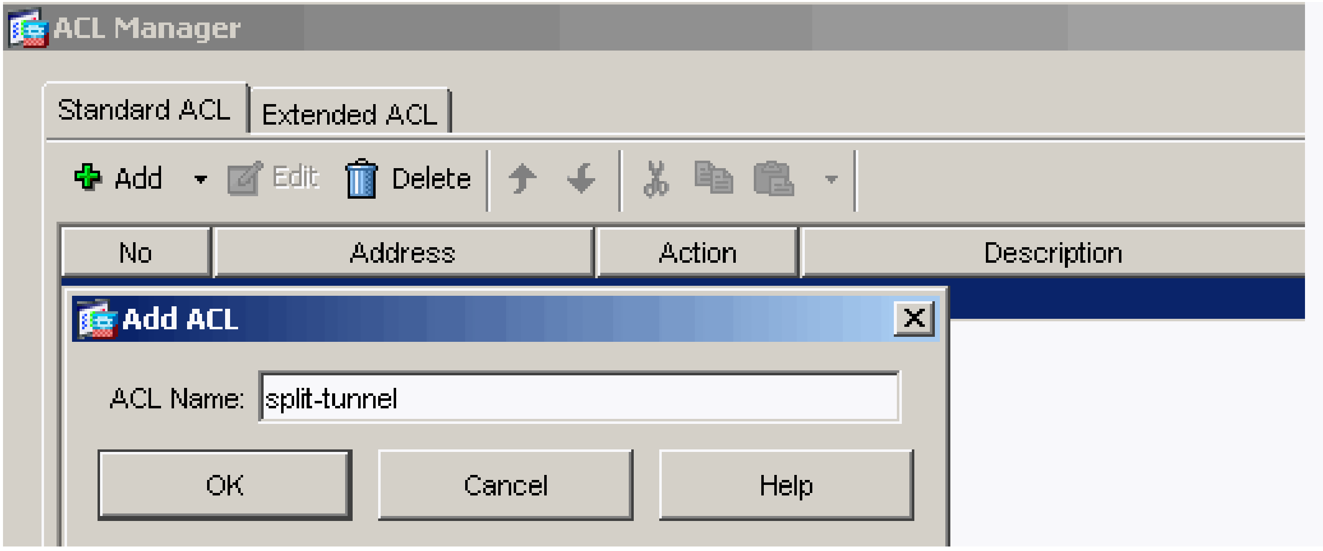
Policy: □ Inherit Tunnel Network List Below

Network List: □ Inherit -- None --

在 ACL Manager 中，选择 **Add > Add ACL...** 以创建新的访问列表。

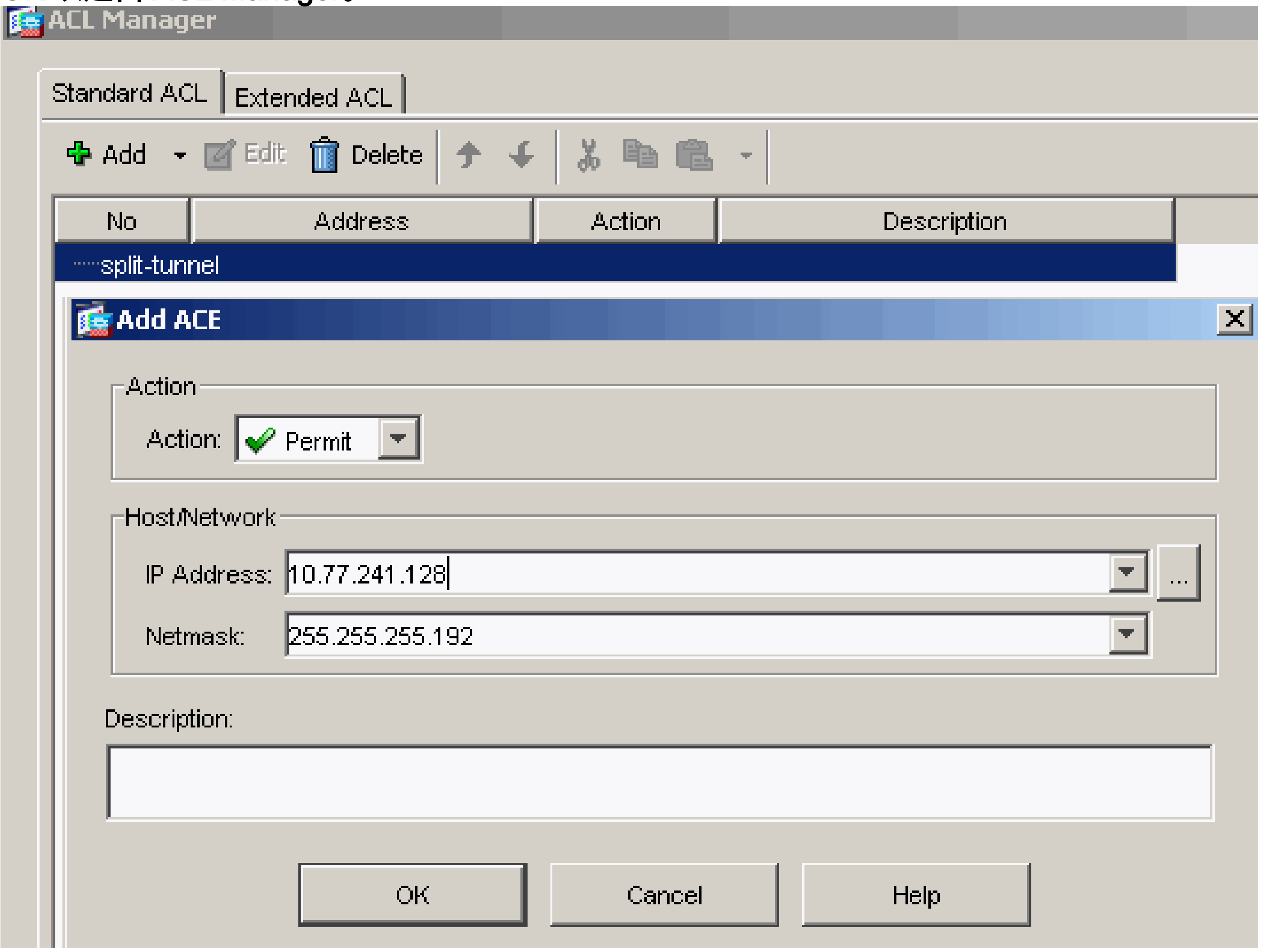


为 ACL 提供一个名称，然后单击 **OK**。



ACL Name: split-tunnel

创建 ACL 名称后，选择 **Add > Add ACE 以添加访问控制项 (ACE)。**定义与 ASA 后的 LAN 对应的 ACE。在本示例中，该网络是 10.77.241.128/26，然后在 Action 中选择 **Permit。**单击 **OK 以退出 ACL Manager。**



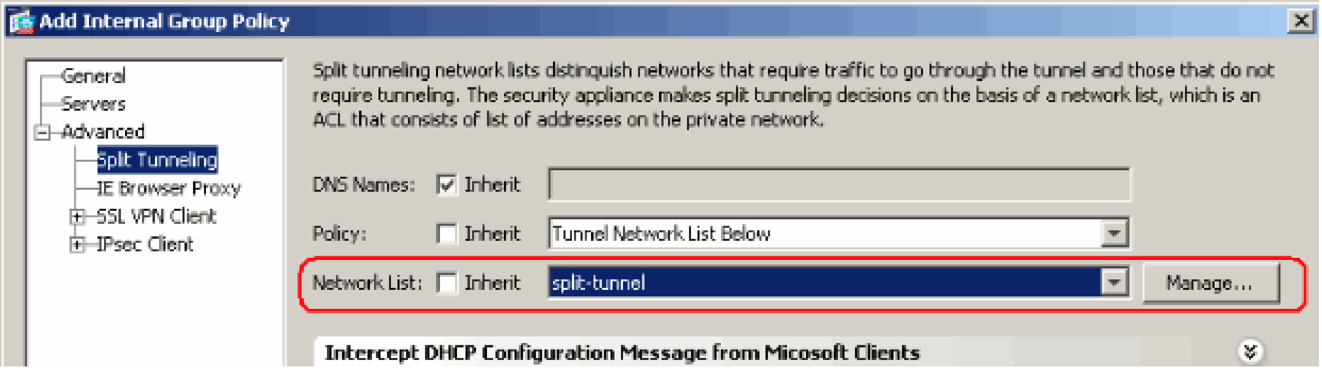
split-tunnel

Action: Permit

IP Address: 10.77.241.128

Netmask: 255.255.255.192

确保在分割隧道的 Network List 中选择刚刚创建的 ACL。单击 **OK 以返回组策略配置。**



Add Internal Group Policy

Split tunneling network lists distinguish networks that require traffic to go through the tunnel and those that do not require tunneling. The security appliance makes split tunneling decisions on the basis of a network list, which is an ACL that consists of list of addresses on the private network.

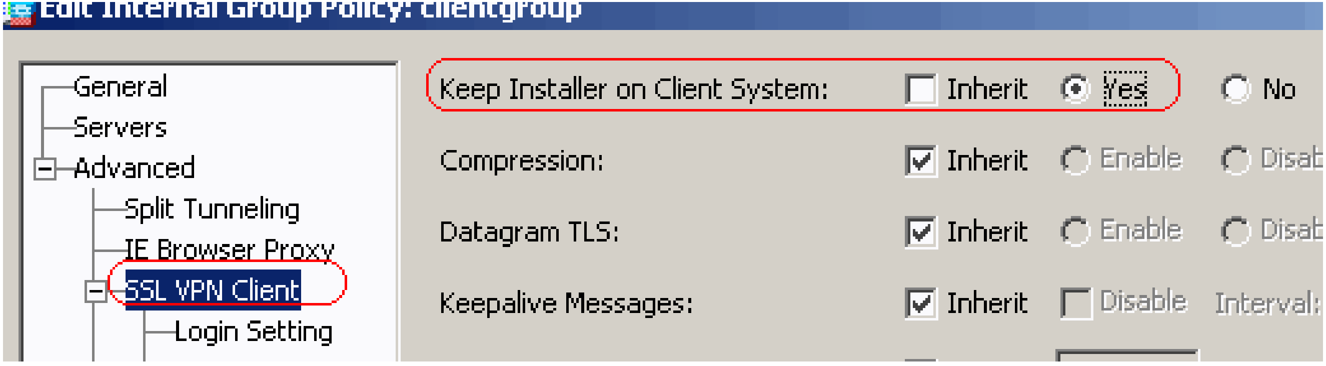
DNS Names: ☑ Inherit

Policy: □ Inherit Tunnel Network List Below

Network List: □ Inherit split-tunnel Manage...

