

Application Note

# L2TP Configuration without IPSec

---

Version 1.0

January 2008



Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, CA 94089 USA  
408 745 2000 or 888 JUNIPER  
[www.juniper.net](http://www.juniper.net)

## Contents

Contents.....	2
Introduction .....	3
Included Platforms and ScreenOS .....	3
Overview .....	3
Network Diagram .....	4
Configuration Overview .....	4
Configuration Steps .....	5
Step 1 : Define L2TP user .....	5
Step 2: Define IP pool.....	6
Step 3: Configure default L2TP setting .....	7
Step 4: Create L2TP tunnel.....	8
Step 5: Define address object for internal resource.....	9
Step 6: Create policy .....	10
Step 7: Configure Windows 2000 native L2TP connection.....	11
Verifying Configuration.....	21
Sample Configuration.....	23

## Introduction

The purpose of this application note is to assist a customer in setting up a remote VPN tunnel using L2TP from a client PC running Microsoft Windows 2000 to Juniper firewall.

## Included Platforms and ScreenOS

This application note demonstrates firewall setup on ScreenOS 5.4r8. However, it also applies to following ScreenOS version:

- ScreenOS 5.0
- ScreenOS 5.1
- ScreenOS 5.2
- ScreenOS 5.3
- ScreenOS 5.4
- ScreenOS 6.0

The product list includes the following:

- NS5000
- ISG1000/2000
- NS500/200/50/25
- SSG550m/550/520m/520/320/350/140
- NS5GT
- SSG5/20

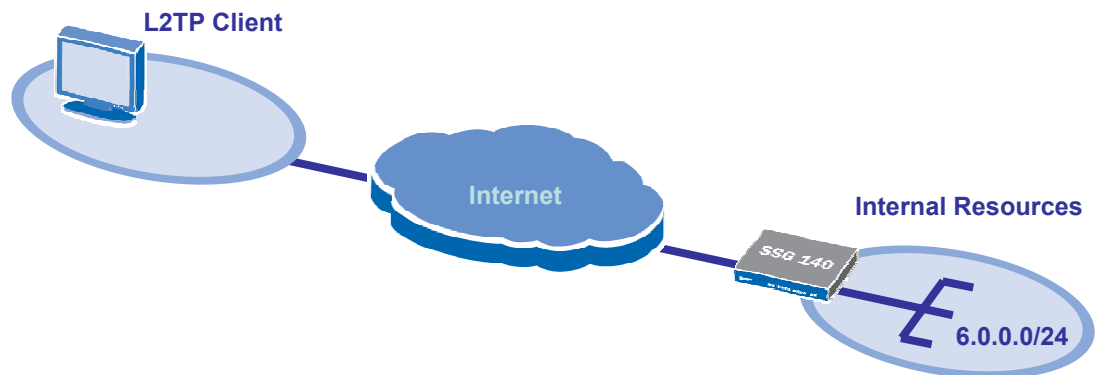
## Overview

To configure a VPN connection using L2TP to a Juniper firewall, a native Microsoft L2TP VPN connection can be used. This application note will provide step-by-step procedures to configure a L2TP VPN connection between Microsoft Windows 2000 and a Juniper firewall.

## Network Diagram

Refer to Figure 1 below for Network Topology used for this configuration example.

Figure 1.



## Configuration Overview

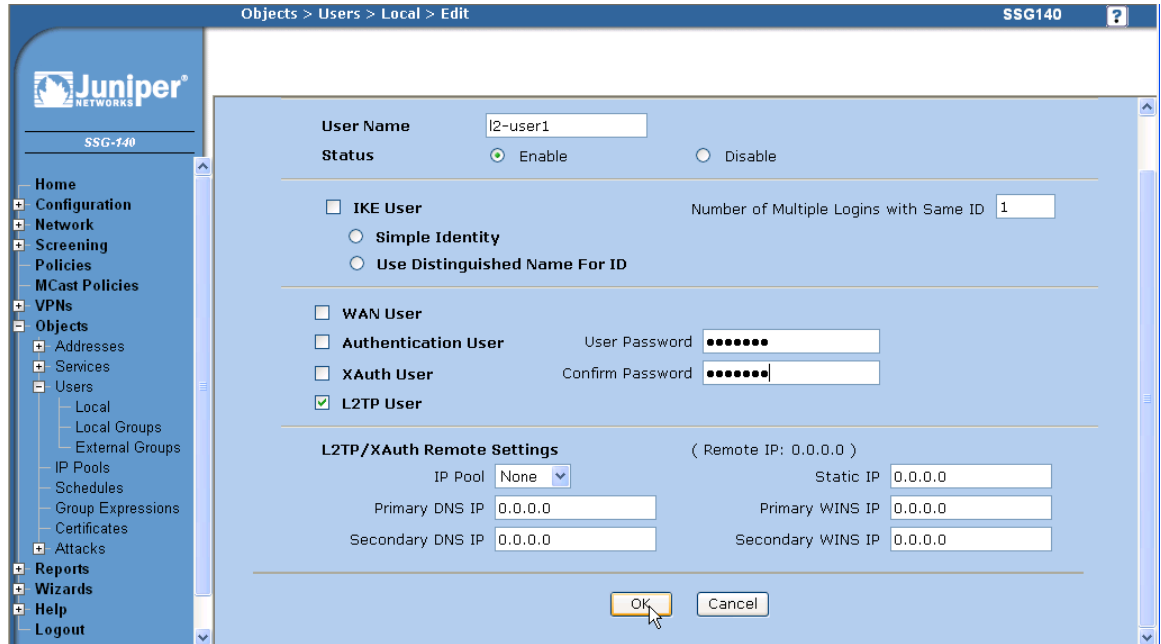
To setup a L2TP tunnel, the customer needs to:

1. Define a L2TP user login and password
2. Define an IP pool for address assignment
3. Configure L2TP default settings
4. Create L2TP tunnel
5. Define an address object for internal resources
6. Create a policy to enable L2TP traffic
7. Configure native L2TP connection on Windows 2000

## Configuration Steps

### Step 1 : Define L2TP user

To define a L2TP user, you need to configure a L2TP user name and password. In this example, we will define the L2TP user “l2-user1” with password “test123”.



The screenshot shows the Juniper SSG-140 WebUI configuration page for a Local user. The page title is "Objects > Users > Local > Edit". The user name is "l2-user1" and the status is "Enable". Under "User Type", "L2TP User" is selected. The "L2TP/XAuth Remote Settings" section shows IP Pool set to "None" and various IP addresses set to "0.0.0.0". The "OK" button is highlighted.

#### WebUI:

Select Objects > Users > Local, then click New.

Enter following, then click OK.

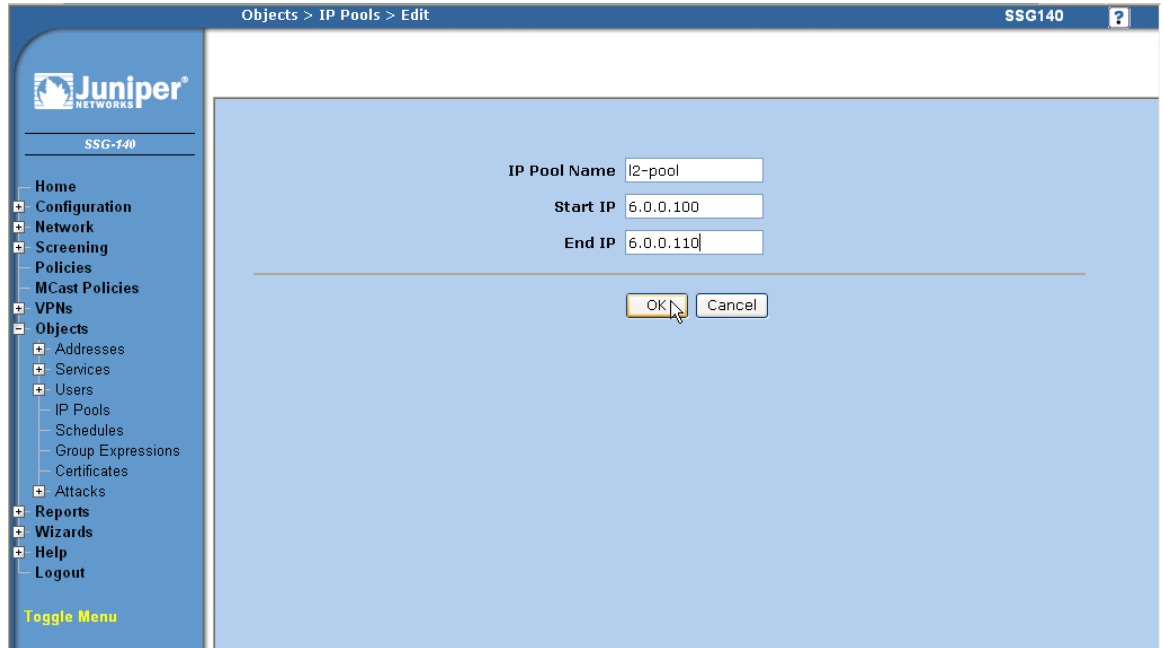
User Name: l2-user1  
 Status: Enable (selected)  
 L2TP User: (selected)  
 User Password: test123 (enter the password)  
 Confirm Password: test123 (enter the password)

