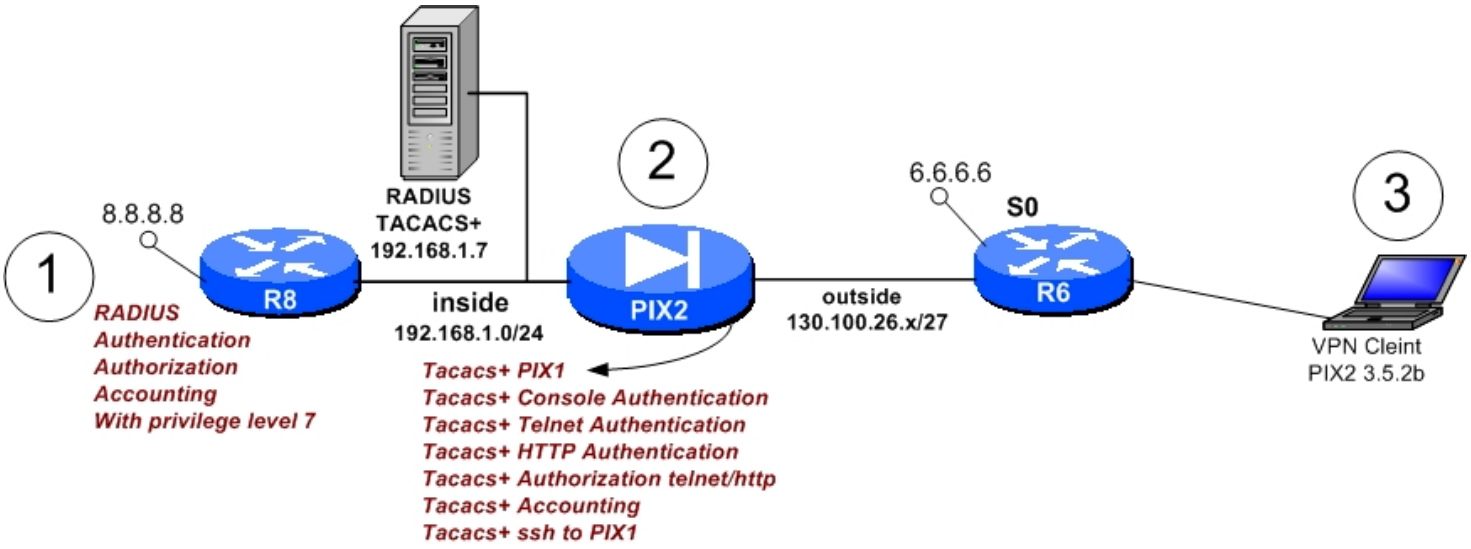
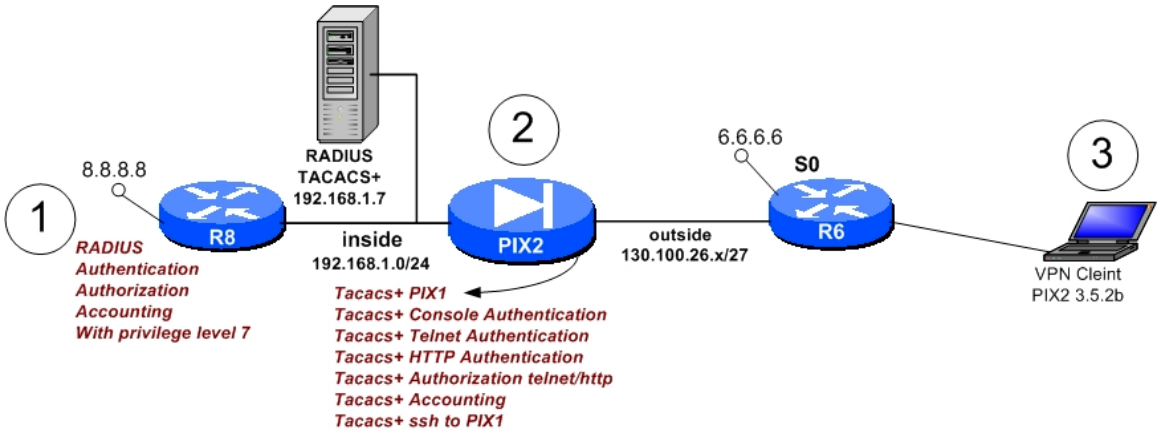