Intercept DHCP Configuration Message from Micosoft Clients

在主页上，单击 **Apply，然后单击 Send（如果需要），以将命令发送到 ASA。**在组策略模式下配置 **SSL VPN 设置。**对于 Keep Installer on Client System 选项，取消选中 **Inherit 复选框，然后单击 Yes 单选按钮。**通过此操作，SVC 软件将保留在客户端计算机上。因此，不必在每次进行连接时都要求 ASA 将 SVC 软件下载到客户端。对于经常访问企业网络的远程用户而言，此选项是一个很好的选择。



Edit Internal Group Policy: clientgroup

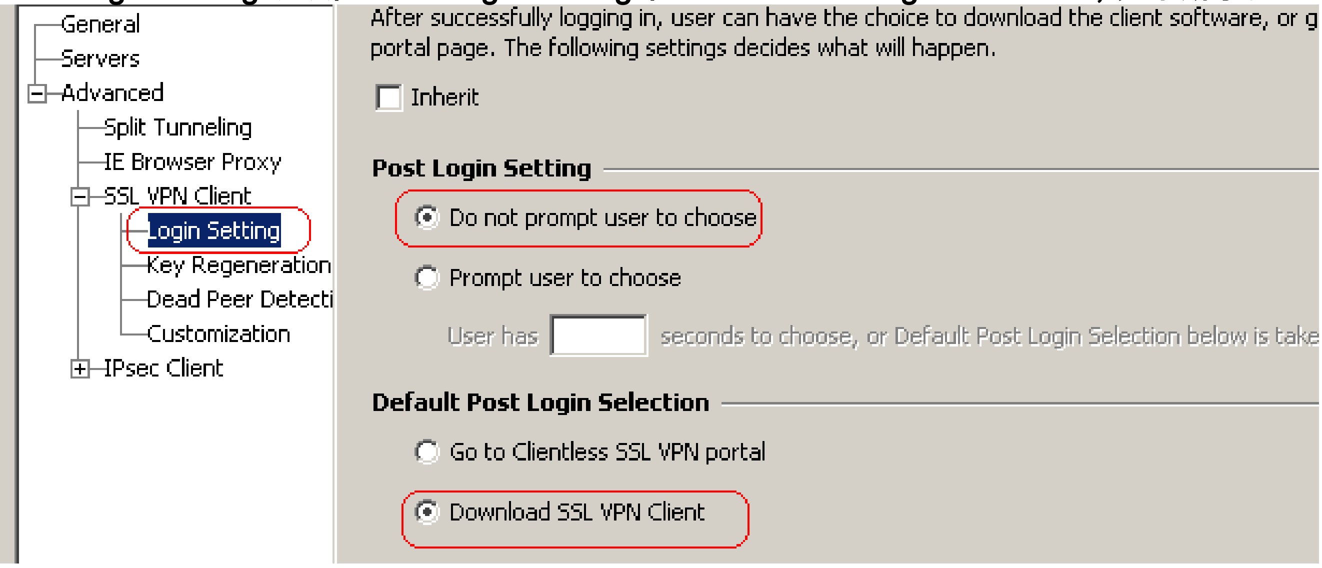
Keep Installer on Client System: □ Inherit ● Yes ○ No

Compression: ☑ Inherit ○ Enable ○ Disab

Datagram TLS: ☑ Inherit ○ Enable ○ Disab

Keepalive Messages: ☑ Inherit □ Disable Interval:

单击 **Login Setting 以设置 Post Login Setting 和 Default Post Login Selection，如下所示。**



After successfully logging in, user can have the choice to download the client software, or g portal page. The following settings decides what will happen.

□ Inherit

Post Login Setting

● Do not prompt user to choose

○ Prompt user to choose

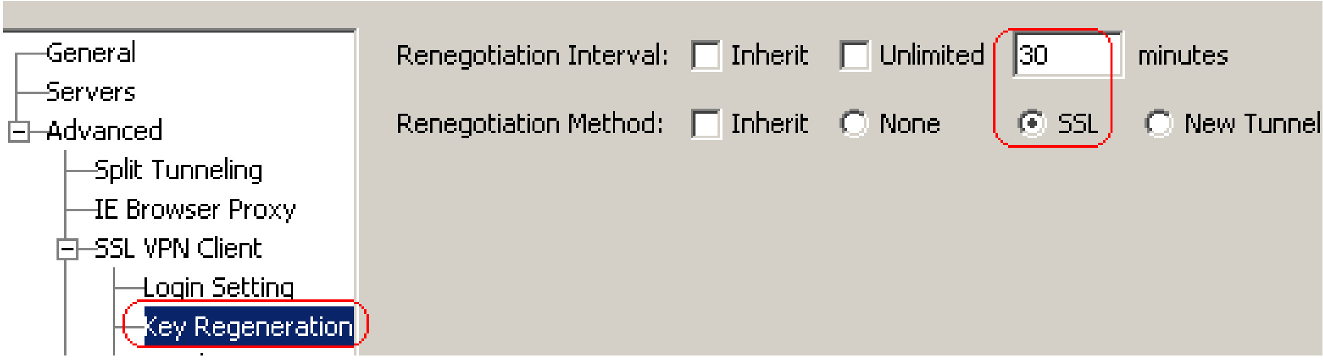
User has [ ] seconds to choose, or Default Post Login Selection below is take

Default Post Login Selection

○ Go to Clientless SSL VPN portal

● Download SSL VPN Client

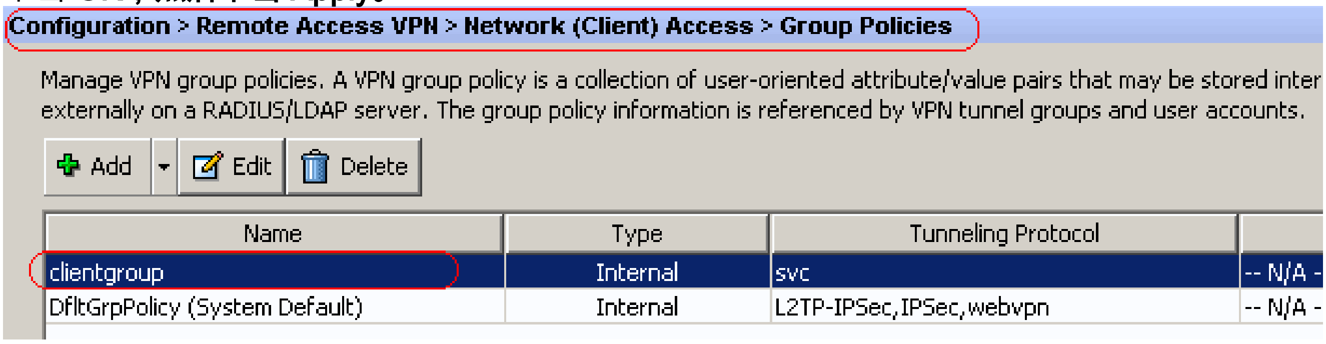
对于 Renegotiation Interval 选项，取消选中 **Inherit 框，取消选中 Unlimited 复选框，然后输入重新生成密钥之前经过的分钟数。**通过设置密钥有效时间限制可增强安全性。对于 Renegotiation Method 选项，取消选中 **Inherit 复选框，然后单击 SSL 单选按钮。**重新协商可以使用当前的 SSL 隧道或为重新协商显式创建的新隧道。



Renegotiation Interval: □ Inherit □ Unlimited 30 minutes

Renegotiation Method: □ Inherit ○ None ● SSL ○ New Tunnel

单击 OK，然后单击 Apply。

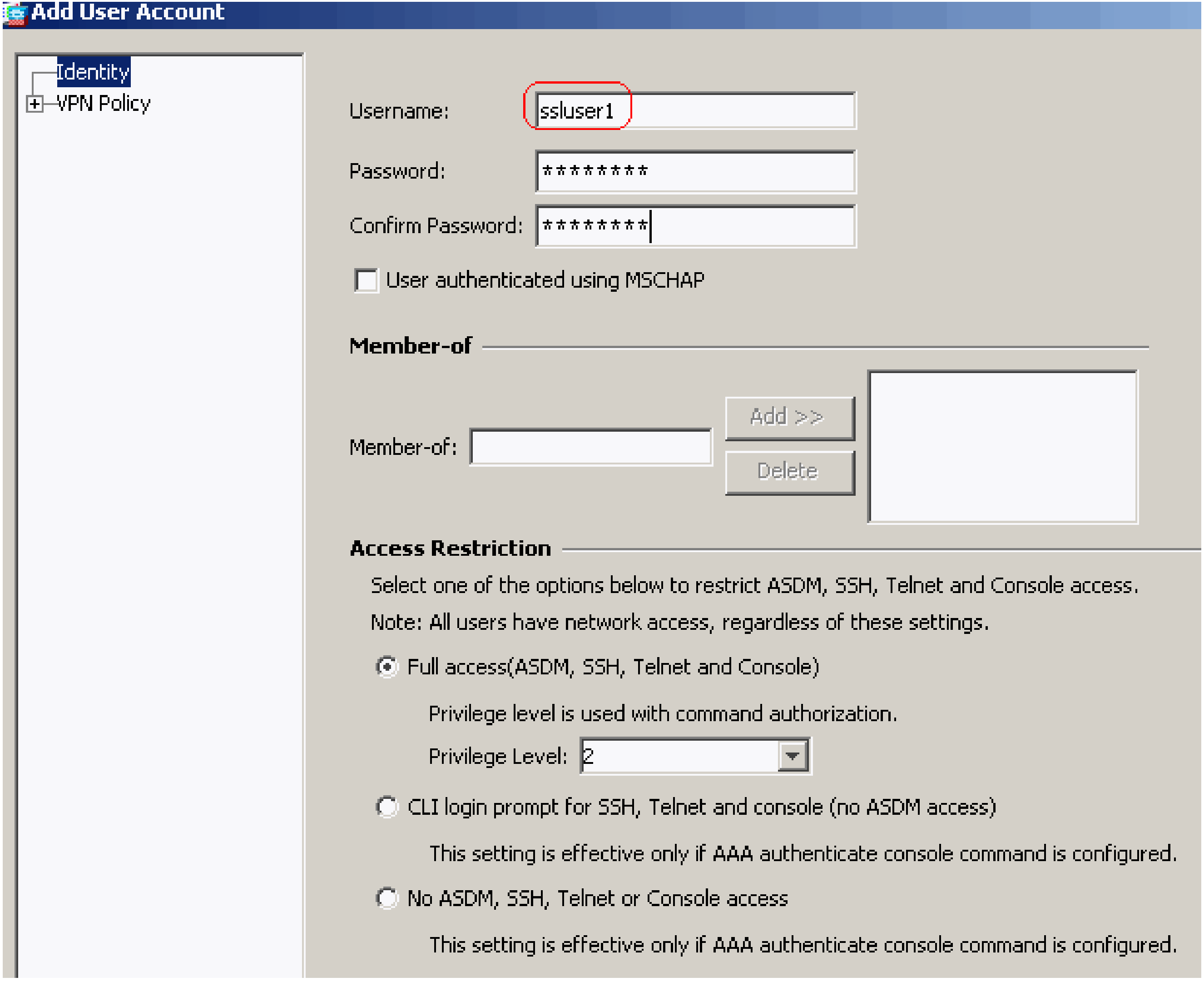

Configuration > Remote Access VPN > Network (Client) Access > Group Policies

Manage VPN group policies. A VPN group policy is a collection of user-oriented attribute/value pairs that may be stored inter externally on a RADIUS/LDAP server. The group policy information is referenced by VPN tunnel groups and user accounts.