#### CLI:

```
set user l2-user1 type l2tp
set user l2-user1 password test123
```

## Step 2: Define IP pool

An IP pool is used to assign a IP address to the L2TP client. Here, we will define a IP pool that will assign IP addresses in the range of 6.0.0.100 to 6.0.0.110 to the L2TP client.



### WebUI:

Select Object > IP Pools , then click New.

Enter following and click OK.

IP Pool Name: L2-pool

Start IP: 6.0.0.100

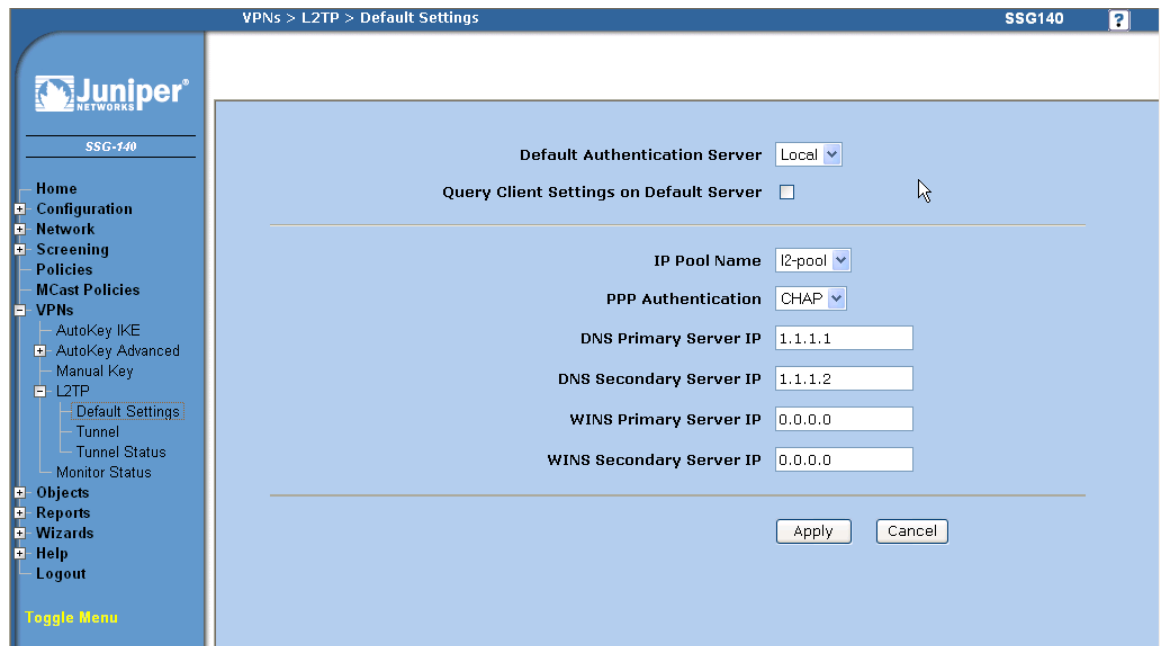
End IP: 6.0.0.110

### CLI:

```
set ippool l2-pool 6.0.0.100 6.0.0.110
```

### Step 3: Configure default L2TP settings

The default L2TP setting including IP pool assignment, PPP Authentication protocol, DNS server setting and WINS server setting can be configured on this L2TP default setting page.



#### WebUI:

Select VPNs > L2TP > Default Settings, then enter following. Click Apply when finished.

IP Pool Name: l2-pool

PPP Authentication: CHAP

DNS Primary Server IP: 1.1.1.1

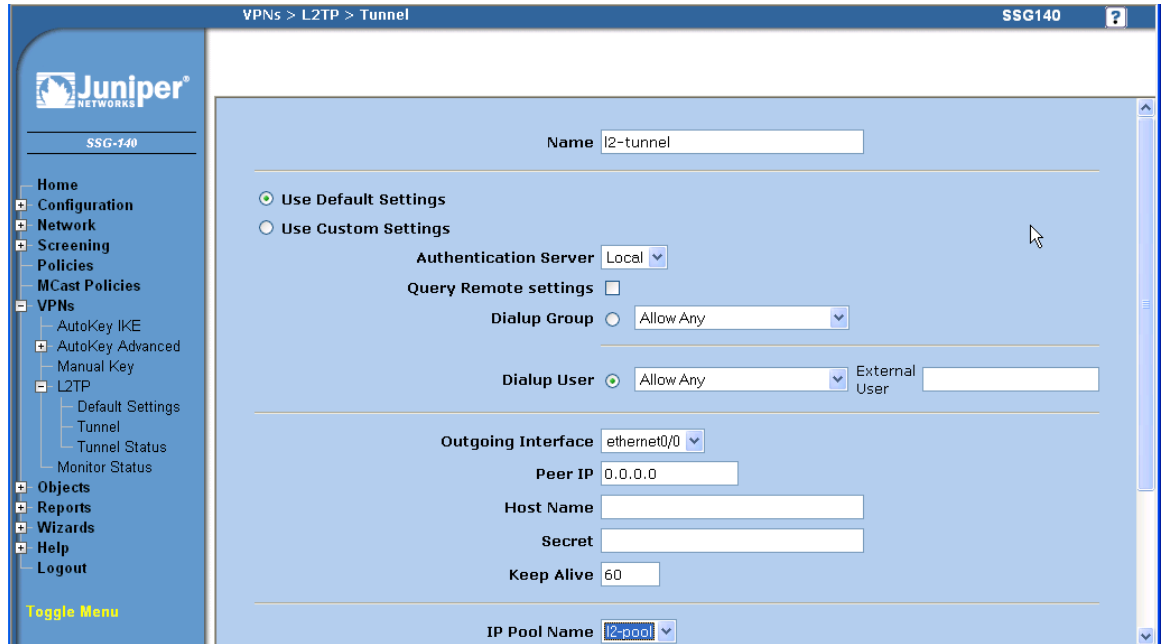
DNS Secondary Server IP: 1.1.1.2

#### CLI:

```
set l2tp default dns1 1.1.1.1
set l2tp default dns2 1.1.1.2
set l2tp default ippool "l2-pool"
set l2tp default ppp-auth chap
```

## Step 4: Create L2TP tunnel

Create the L2TP tunnel by specifying the outgoing interface and IP pool.



### WebUI:

Select VPNs > L2TP > Tunnel, then click New.

Enter following and click OK.