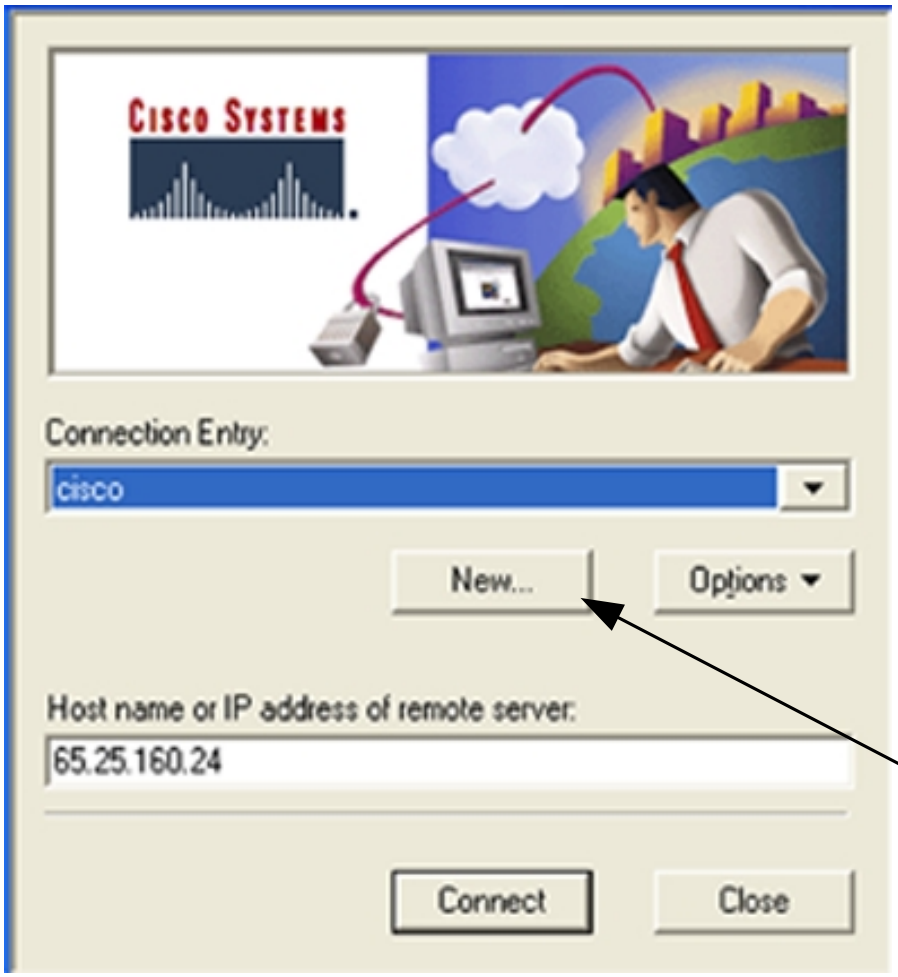
Figure 1 Section 4 AAA Configuring Easy VPN Server with Split tunnel on PIX