Name	Type	Tunneling Protocol	
clientgroup	Internal	svc	-- N/A -
DfltGrpPolicy (System Default)	Internal	L2TP-IPSec,IPSec,webvpn	-- N/A -

等效 CLI 配置：

5. 选择Configuration > Remote Access VPN > AAA Setup > Local Users > Add以创建新的用户帐户ssluser1。单击OK，然后应用。


Add User Account

Username: ssluser1

Password: ********

Confirm Password: ********

□ User authenticated using MSCHAP

Member-of

Member-of:

Access Restriction

Select one of the options below to restrict ASDM, SSH, Telnet and Console access.

Note: All users have network access, regardless of these settings.

● Full access(ASDM, SSH, Telnet and Console)

Privilege level is used with command authorization.

Privilege Level: 2

○ CLI login prompt for SSH, Telnet and console (no ASDM access)

This setting is effective only if AAA authenticate console command is configured.

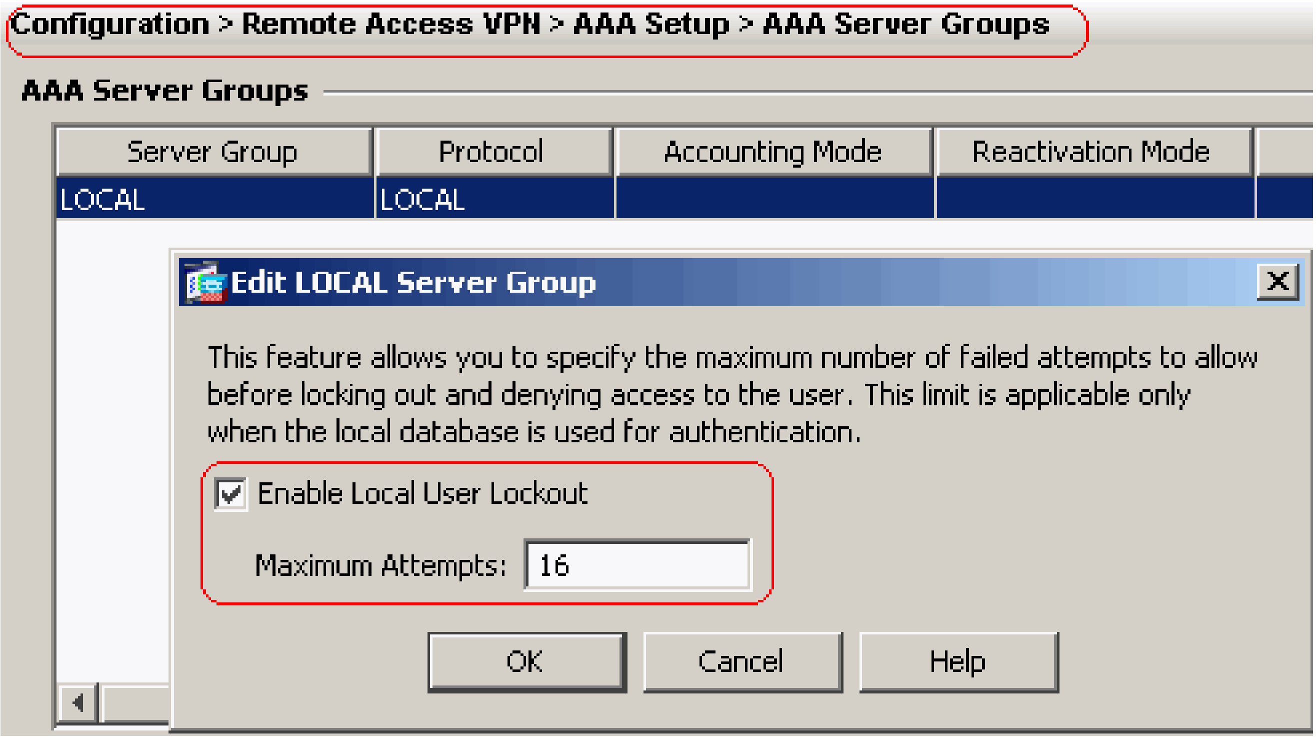
○ No ASDM, SSH, Telnet or Console access

This setting is effective only if AAA authenticate console command is configured.

等效 CLI 配置：

6. 选择 Configuration > Remote Access VPN > AAA Setup > AAA Servers Groups > Edit，以便

通过选中 Enable Local User Lockout 复选框并将 Maximum Attempts 值设为 16，修改默认服务器组 LOCAL。



Configuration > Remote Access VPN > AAA Setup > AAA Server Groups

AAA Server Groups

Server Group	Protocol	Accounting Mode	Reactivation Mode
LOCAL	LOCAL		

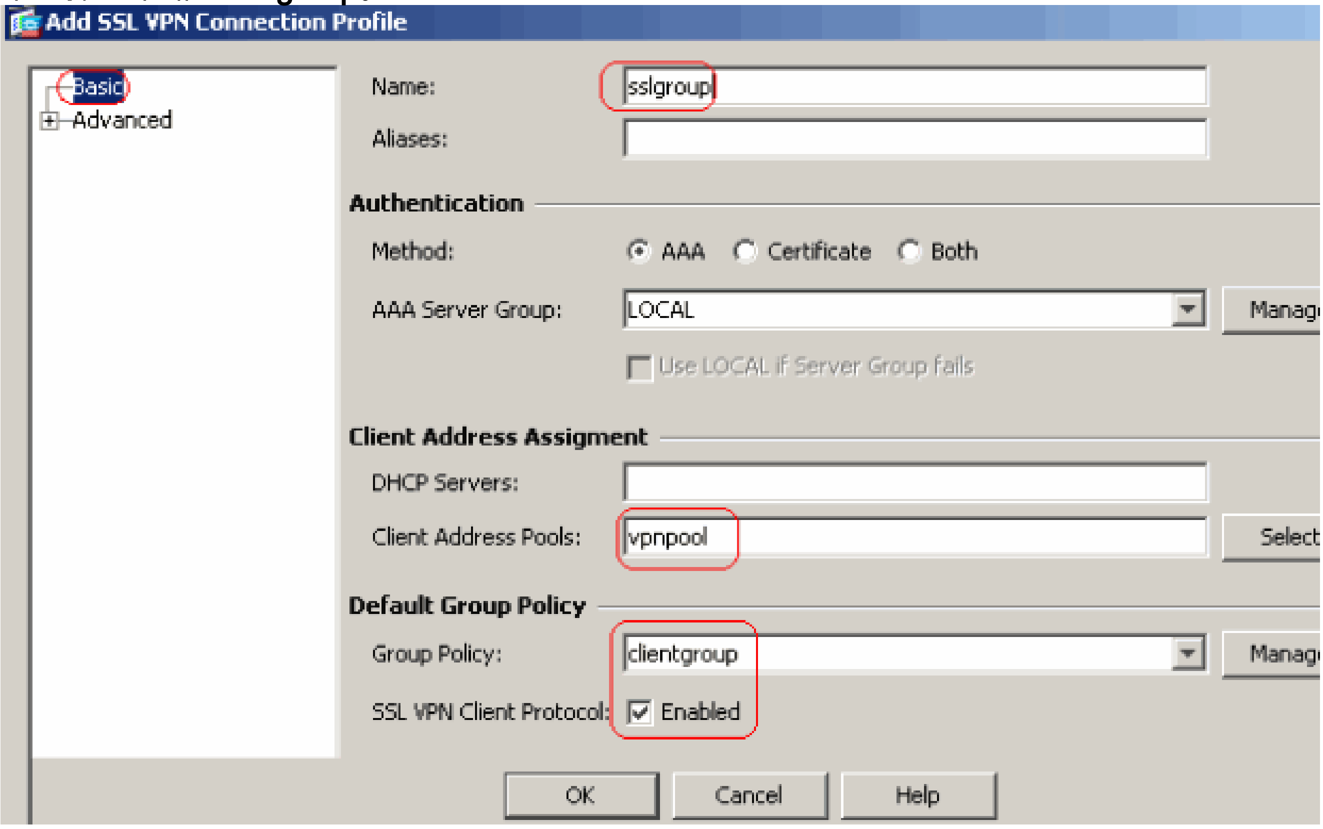
Edit LOCAL Server Group

This feature allows you to specify the maximum number of failed attempts to allow before locking out and denying access to the user. This limit is applicable only when the local database is used for authentication.