Name: l2-tunnel  
 Outgoing Interface: ethernet0/0  
 IP Pool Name: l2-pool

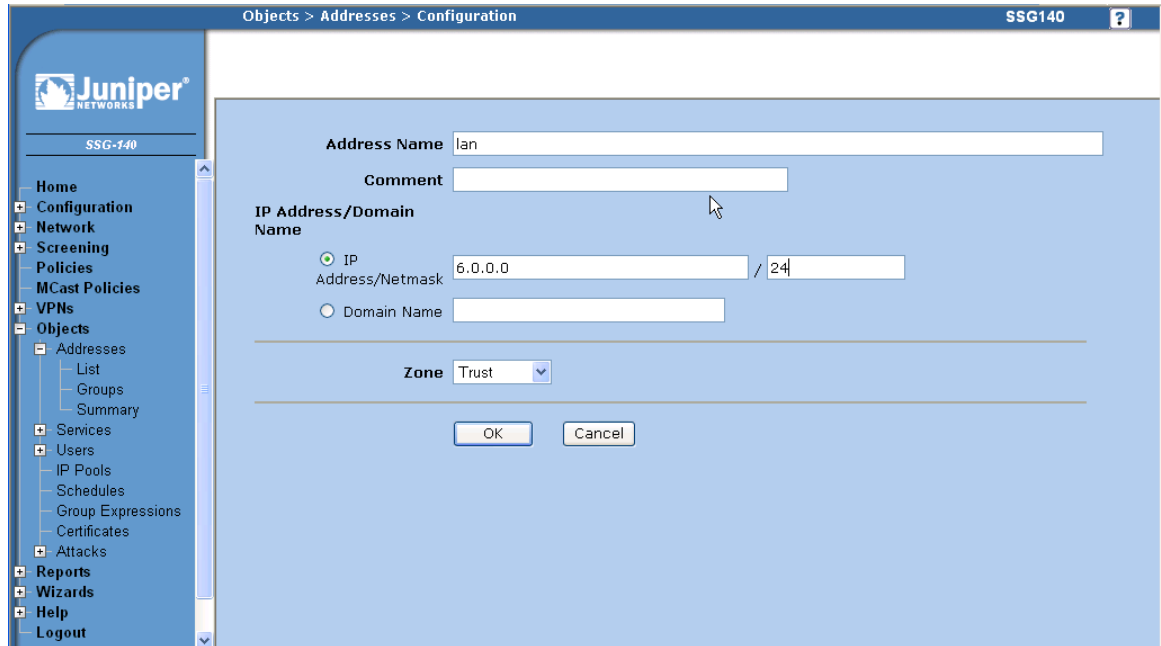
### CLI:

```
set l2tp "l2-tunnel" outgoing-interface ethernet0/0
set l2tp "l2-tunnel" remote-setting ippool "l2-pool"
```



## Step 5: Define address object for internal resources

An address object for internal resources is used in a policy to enforce traffic that passes through the firewall from the L2TP client.



The screenshot shows the Juniper WebUI configuration page for an address object. The breadcrumb navigation at the top reads "Objects > Addresses > Configuration". The page title is "SSG140". On the left is a navigation tree with categories: Home, Configuration, Network, Screening, Policies, MCast Policies, VPNs, Objects (expanded), Services, Users, Reports, Wizards, Help, and Logout. Under "Objects", "Addresses" is expanded to show "List", "Groups", and "Summary". The main configuration area is titled "Configuration" and contains the following fields:

- Address Name:** lan
- Comment:** (empty text box)
- IP Address/Domain Name:**
  - IP: Address/Netmask 6.0.0.0 / 24
  - Domain Name: (empty text box)
- Zone:** Trust (dropdown menu)

At the bottom of the configuration area are "OK" and "Cancel" buttons.

### WebUI:

Select Objects > Addresses > List, select Trust and click New.

Enter following and click OK.

Address Name: lan

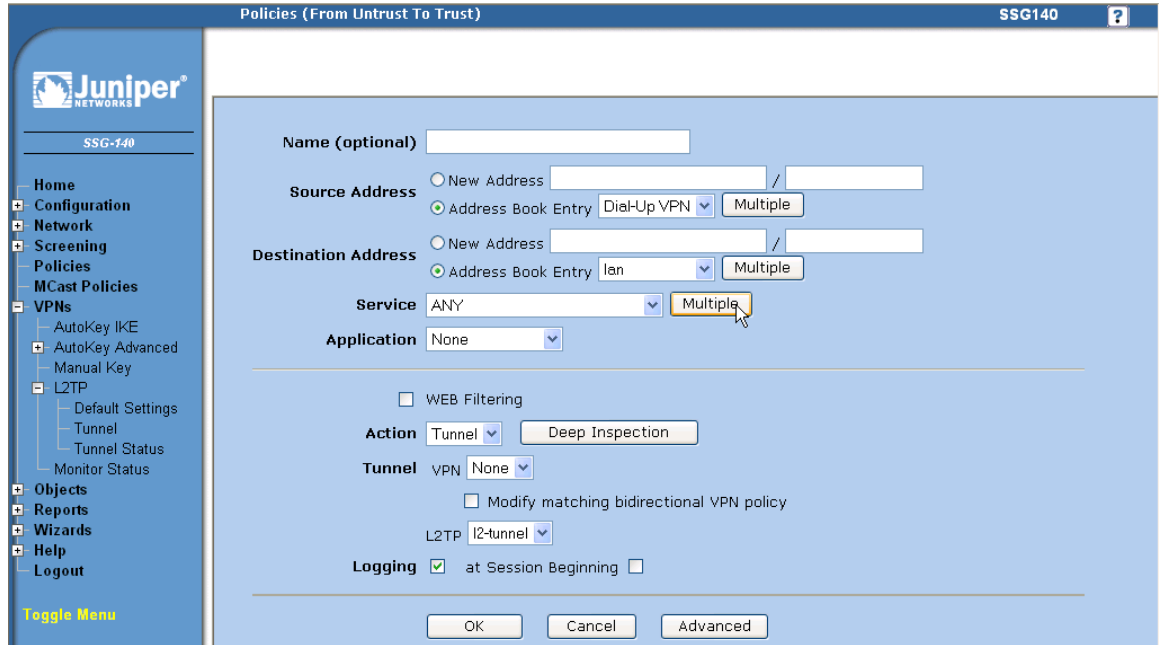
IP Address/Netmask: 6.0.0.0/24

### CLI:

```
set address trust lan 6.0.0.0/24
```

## Step 6: Create policy

To enable the L2TP client to send traffic passing through the tunnel to internal resources, a policy is need. Here, we created a policy to enable any traffic from the L2TP client to access internal resource.



### WebUI:

Select Policy with following selection, then click New.

From: Untrust

To: Trust

Enter following and click OK.

Source Address: Address Book Entry (selected), Dial-Up VPN

Destination Address: Address Book Entry, lan

L2TP: l2-tunnel

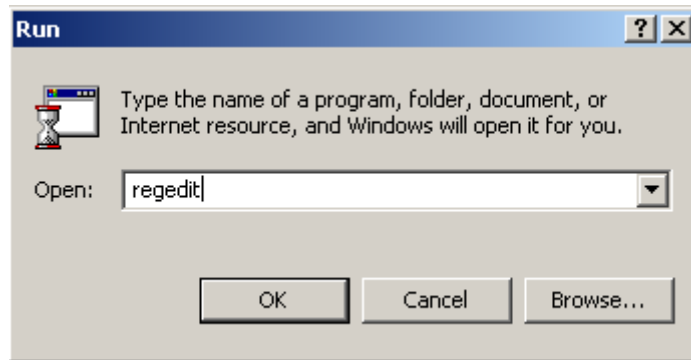
### CLI:

```
set policy id 1 from "Untrust" to "Trust" "Dial-Up VPN" "lan" "ANY" tunnel l2tp
"l2-tunnel"
```