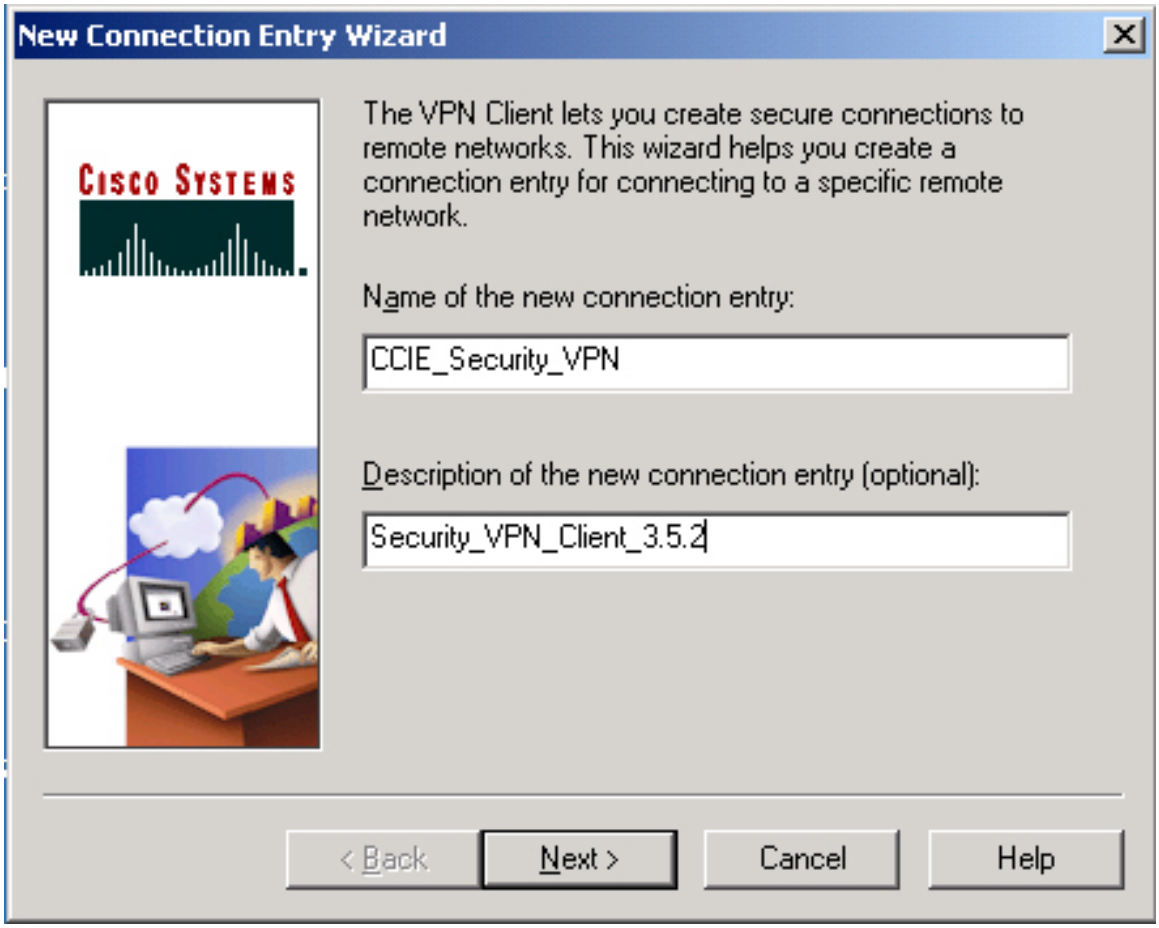
```
PIX Version 6.2(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 DMZ2 security10
nameif ethernet3 DMZ security15

enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIX2
domain-name cisco.com
names
name 130.100.26.6 R6

access-list outside_access_in permit icmp any 130.100.26.0
255.255.255.240
access-list outside_access_in permit tcp any host
130.100.26.7 eq tacacs
access-list outside_access_in permit udp any host
130.100.26.8 eq ntp
access-list outside_access_in permit udp any host
130.100.26.7 eq radius
access-list outside_access_in permit udp any host
130.100.26.7 eq radius-acct


access-list inside_authentication_TACACS+ permit tcp any any
eq telnet
access-list inside_authentication_TACACS+ permit tcp any any
eq www
access-list inside_authorization_TACACS+ permit tcp any any
eq telnet
access-list inside_authorization_TACACS+ permit tcp any any
eq www
access-list inside_accounting_TACACS+ permit tcp any any eq
telnet
access-list inside_accounting_TACACS+ permit tcp any any eq
www
```