☑ Enable Local User Lockout

Maximum Attempts: 16

7. 单击 **OK，然后单击 Apply。等效 CLI 配置：**
8. 配置隧道组。选择 **Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles Connection Profiles > Add 以创建新的隧道组 sslgroup。**在 **Basic 选项卡中，您可以执行如下列出的配置：**将隧道组命名为 **sslgroup。**在 Client Address Assignment 下，从下拉列表中选择地址池 **vpnpool。**在 Default Group Policy 下，从下拉列表中选择组策略 **clientgroup。**



Add SSL VPN Connection Profile

Name: sslgroup

Aliases:

Authentication

Method: ● AAA ○ Certificate ○ Both

AAA Server Group: LOCAL

□ Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:

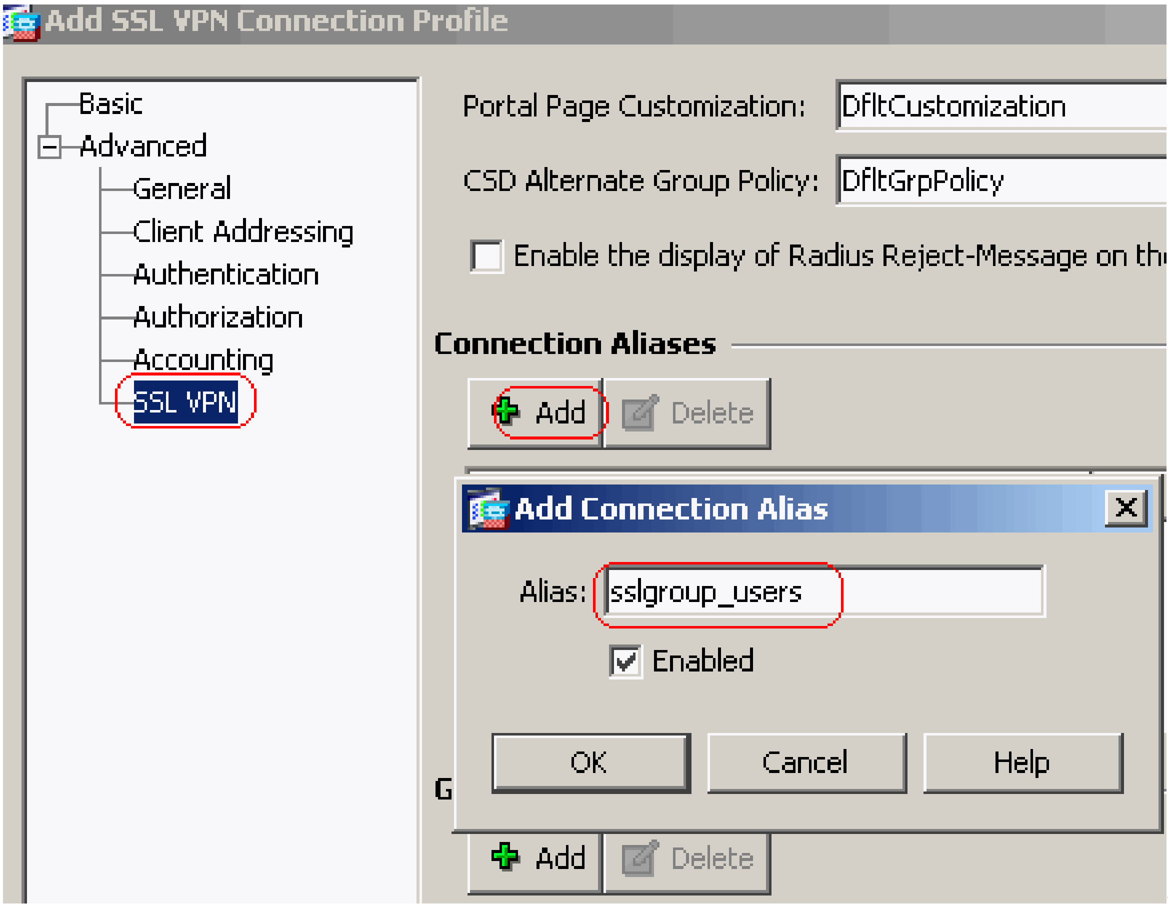
Client Address Pools: vpnpool

Default Group Policy

Group Policy: clientgroup

SSL VPN Client Protocol: ☑ Enabled

在 SSL VPN > Connection Aliases 选项卡下，将组别名指定为 sslgroup_users，然后单击



Portal Page Customization: DfltCustomization

CSD Alternate Group Policy: DfltGrpPolicy

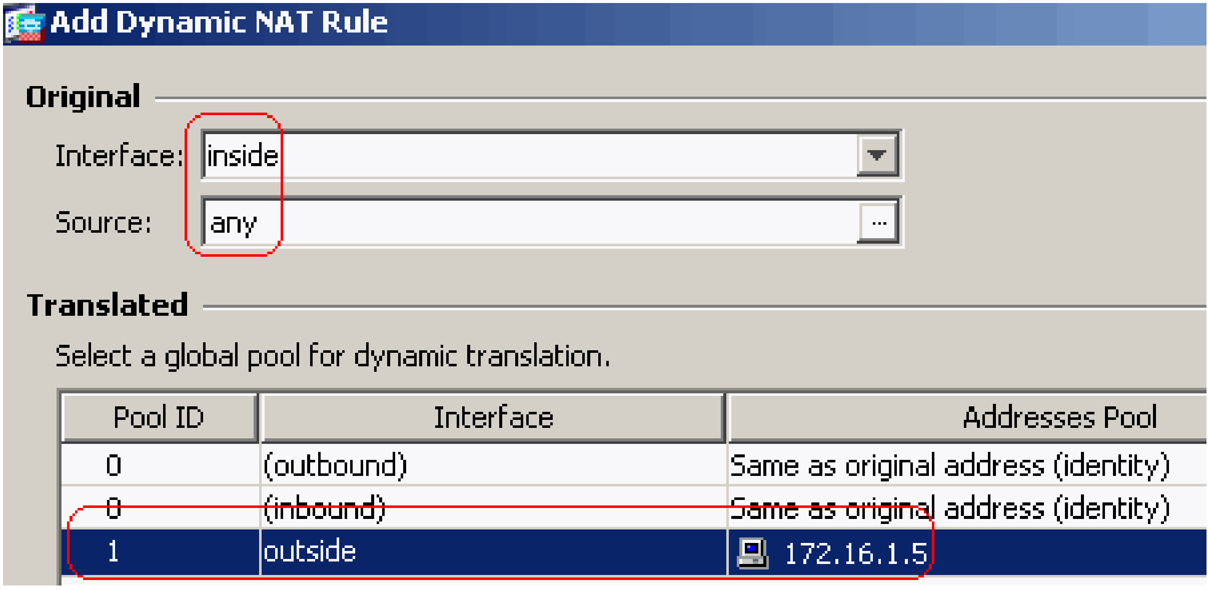
□ Enable the display of Radius Reject-Message on th

Alias: sslgroup_users

☑ Enabled

OK。单击 OK，然后单击 Apply。等效 CLI 配置：

9. 配置 NAT。选择 **Configuration > Firewall > NAT Rules > Add Dynamic NAT Rule，这样来自内部网络的数据流就可以转换为外部 IP 地址 172.16.1.5。**



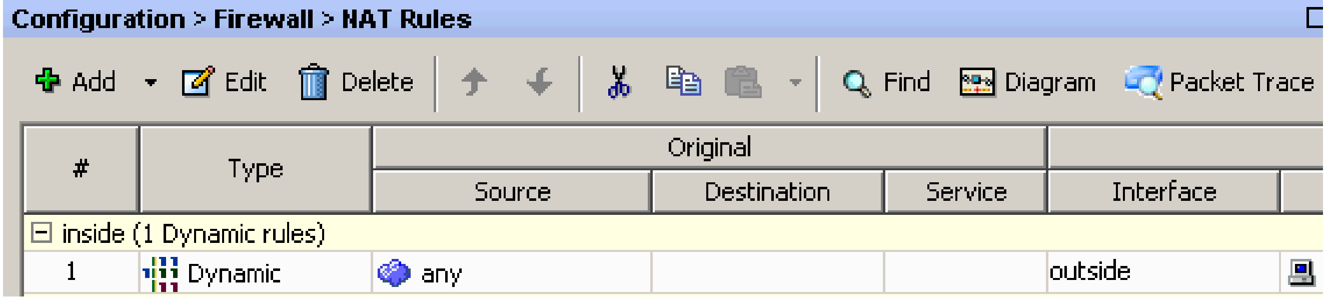
Interface: inside

Source: any

Select a global pool for dynamic translation.

Pool ID	Interface	Addresses Pool
0	(outbound)	Same as original address (identity)
0	(inbound)	Same as original address (identity)
1	outside	172.16.1.5

Click **OK**.Click **OK.**



#	Type	Original			
		Source	Destination	Service	Interface
inside (1 Dynamic rules)					
1	Dynamic	any			outside

单击 Apply。等效 CLI 配置：

10. 为从内部网络到VPN客户端的返回流量配置nat-exemption。

    ```
    ciscoasa(config)#access-list nonat permit ip 10.77.241.0 192.168.10.0
    ciscoasa(config)#access-list nonat permit ip 192.168.10.0 10.77.241.0
    ciscoasa(config)#nat (inside) 0 access-list nonat
    ```

ASA CLI 配置

Cisco ASA 8.0(2)

```
ciscoasa(config)#show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 10.77.241.142 255.255.255.192
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/asa802-k8.bin
ftp mode passive
clock timezone IST 5 30
dns server-group DefaultDNS
 domain-name default.domain.invalid
access-list split-tunnel standard permit 10.77.241.128
255.255.255.192
!--- ACL for Split Tunnel network list for encryption.
access-list nonat permit ip 10.77.241.0 192.168.10.0
access-list nonat permit ip 192.168.10.0 10.77.241.0 !--
- ACL to define the traffic to be exempted from NAT.
pager lines 24 logging enable logging asdm informational
```

```
mtu inside 1500 mtu outside 1500 ip local pool vpnpool
192.168.10.1-192.168.10.254 mask 255.255.255.0

!--- The address pool for the Cisco AnyConnect SSL VPN
Clients no failover icmp unreachable rate-limit 1 burst-
size 1 asdm image disk0:/asdm-602.bin no asdm history
enable arp timeout 14400 global (outside) 1 172.16.1.5

!--- The global address for Internet access used by VPN
Clients. !--- Note: Uses an RFC 1918 range for lab
setup. !--- Apply an address from your public range
provided by your ISP. nat (inside) 0 access-list nonat
!--- The traffic permitted in "nonat" ACL is exempted
from NAT. nat (inside) 1 0.0.0.0 0.0.0.0


route outside 0.0.0.0 0.0.0.0 172.16.1.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
no crypto isakmp nat-traversal
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
```

```
webvpn
 enable outside

!--- Enable WebVPN on the outside interface  svc image
disk0:/anyconnect-win-2.0.0343-k9.pkg 1

!--- Assign an order to the AnyConnect SSL VPN Client
image svc enable

!--- Enable the security appliance to download SVC
images to remote computers tunnel-group-list enable

!--- Enable the display of the tunnel-group list on the
WebVPN Login page group-policy clientgroup internal

!--- Create an internal group policy "clientgroup"
group-policy clientgroup attributes
 vpn-tunnel-protocol svc

!--- Specify SSL as a permitted VPN tunneling protocol
split-tunnel-policy tunnelspecified
 split-tunnel-network-list value split-tunnel

!--- Encrypt the traffic specified in the split tunnel
ACL only webvpn
  svc keep-installer installed

!--- When the security appliance and the SVC perform a
rekey, they renegotiate !--- the crypto keys and
initialization vectors, increasing the security of the
connection. svc rekey time 30

!--- Command that specifies the number of minutes from
the start of the !--- session until the rekey takes
place, from 1 to 10080 (1 week). svc rekey method ssl

!--- Command that specifies that SSL renegotiation takes
place during SVC rekey. svc ask none default svc

username ssluser1 password ZRhW85jZqEaVd5P. encrypted

!--- Create a user account "ssluser1" tunnel-group
sslgroup type remote-access

!--- Create a tunnel group "sslgroup" with type as
remote access tunnel-group sslgroup general-attributes
 address-pool vpnpool

!--- Associate the address pool vpnpool created default-
group-policy clientgroup

!--- Associate the group policy "clientgroup" created
tunnel-group sslgroup webvpn-attributes
 group-alias sslgroup_users enable

!--- Configure the group alias as sslgroup-users prompt
hostname context
Cryptochecksum:af3c4bfc4ffc07414c4dfbd29c5262a9 : end
ciscoasa(config)#
```