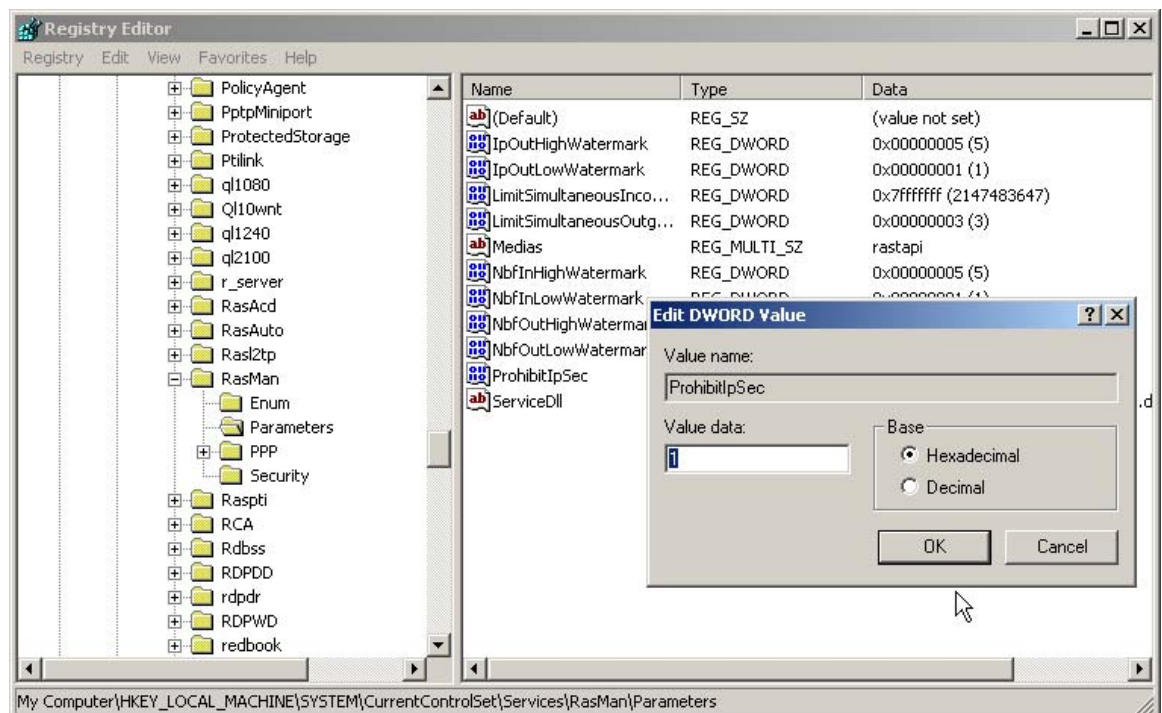
## Step 7: Configure native L2TP connection on Windows 2000

By default, the native L2TP client in Windows 2000 is enabled with encryption. That is the default L2TP connection from Windows 2000 native client, that is L2TP over IPsec. To override this default behavior, we need to edit the registry key ProhibitIPSec.

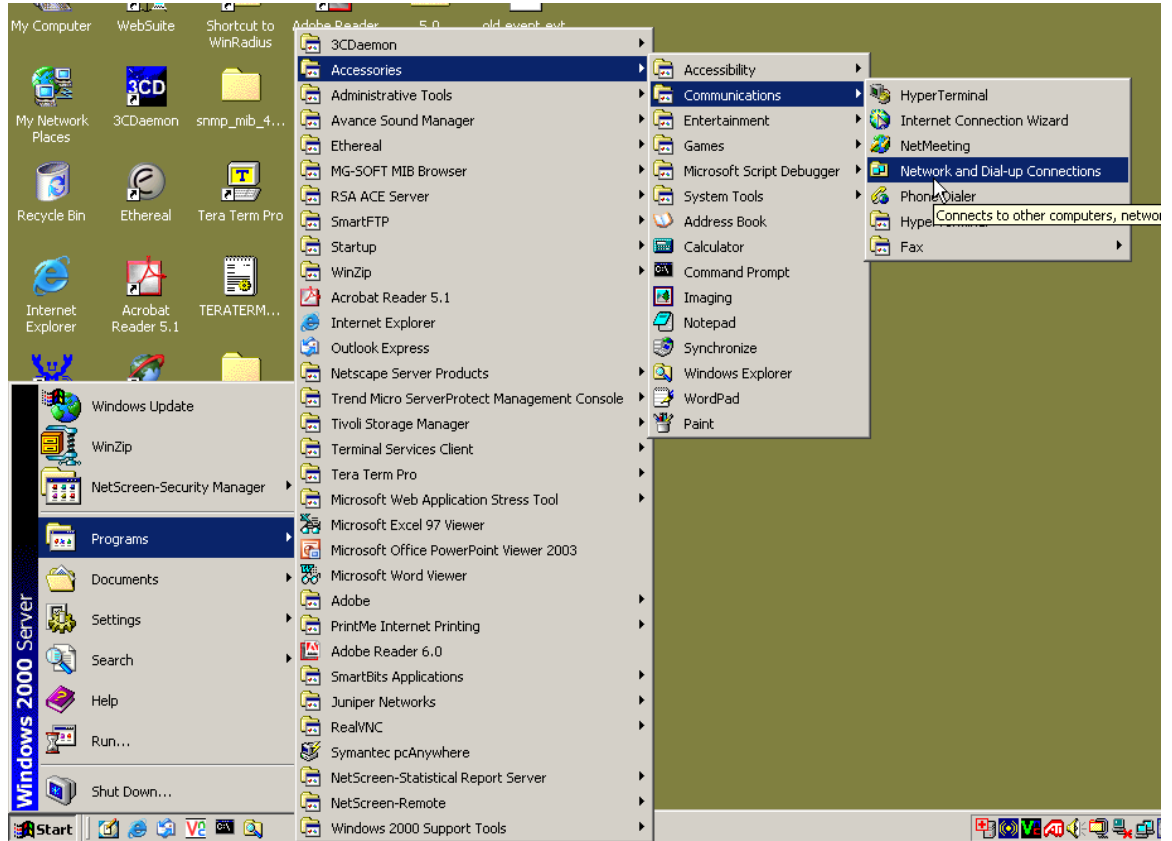
1. Login to Windows 2000 as administrator.
2. Execute regedit to access the Windows 2000 registry.



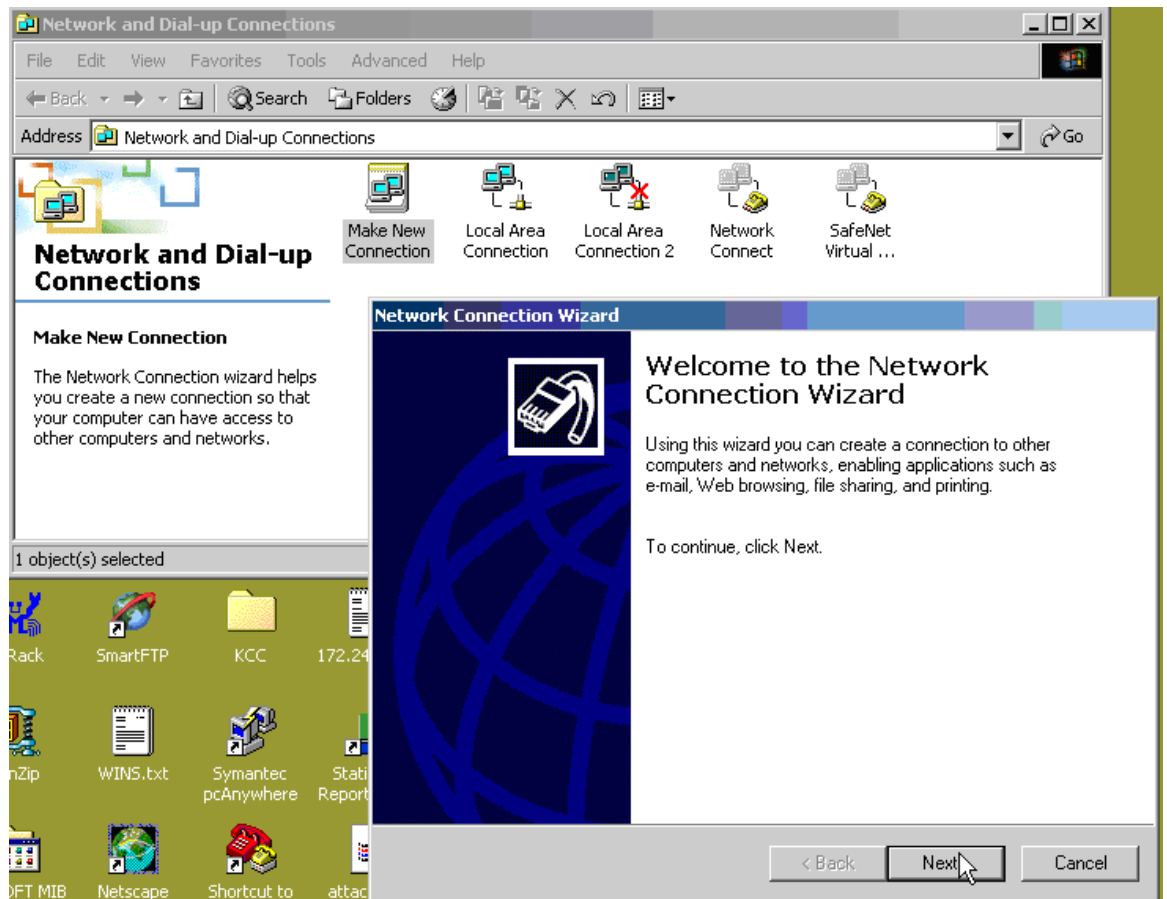
3. Navigate to the following:  
LOCAL\_MACHINE/SYSTEM/CurrentControlSet/Services/RasMan/Parameters/
4. If the ProhibitIPSec registry key exists, go to step 7. If the ProhibitIPSec registry key does not exist, create one: Select Edit > New > DWORD, then enter ProhibitIPSec on the new registry key.
5. Change the registry key value to 1.