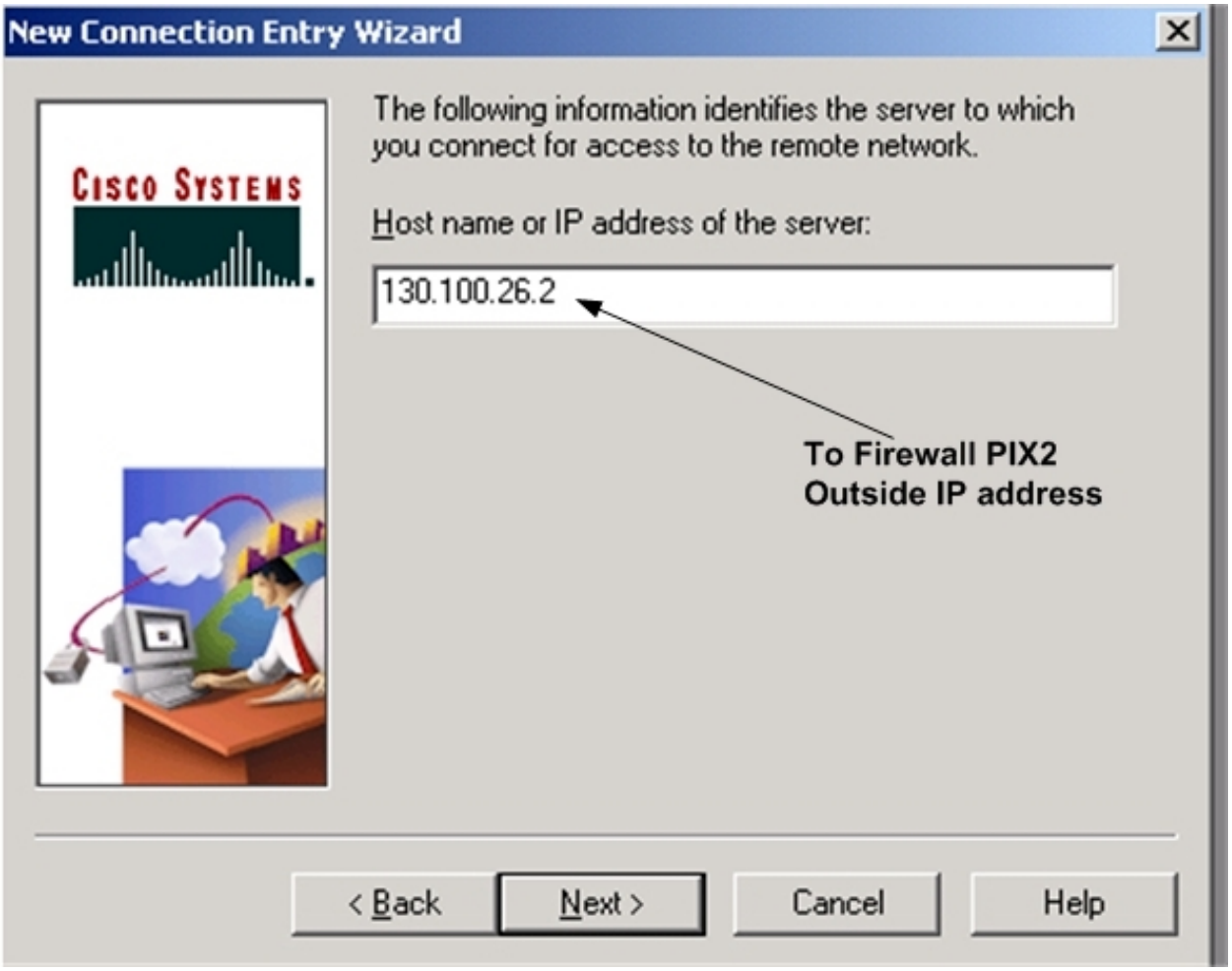
```
access-list 101 permit ip 192.168.1.0 255.255.255.0
192.168.3.0 255.255.255.0
access-group outside_access_in in interface outside

interface ethernet0 10full
interface ethernet1 auto
interface ethernet2 auto
interface ethernet3 10baset

ip address outside 130.100.26.2 255.255.255.224
ip address inside 192.168.1.222 255.255.255.0

ip local pool ippool 192.168.3.1-192.168.3.254

global (outside) 10 interface

nat (inside) 0 access-list 101
nat (inside) 10 0.0.0.0 0.0.0.0 0 0

static (inside,outside) 130.100.26.7 192.168.1.7 netmask
255.255.255.255 0 0
static (inside,outside) 130.100.26.8 192.168.1.1 netmask
255.255.255.255 0 0

route outside 0.0.0.0 0.0.0.0 R6 1
route inside 8.8.8.0 255.255.255.0 192.168.1.1 1

aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ (inside) host 192.168.1.7 cisco6727
timeout 5
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local

aaa authentication match inside_authentication_TACACS+
inside TACACS+
aaa authentication telnet console TACACS+
aaa authentication ssh console TACACS+
aaa authorization match inside_authorization_TACACS+ inside
TACACS+
aaa accounting match inside_accounting_TACACS+ inside
TACACS+

sysopt connection permit-ipsecno sysopt route dnat

auth-prompt prompt Authentication Login please
auth-prompt accept Welcome to CCIE Lab
auth-prompt reject You enter wrong login: Check ACS Server

crypto ipsec transform-set ccie esp-des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set ccie
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap interface outside



isakmp enable outside
isakmp identity address
```

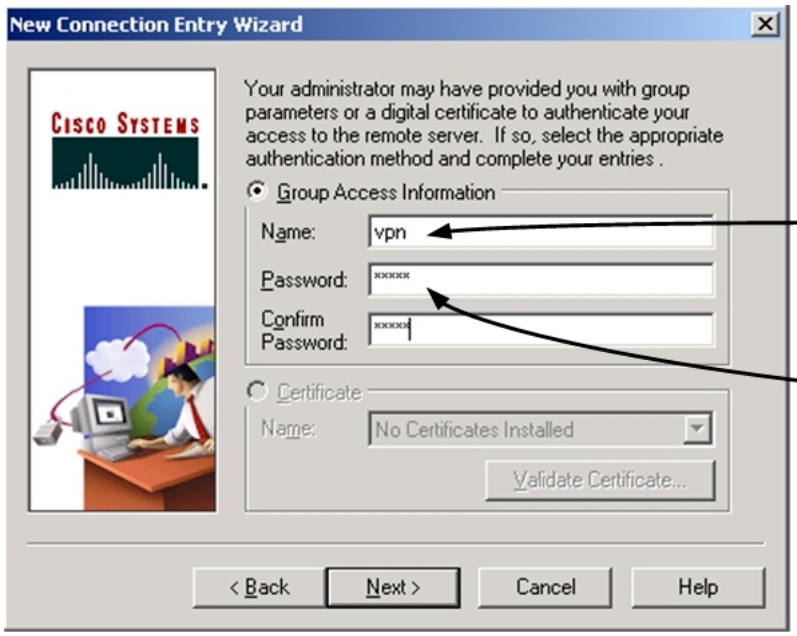
```
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
isakmp policy 20 authentication pre-share
isakmp policy 20 encryption des
isakmp policy 20 hash md5
isakmp policy 20 group 1
isakmp policy 20 lifetime 86400


vpngroup vpn address-pool ippool
vpngroup vpn dns-server 156.46.10.10
vpngroup vpn wins-server 10.1.1.1
vpngroup vpn default-domain cisco.com
vpngroup vpn split-tunnel 101
vpngroup vpn pfs
vpngroup vpn idle-time 1800
vpngroup vpn password cisco



telnet 192.168.1.100 255.255.255.0 inside
ssh 192.168.1.100 255.255.255.255 inside
ssh 192.168.1.1 255.255.255.255 inside
username admin password f3UhLvUj1QsXsuK7 encrypted privilege
15
username user2tacacs password mbO2jYs13AXlIAGa encrypted
privilege 2
```