使用 SVC 建立 SSL VPN 连接

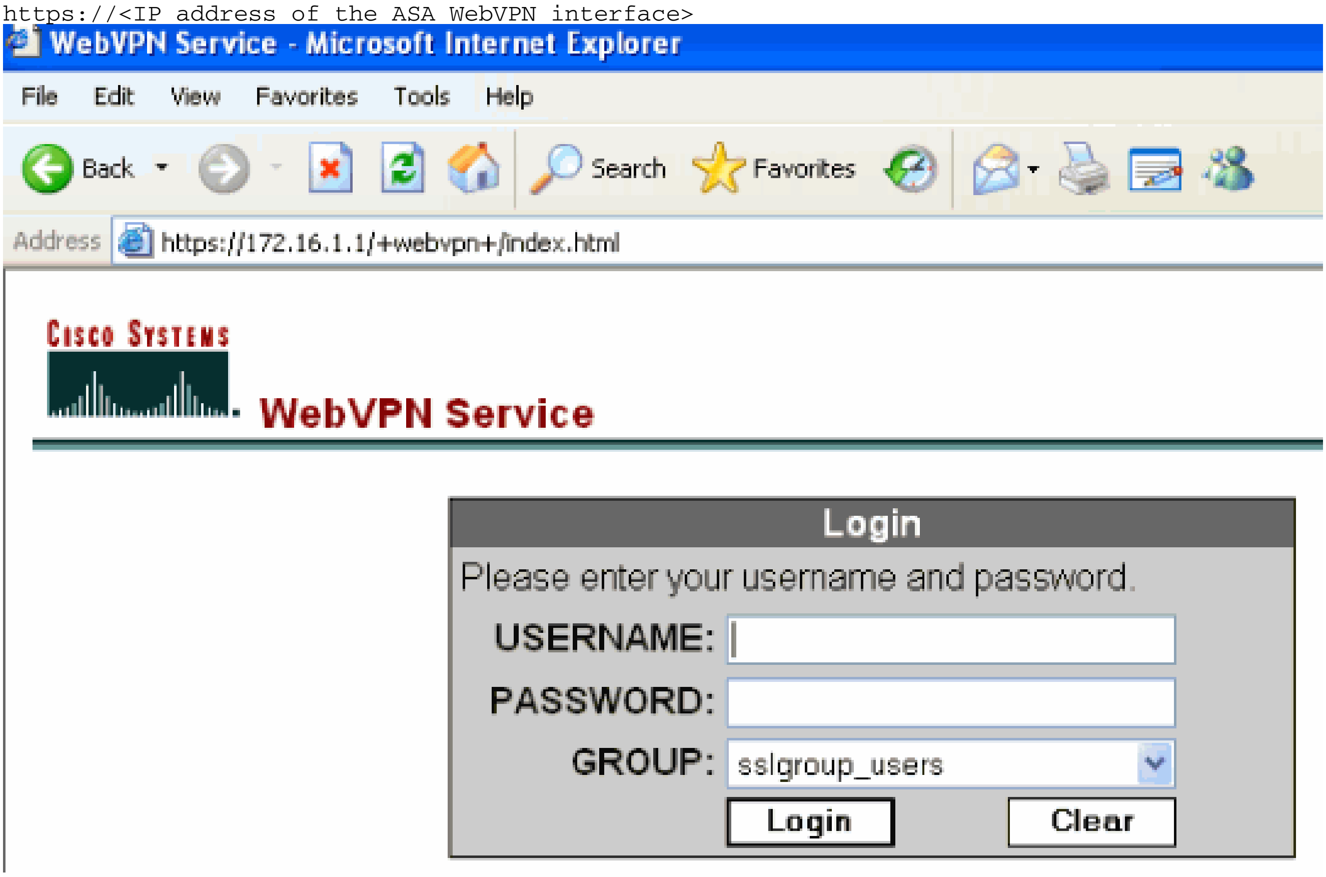
要建立与 ASA 的 SSL VPN 连接，请执行以下步骤：

1. 以如下所示格式在 Web 浏览器中输入 ASA 的 Webvpn 接口的 URL 或 IP 地址。

   ```
   https://url
   ```

   或者

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

   WebVPN Service - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address

   https://172.16.1.1/+webvpn+/index.html

   Cisco Systems
WebVPN Service
Login

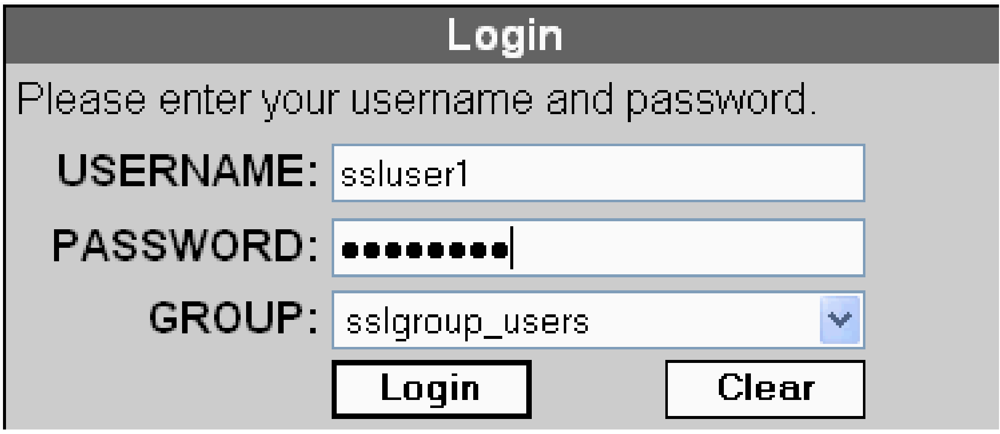
   Please enter your username and password.

   USERNAME:

   PASSWORD:

   GROUP: sslgroup_users

2. 请输入您的用户名和密码。然后，从下拉列表中选择相应的组，如下所示。

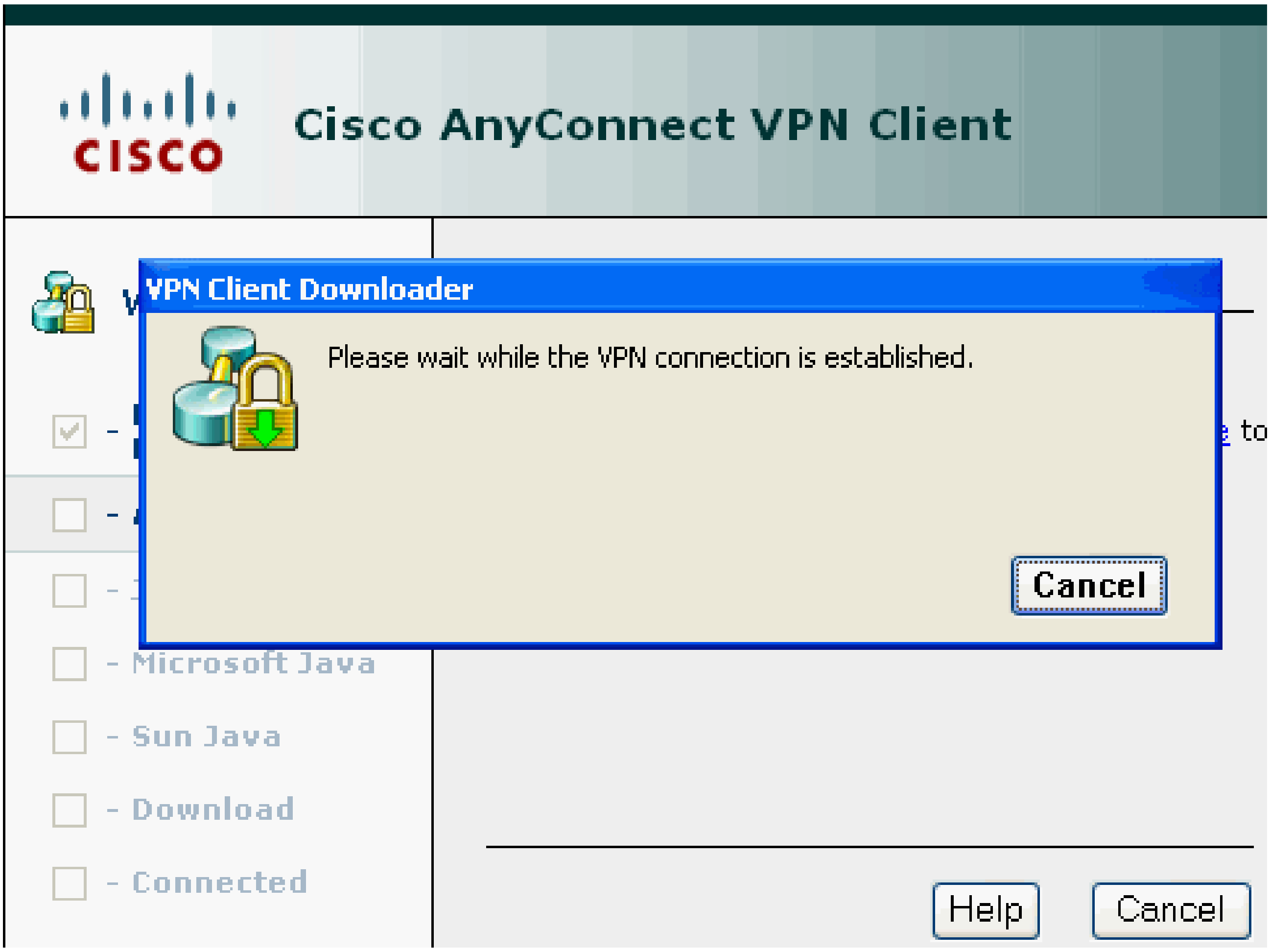
   Please enter your username and password.