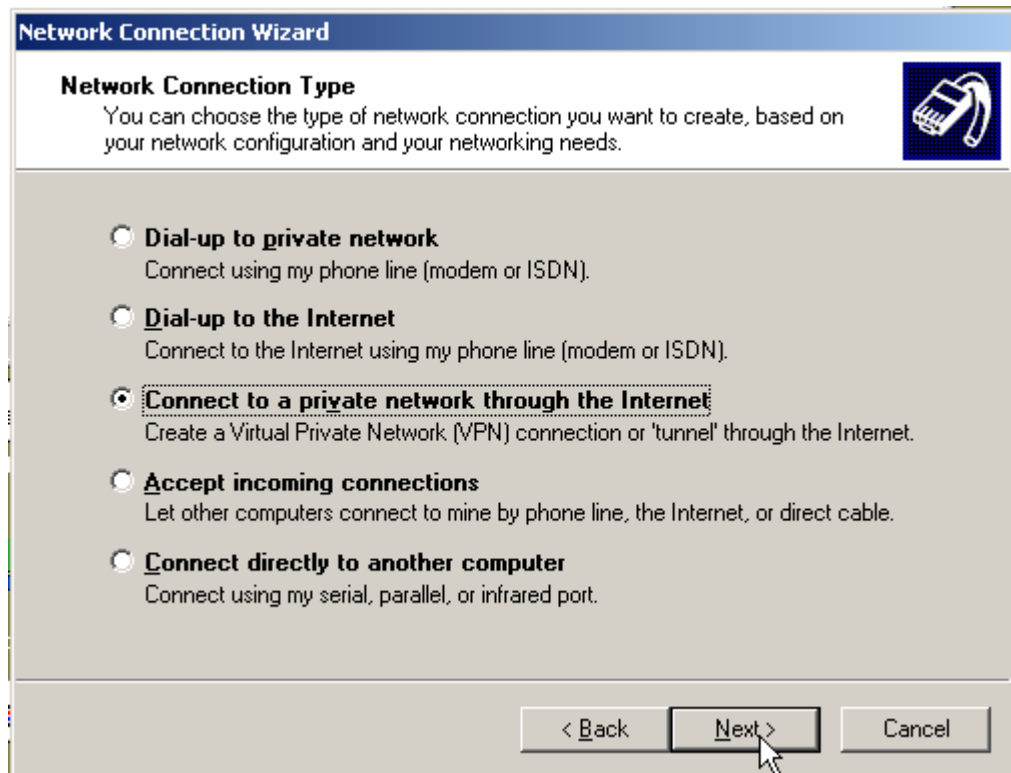
6. Save the change and reboot the PC.
7. Select "Start" > "Programs" > "Accessories" > "Communications" > "Network and Dial-up Connection".



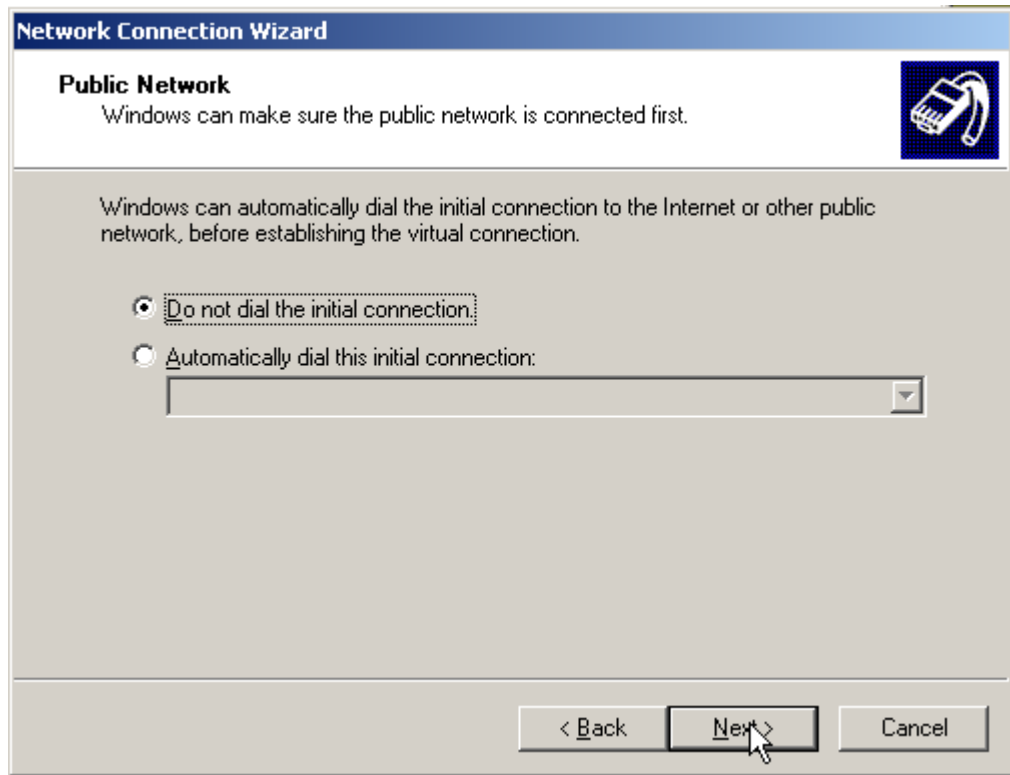
8. Double click “Make New Connection” and click Next.