Cisco Systems
Connection Entry:
cisco
New...
Options
Host name or IP address of remote server:
65.25.160.24
Connect
Close


New Connection Entry Wizard
Cisco Systems
The VPN Client lets you create secure connections to remote networks. This wizard helps you create a connection entry for connecting to a specific remote network.
Name of the new connection entry:
CCIE_Security_VPN
Description of the new connection entry (optional):
Security_VPN_Client_3.5.2
< Back
Next >
Cancel
Help

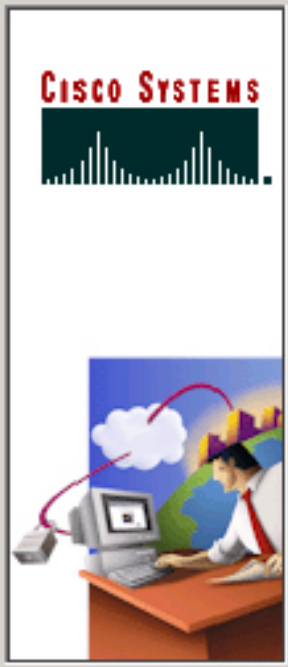




PIX2 vpngroup configuration

```
vpngroup vpn address-pool ippool
vpngroup vpn dns-server 156.46.10.10
vpngroup vpn wins-server 10.1.1.1
vpngroup vpn default-domain cisco.com
vpngroup vpn split-tunnel 101
vpngroup vpn pfs
vpngroup vpn idle-time 1800
vpngroup vpn password ********
```

New Connection Entry Wizard



You have successfully created a new virtual private networking connection entry named:

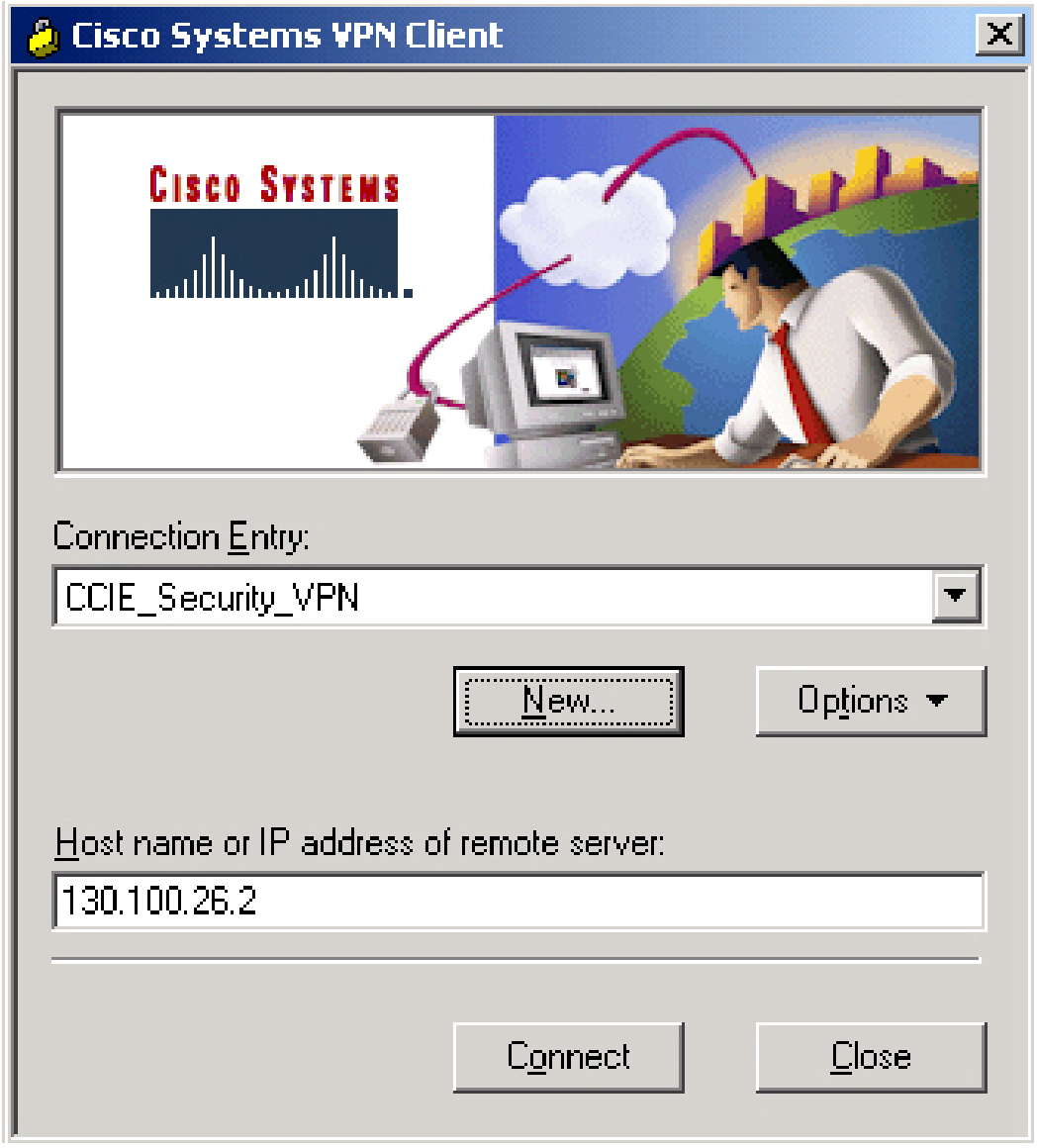
CCIE_Security_VPN

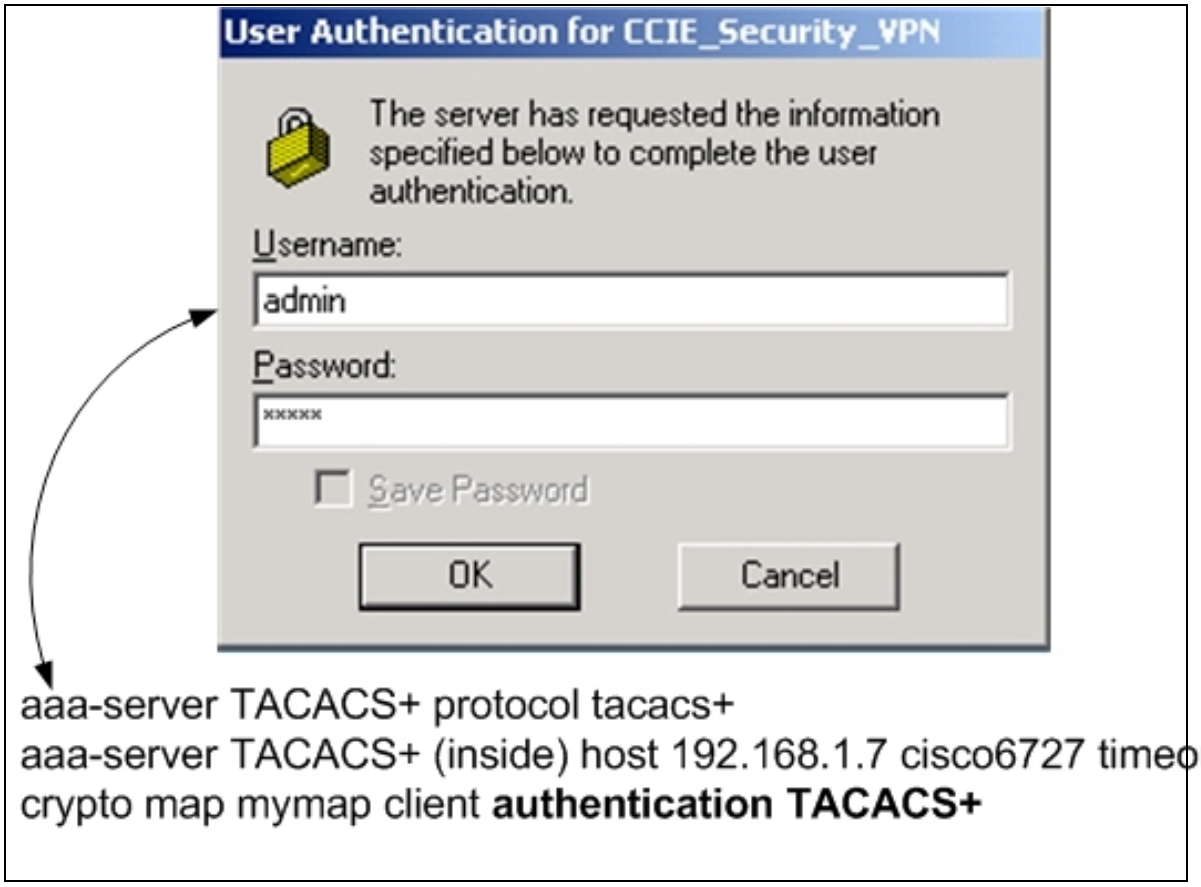
Click Finish to save this entry.