   USERNAME: ssluser1

   PASSWORD: ●●●●●●●●●

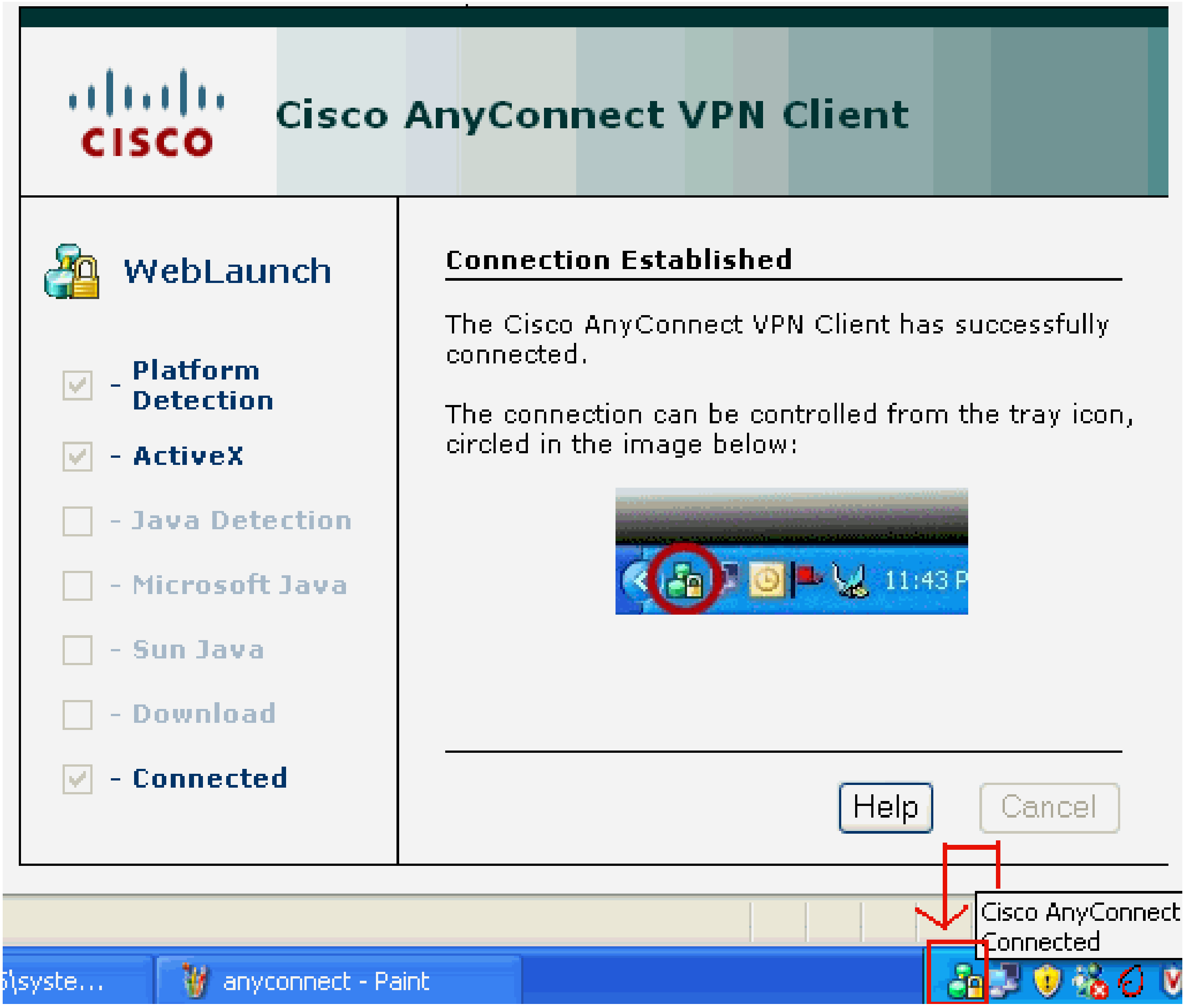
   GROUP: sslgroup_users

   在 SSL VPN 连接建立之前，将会出现以下窗口。



Please wait while the VPN connection is established.

注意：在下载SVC之前，必须在计算机中安装ActiveX软件。在连接建立后，您将看到以下窗口。



Cisco AnyConnect VPN Client

WebLaunch

☑ - Platform Detection

☑ - ActiveX

□ - Java Detection

□ - Microsoft Java

□ - Sun Java

□ - Download

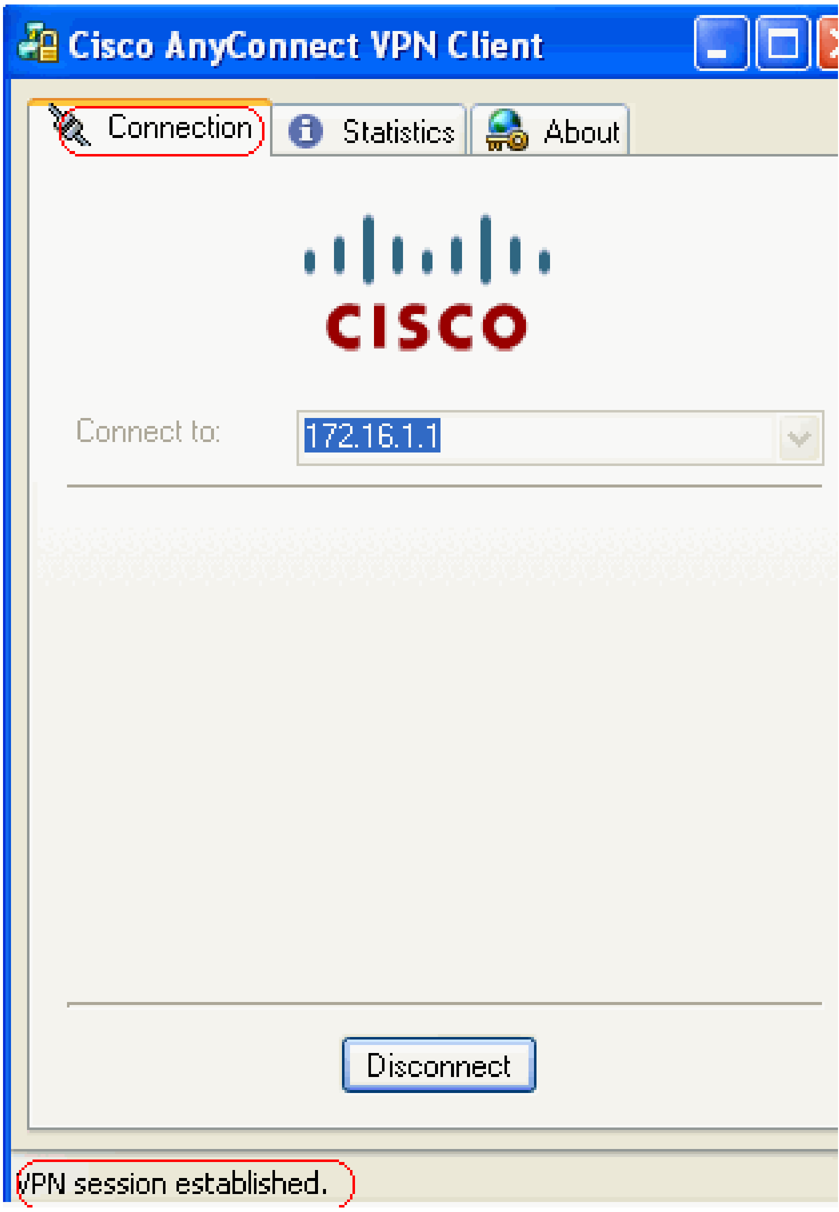
☑ - Connected

Connection Established

The Cisco AnyConnect VPN Client has successfully connected.

The connection can be controlled from the tray icon, circled in the image below:

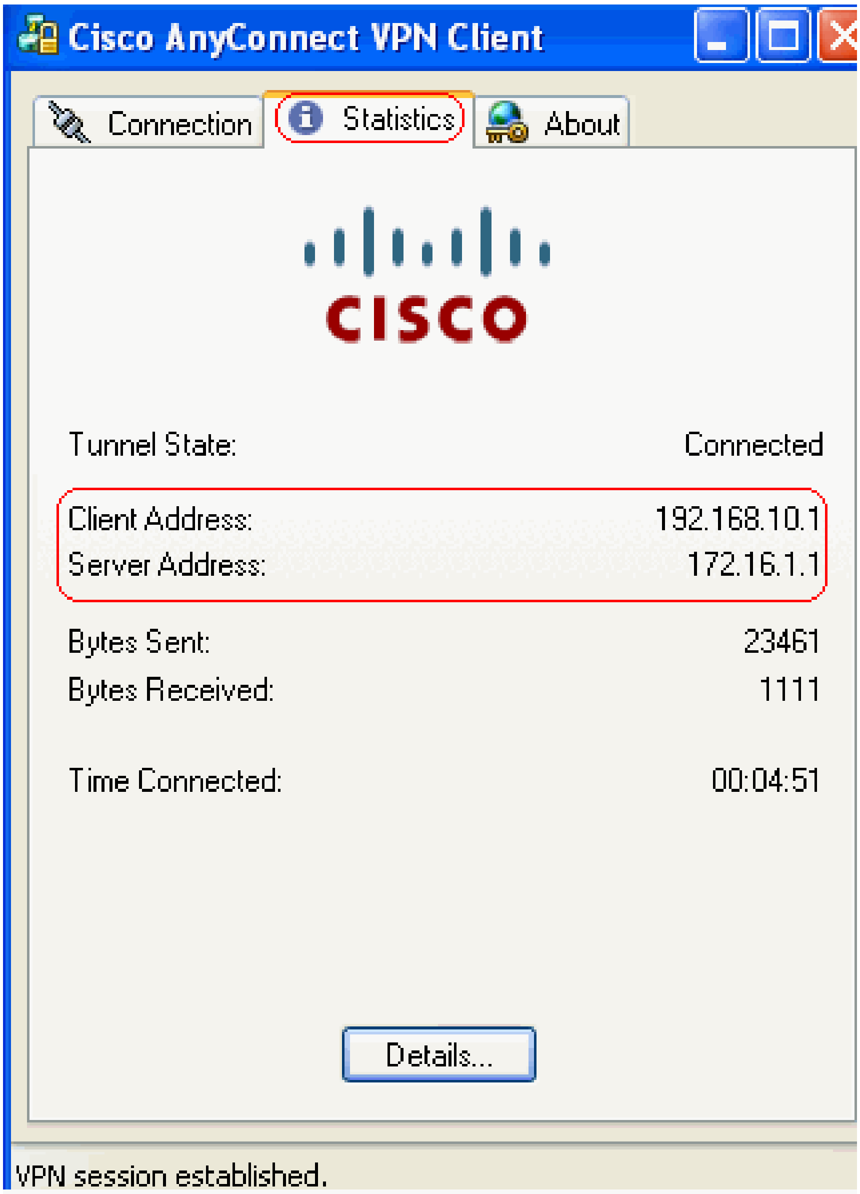
3. 单击出现在计算机任务栏中的锁图标。



Connect to: 172.16.1.1

VPN session established.