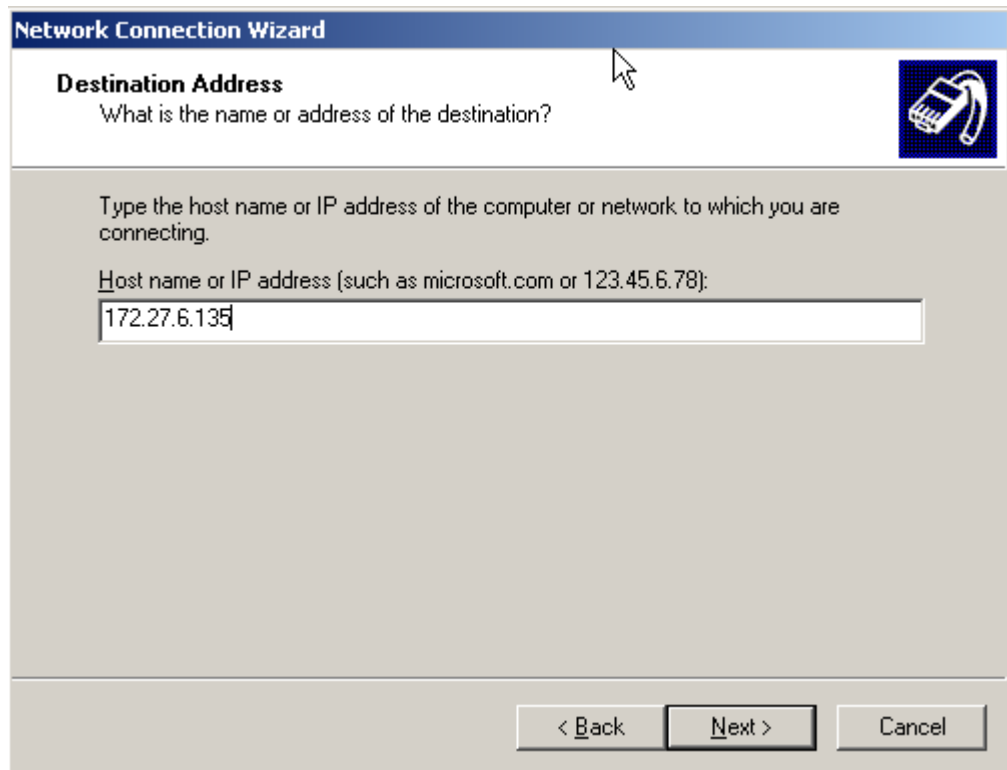
9. Select “Connect to a private network through the Internet” and click Next.



10. Select “Do not dial the initial connection” and click Next.



11. Enter the IP address of the firewall (172.27.6.135) and click Next.



**Network Connection Wizard**

**Destination Address**  
What is the name or address of the destination?

Type the host name or IP address of the computer or network to which you are connecting.

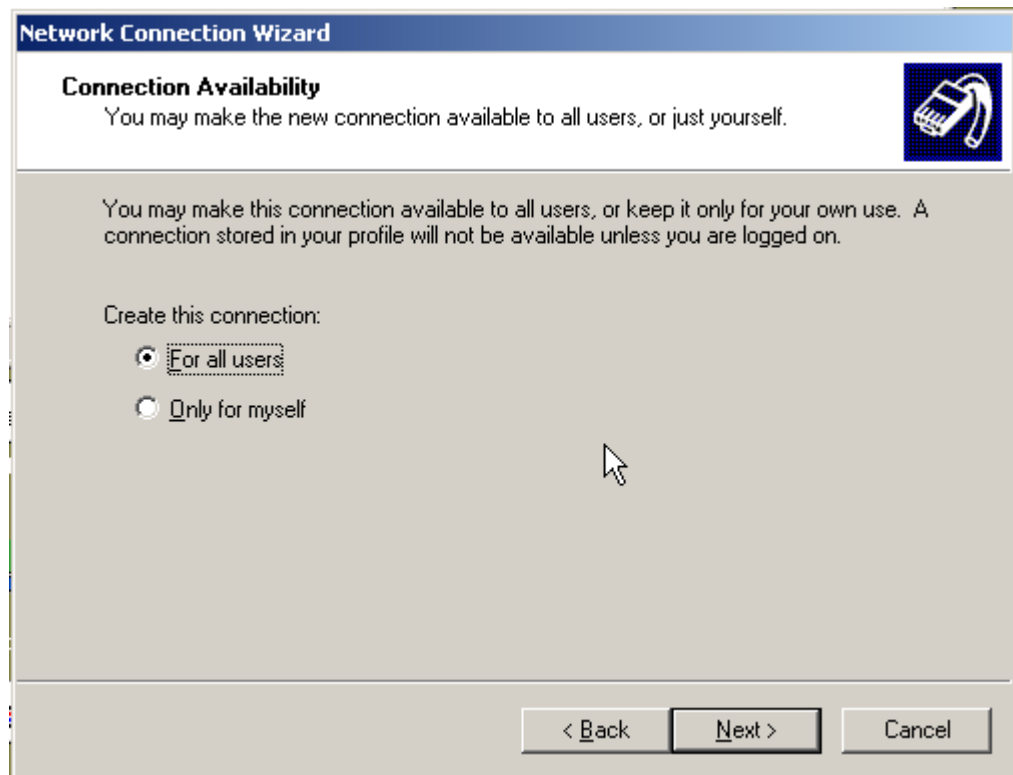
Host name or IP address (such as microsoft.com or 123.45.6.78):

172.27.6.135

< Back    Next >    Cancel



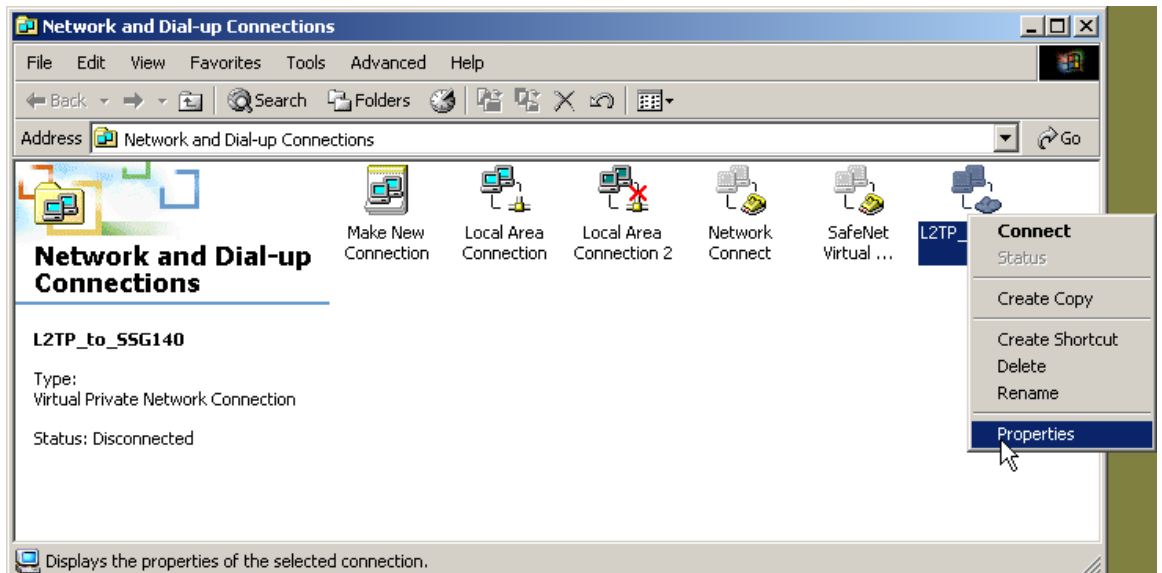
12. Select "For all users" and click Next.