To connect to the remote network, select the Connect button from the main window.

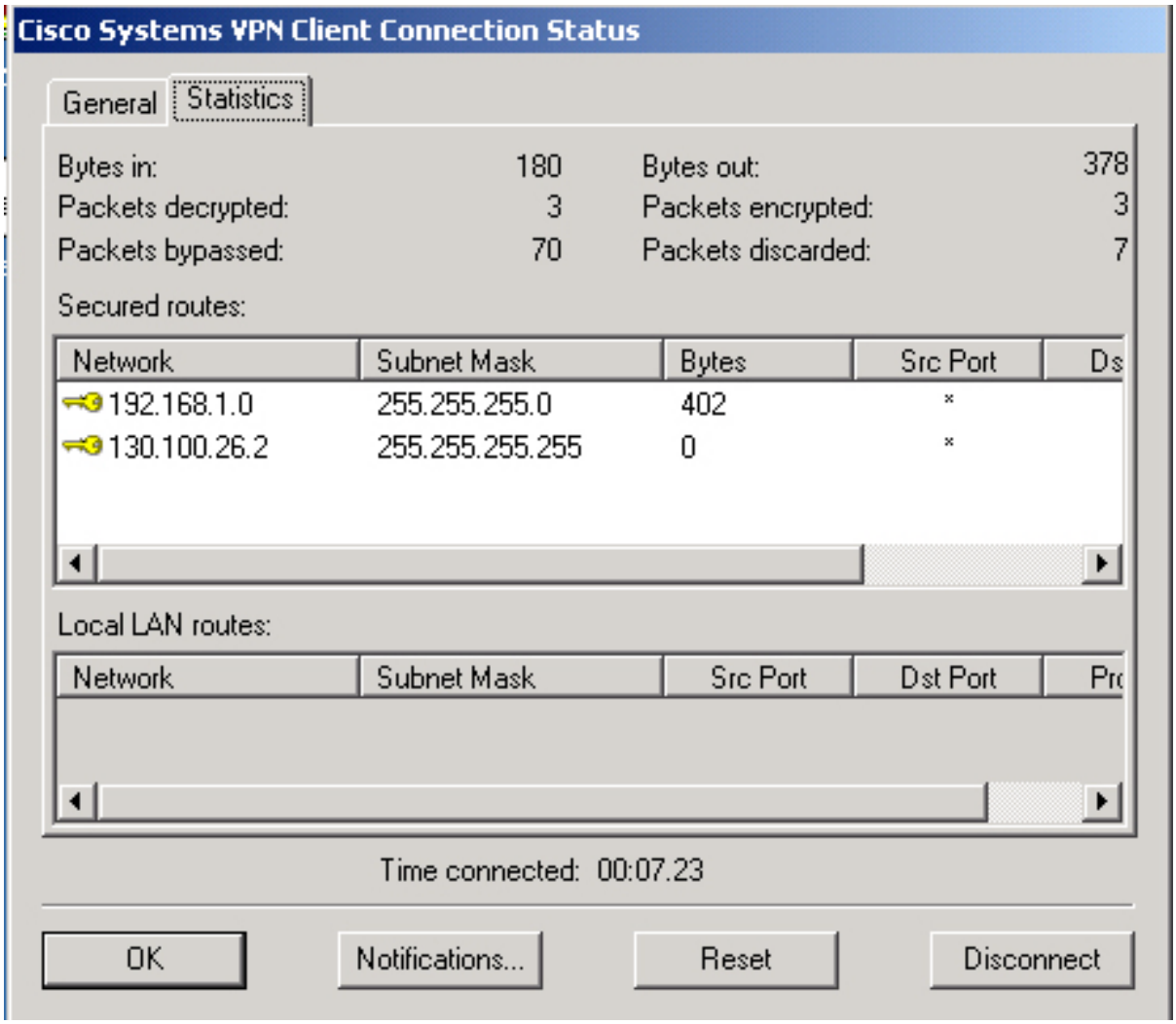
To modify this connection entry, click Options on the main window and select Properties from the menu that appears.