将会出现以下窗口，并提供有关 SSL 连接的信息。例如，**192.168.10.1 是 ASA 指定的 IP 等等。**



Tunnel State: Connected

Client Address: 192.168.10.1

Server Address: 172.16.1.1

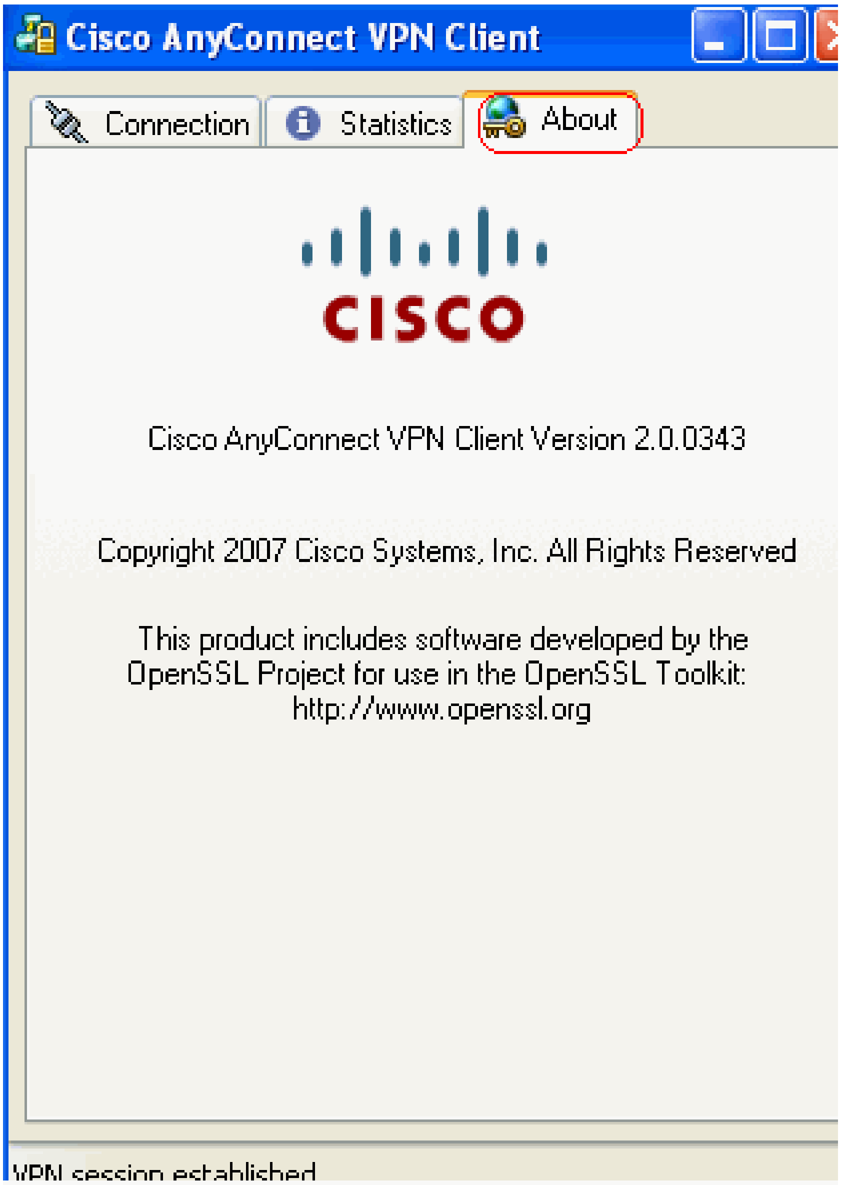
Bytes Sent: 23461

Bytes Received: 1111

Time Connected: 00:04:51

VPN session established.

以下窗口显示了 Cisco AnyConnect VPN Client 的版本信息。



Cisco AnyConnect VPN Client Version 2.0.0343

Copyright 2007 Cisco Systems, Inc. All Rights Reserved

This product includes software developed by the
OpenSSL Project for use in the OpenSSL Toolkit:
http://www.openssl.org

VPN session established

验证

使用本部分可确认配置能否正常运行。

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。

- **show webvpn svc — 显示存储在 ASA 闪存中的 SVC 映像。**

```
ciscoasa#show webvpn svc
1. disk0:/anyconnect-win-2.0.0343-k9.pkg 1
  CISCO STC win2k+
  2,0,0343
  Mon 04/23/2007  4:16:34.63

1 SSL VPN Client(s) installed
```

- **show vpn-sessiondb svc — 显示有关当前 SSL 连接的信息。**

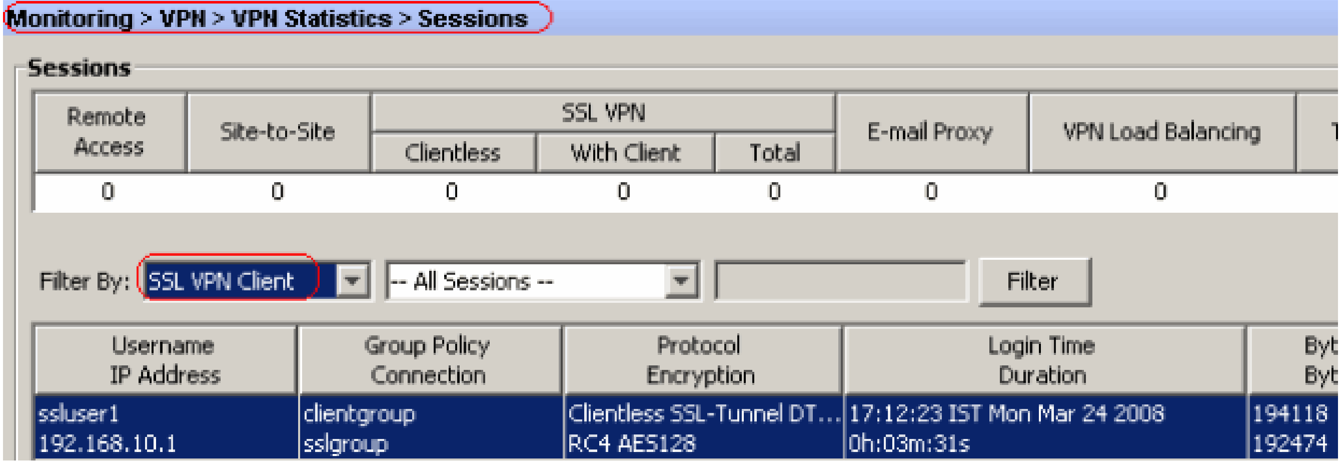
```
ciscoasa#show vpn-sessiondb svc

Session Type: SVC

Username     : ssluser1               Index        : 12
```

```
Assigned IP  : 192.168.10.1           Public IP    : 192.168.1.1
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 194118                 Bytes Rx     : 197448
Group Policy : clientgroup            Tunnel Group : sslgroup
Login Time   : 17:12:23 IST Mon Mar 24 2008
Duration     : 0h:12m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

- show webvpn group-alias — 显示为各组配置的别名。

```
ciscoasa#show webvpn group-alias
Tunnel Group: sslgroup   Group Alias: sslgroup_users enabled
```

- 在 ASDM 中，选择 Monitoring > VPN > VPN Statistics > Sessions 以了解 ASA 的当前 Webvpn 会话。



Monitoring > VPN > VPN Statistics > Sessions

Sessions

Remote Access	Site-to-Site	SSL VPN			E-mail Proxy	VPN Load Balancing	T
		Clientless	With Client	Total			
0	0	0	0	0	0	0	

Filter By: SSL VPN Client　-- All Sessions --　Filter

Username IP Address	Group Policy Connection	Protocol Encryption	Login Time Duration	Byt Byt
ssluser1 192.168.10.1	clientgroup sslgroup	Clientless SSL-Tunnel DT... RC4 AES128	17:12:23 IST Mon Mar 24 2008 0h:03m:31s	194118 192474

故障排除

本部分提供的信息可用于对配置进行故障排除。

1. vpn-sessiondb logoff name <username> — 用于注销特定用户名的 SSL VPN 会话的命令。

```
ciscoasa#vpn-sessiondb logoff name ssluser1
Do you want to logoff the VPN session(s)? [confirm] Y
INFO: Number of sessions with name "ssluser1" logged off : 1

ciscoasa#Called vpn_remove_uauth: success!
webvpn_svc_np_tear_down: no ACL
webvpn_svc_np_tear_down: no IPv6 ACL
np_svc_destroy_session(0xB000)
```

   同样地，您也可以使用 vpn-sessiondb logoff svc 命令终止所有 SVC 会话。

2. **注意**：如果PC进入待机或休眠模式，则SSL VPN连接可以终止。