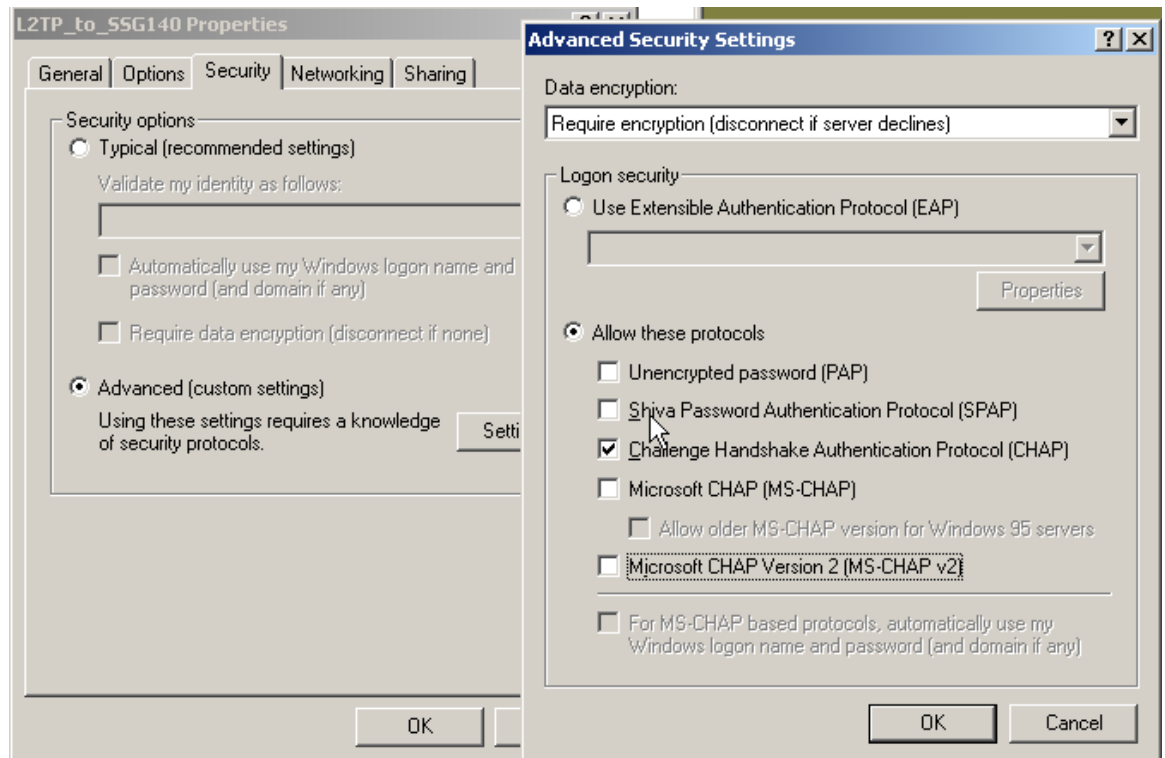
- Click Next again and enter the connection name (L2TP\_to\_SSG140), then click Finish.



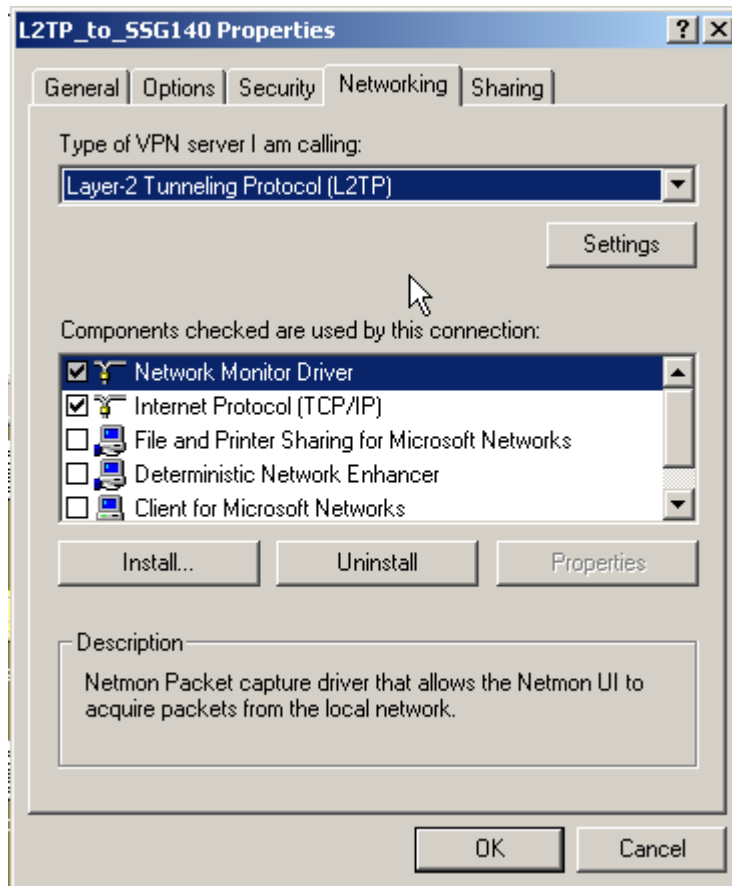
- Select the L2TP connection icon (L2TP\_to\_SSG140), right click and select Properties.



15. From the Security tag, select “Allow these protocols”. Uncheck all other protocols but just check “Challenge Handshake Authentication Protocol (CHAP)”, then click OK.



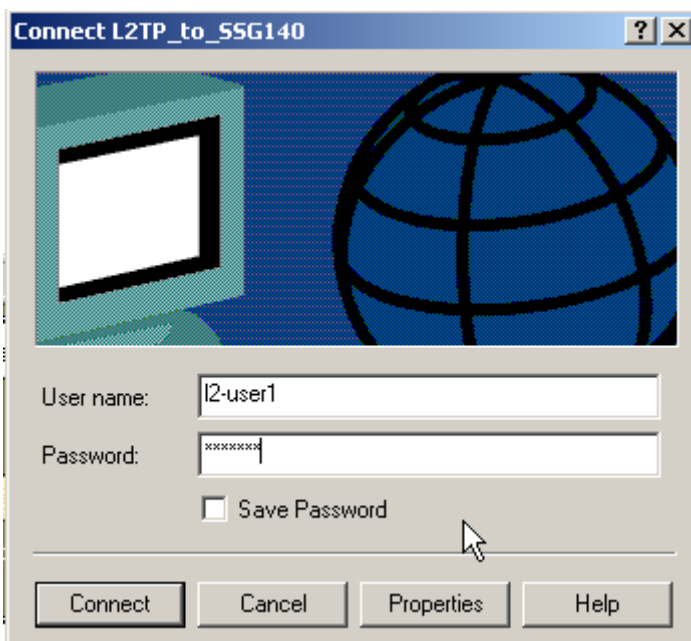
- From the Networking tag, select "Layer-2 Tunneling Protocol (L2TP)" from "Type of VPN" and click OK.



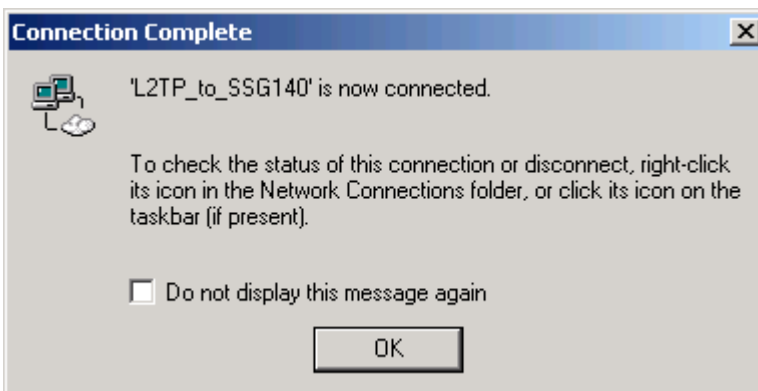
## Verifying Configuration

The configuration can be verified by connecting the PC L2TP client to firewall.