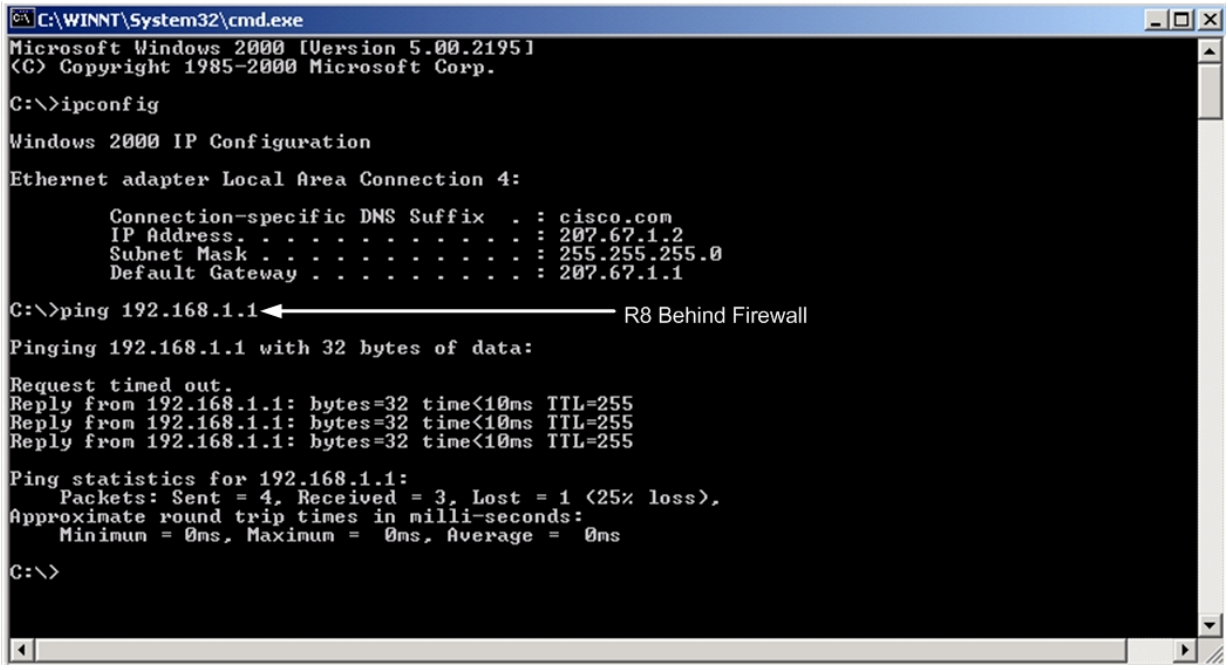
< Back | Finish | Cancel | Help


Cisco Systems VPN Client
Cisco Systems
Connection Entry:
CCIE_Security_VPN
New...
Options
Host name or IP address of remote server:
130.100.26.2
Connect
Close


User Authentication for CCIE_Security_VPN
The server has requested the information specified below to complete the user authentication.
Username:
admin
Password:
*****
Save Password
OK
Cancel
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ (inside) host 192.168.1.7 cisco6727 timeout 5
crypto map mymap client **authentication TACACS+**


Connecting to 130.100.26.2
Authenticating user...
Connection History
Initializing the connection...
Contacting the gateway at 130.100.26.2...
Authenticating user...
Cancel


Cisco Systems VPN Client Connection Status
General
Statistics
Bytes in: 180
Bytes out: 378
Packets decrypted: 3
Packets encrypted: 3
Packets bypassed: 70
Packets discarded: 7
Secured routes:
Network
Subnet Mask
Bytes
Src Port
Ds
192.168.1.0
255.255.255.0
402
*
130.100.26.2
255.255.255.255
0
*
Local LAN routes:
Network
Subnet Mask
Src Port
Dst Port
Pr
Time connected: 00:07.23
OK
Notifications...
Reset
Disconnect


C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.
C:\>ipconfig
Windows 2000 IP Configuration
Ethernet adapter Local Area Connection 4:
Connection-specific DNS Suffix . : cisco.com
IP Address. . . . . : 207.67.1.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 207.67.1.1
C:\>ping 192.168.1.1
R8 Behind Firewall
Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Reply from 192.168.1.1: bytes=32 time<10ms TTL=255
Reply from 192.168.1.1: bytes=32 time<10ms TTL=255
Reply from 192.168.1.1: bytes=32 time<10ms TTL=255
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>