```
webvpn_rx_data_cstp
webvpn_rx_data_cstp: got message
SVC message: t/s=5/16: Client PC is going into suspend mode (Sleep, Hibernate, e
tc)
Called vpn_remove_uauth: success!
webvpn_svc_np_tear_down: no ACL
webvpn_svc_np_tear_down: no IPv6 ACL
np_svc_destroy_session(0xA000)


ciscoasa#show vpn-sessiondb svc
```

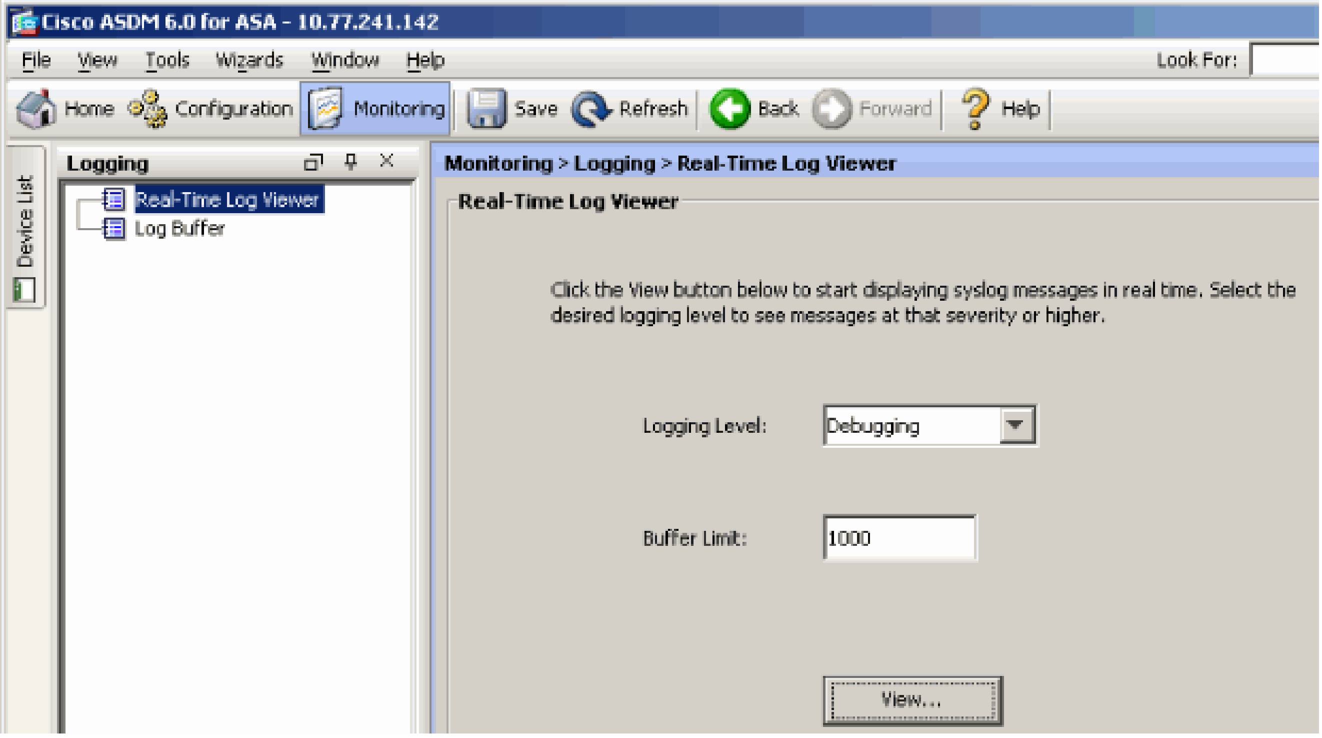
```
INFO: There are presently no active sessions
```

3. **Debug webvpn svc <1-255> — 提供实时 webvpn 事件以建立会话。**

```
Ciscoasa#debug webvpn svc 7

webvpn_rx_data_tunnel_connect
CSTP state = HEADER_PROCESSING
http_parse_cstp_method()
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
webvpn_cstp_parse_request_field()
...input: 'Host: 172.16.1.1'
Processing CSTP header line: 'Host: 172.16.1.1'
webvpn_cstp_parse_request_field()
...input: 'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343'
Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343
'
Setting user-agent to: 'Cisco AnyConnect VPN Client 2, 0, 0343'
webvpn_cstp_parse_request_field()
...input: 'Cookie: webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B
7D75F4EDEF26'
Processing CSTP header line: 'Cookie: webvpn=16885952@12288@1206098825@D251883E8
625B92C1338D631B08B7D75F4EDEF26'
Found WebVPN cookie: 'webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B
08B7D75F4EDEF26'
WebVPN Cookie: 'webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B7D7
5F4EDEF26'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Version: 1'
Processing CSTP header line: 'X-CSTP-Version: 1'
Setting version to '1'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Hostname: tacweb'
Processing CSTP header line: 'X-CSTP-Hostname: tacweb'
Setting hostname to: 'tacweb'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Accept-Encoding: deflate;q=1.0'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: deflate;q=1.0'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-MTU: 1206'
Processing CSTP header line: 'X-CSTP-MTU: 1206'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Address-Type: IPv4'
Processing CSTP header line: 'X-CSTP-Address-Type: IPv4'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Master-Secret: CE151BA2107437EDE5EC4F5EE6AEBAC12031550B1812D40
642E22C6AFCB9501758FF3B7B5545973C06F6393C92E59693'
Processing CSTP header line: 'X-DTLS-Master-Secret: CE151BA2107437EDE5EC4F5EE6AE
BAC12031550B1812D40642E22C6AFCB9501758FF3B7B5545973C06F6393C92E59693'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA'
Processing CSTP header line: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3
-SHA:DES-CBC-SHA'
Validating address: 0.0.0.0
CSTP state = WAIT_FOR_ADDRESS
webvpn_cstp_accept_address: 192.168.10.1/0.0.0.0
CSTP state = HAVE_ADDRESS
No subnetmask... must calculate it
SVC: NP setup
np_svc_create_session(0x3000, 0xD41611E8, TRUE)
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
SVC ACL ID: -1
vpn_put_uauth success!
```

```
SVC IPv6 ACL Name: NULL
SVC IPv6 ACL ID: -1
SVC: adding to sessmgmt
SVC: Sending response
Unable to initiate NAC, NAC might not be enabled or invalid policy
CSTP state = CONNECTED
webvpn_rx_data_cstp
webvpn_rx_data_cstp: got internal message
Unable to initiate NAC, NAC might not be enabled or invalid policy
```

4. 在 ASDM 中，选择 **Monitoring > Logging > Real-time Log Viewer > View 以查看实时事件。**



Monitoring > Logging > Real-Time Log Viewer

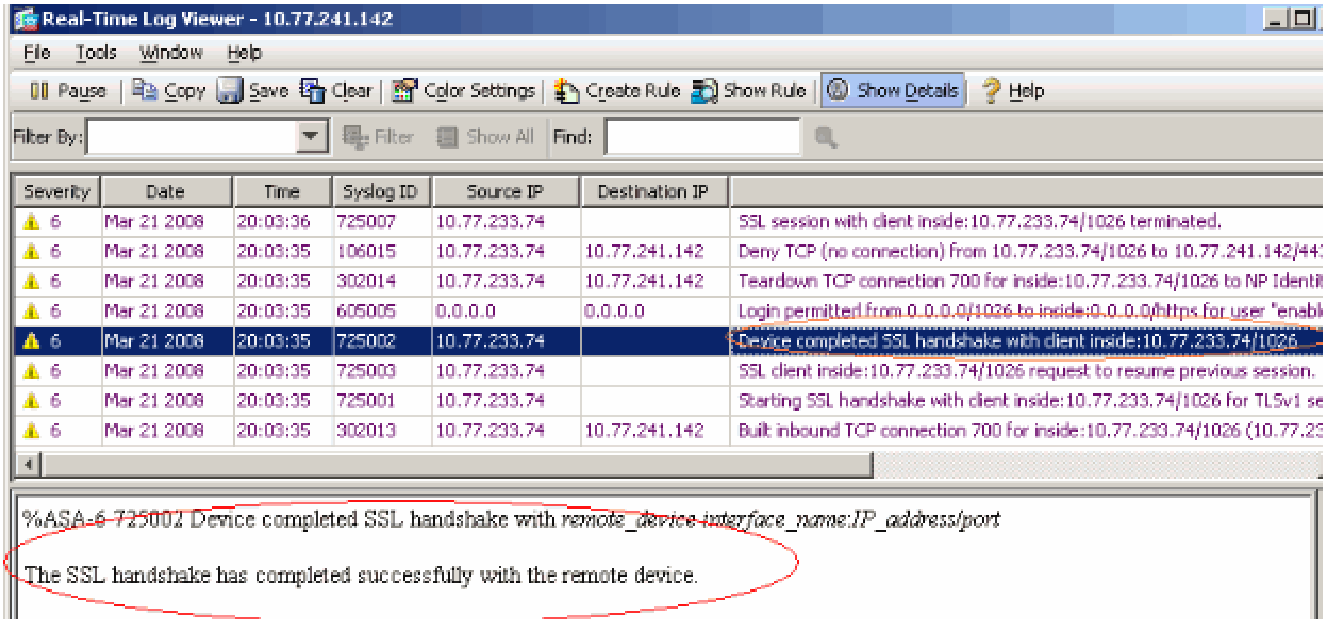
Real-Time Log Viewer

Click the View button below to start displaying syslog messages in real time. Select the desired logging level to see messages at that severity or higher.

Logging Level: Debugging

Buffer Limit: 1000

本示例显示已与前端设备建立了 SSL 会话。



Severity	Date	Time	Syslog ID	Source IP	Destination IP	
⚠ 6	Mar 21 2008	20:03:36	725007	10.77.233.74		SSL session with client inside:10.77.233.74/1026 terminated.
⚠ 6	Mar 21 2008	20:03:35	106015	10.77.233.74	10.77.241.142	Deny TCP (no connection) from 10.77.233.74/1026 to 10.77.241.142/44
⚠ 6	Mar 21 2008	20:03:35	302014	10.77.233.74	10.77.241.142	Teardown TCP connection 700 for inside:10.77.233.74/1026 to NP Identi
⚠ 6	Mar 21 2008	20:03:35	605005	0.0.0.0	0.0.0.0	Login permitted from 0.0.0.0/1026 to inside:0.0.0.0/https for user "enabl
⚠ 6	Mar 21 2008	20:03:35	725002	10.77.233.74		Device completed SSL handshake with client inside:10.77.233.74/1026
⚠ 6	Mar 21 2008	20:03:35	725003	10.77.233.74		SSL client inside:10.77.233.74/1026 request to resume previous session.
⚠ 6	Mar 21 2008	20:03:35	725001	10.77.233.74		Starting SSL handshake with client inside:10.77.233.74/1026 for TLSv1 se
⚠ 6	Mar 21 2008	20:03:35	302013	10.77.233.74	10.77.241.142	Built inbound TCP connection 700 for inside:10.77.233.74/1026 (10.77.23

%ASA-6-725002 Device completed SSL handshake with *remote_device interface_name:IP_address/port*

The SSL handshake has completed successfully with the remote device.

相关信息

- Cisco 5500 系列自适应安全设备支持页
- AnyConnect VPN 客户端版本 2.0 的发行版本注释
- ASA/PIX：在 ASA 上允许 VPN Client 使用分割隧道的配置示例

- 路由器允许 VPN Client 使用分割隧道连接 IPsec 和 Internet 的配置示例
- PIX/ASA 7.x 以及用于公共 Internet VPN 的单接口 VPN Client 的配置示例
- 在 ASA 上用 ASDM 配置 SSL VPN Client (SVC) 的示例
- 技术支持和文档 - Cisco Systems