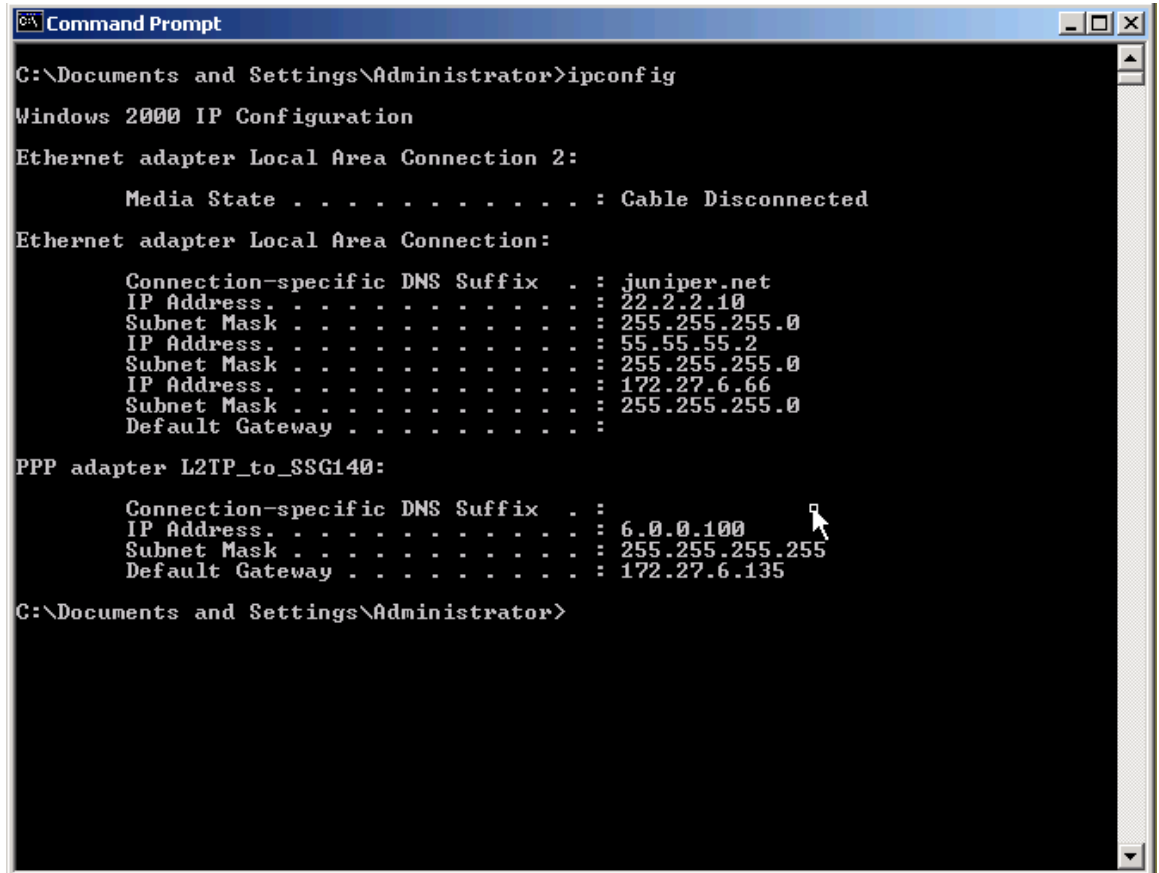
1. From “Network and Dial-up Connections”, double click the L2TP connection icon.
2. From the connect window, enter username and password, then click Connect.



3. When the connection is done, a connection complete window will be prompted.



4. After connected, open a command prompt. From the command prompt, execute the command “ipconfig” to check the IP address assigned.



```

C:\Documents and Settings\Administrator>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 2:

    Media State . . . . . : Cable Disconnected

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : juniper.net
    IP Address. . . . . : 22.2.2.10
    Subnet Mask . . . . . : 255.255.255.0
    IP Address. . . . . : 55.55.55.2
    Subnet Mask . . . . . : 255.255.255.0
    IP Address. . . . . : 172.27.6.66
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

PPP adapter L2TP_to_SSG140:

    Connection-specific DNS Suffix  . :
    IP Address. . . . . : 6.0.0.100
    Subnet Mask . . . . . : 255.255.255.255
    Default Gateway . . . . . : 172.27.6.135

C:\Documents and Settings\Administrator>

```

5. From the command prompt, ping to internal resources to check connectivity.
6. From the firewall CLI, check the L2TP tunnel status:

```

SSG140-> get l2tp l2-tunnel active
L2TP Name      Tunnel Id Peer Address      Port Peer Host      Calls State      t_info
-----
l2-tunnel      ( 4/ 4) 172.27.6.66      1701 tac1.tac1.ap      1  estblsh  80008004
call id(local/peer)=(1/1)
  assigned ip=6.0.0.100, user="l2-user1", type=incoming, state=establish
  Logged in at: 01/28/2008 16:28:31
l2-tunnel      ( 0/ 0) 0.0.0.0          0          0  idle  80000001

```

From the above output, it shows the source IP of the L2TP client and connection status. In addition, it shows the username and IP addresss assigned to the L2TP connection.

## Sample Configuration

```
SSG140-> get config
Total Config size 3692:
set clock timezone 0
set vrouter trust-vr sharable
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset auto-route-export
exit
set auth-server "Local" id 0
set auth-server "Local" server-name "Local"
set auth default auth server "Local"
set auth radius accounting port 1646
set admin name "netscreen"
set admin password "nKVUM2rwMUzPcrkG5sWIHdCtqkAibn"
set admin auth timeout 10
set admin auth server "Local"
set admin format dos
set zone "Trust" vrouter "trust-vr"
set zone "Untrust" vrouter "trust-vr"
set zone "DMZ" vrouter "trust-vr"
set zone "VLAN" vrouter "trust-vr"
set zone "Untrust-Tun" vrouter "trust-vr"
set zone "Trust" tcp-rst
set zone "Untrust" block
unset zone "Untrust" tcp-rst
set zone "MGT" block
set zone "DMZ" tcp-rst
set zone "VLAN" block
unset zone "VLAN" tcp-rst
set zone "Untrust" screen tear-drop
set zone "Untrust" screen syn-flood
set zone "Untrust" screen ping-death
set zone "Untrust" screen ip-filter-src
set zone "Untrust" screen land
set zone "V1-Untrust" screen tear-drop
set zone "V1-Untrust" screen syn-flood
set zone "V1-Untrust" screen ping-death
set zone "V1-Untrust" screen ip-filter-src
set zone "V1-Untrust" screen land
set interface "ethernet0/0" zone "Untrust"
set interface "ethernet0/1" zone "DMZ"
set interface "ethernet0/2" zone "Trust"
set interface "bril/0" zone "Untrust"
set interface ethernet0/0 ip 172.27.6.135/24
set interface ethernet0/0 route
unset interface vlan1 ip
set interface ethernet0/2 ip 6.0.0.1/24
set interface ethernet0/2 route
unset interface vlan1 bypass-others-ipsec
unset interface vlan1 bypass-non-ip
set interface ethernet0/0 ip manageable
set interface ethernet0/2 ip manageable
set interface ethernet0/0 manage ping
set interface ethernet0/0 manage ssh
set interface ethernet0/0 manage telnet
set interface ethernet0/0 manage snmp
set interface ethernet0/0 manage ssl
set interface ethernet0/0 manage web
set interface ethernet0/0 manage mtrace
set interface ethernet0/2 manage mtrace
unset flow no-tcp-seq-check
set flow tcp-syn-check
set console timeout 0
set pki authority default scep mode "auto"
set pki x509 default cert-path partial
set address "Trust" "lan" 6.0.0.0 255.255.255.0
set ippool "l2-pool" 6.0.0.100 6.0.0.110
```

```
set user "l2-user1" uid 1
set user "l2-user1" type l2tp
set user "l2-user1" password "mLFwMNHhNOzn2fsyjDCRjF4NCIncKcSfsQ=="
unset user "l2-user1" type auth
set user "l2-user1" "enable"
set ike respond-bad-spi 1
unset ike ikeid-enumeration
unset ike dos-protection
unset ipsec access-session enable
set ipsec access-session maximum 5000
set ipsec access-session upper-threshold 0
set ipsec access-session lower-threshold 0
set ipsec access-session dead-p2-sa-timeout 0
unset ipsec access-session log-error
unset ipsec access-session info-exch-connected
unset ipsec access-session use-error-log
set l2tp default dns1 1.1.1.1
set l2tp default dns2 1.1.1.2
set l2tp default ippool "l2-pool"
set l2tp default ppp-auth chap
set l2tp "l2-tunnel" id 1 outgoing-interface ethernet0/0
set l2tp "l2-tunnel" remote-setting ippool "l2-pool"
set url protocol websense
exit
set policy id 1 from "Untrust" to "Trust" "Dial-Up VPN" "lan" "ANY" tunnel l2tp
"l2-tunnel" log
set policy id 1
exit
set nsmgmt bulkcli reboot-timeout 60
set nsmgmt bulkcli reboot-wait 0
set ssh version v2
set config lock timeout 5
set snmp port listen 161
set snmp port trap 162
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset add-default-route
set route 0.0.0.0/0 gateway 172.27.6.1
set route 172.27.0.0/16 gateway 172.27.6.1
exit
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
exit
SSG140->
```

---

Copyright © 2007, Juniper Networks, Inc. All rights reserved. Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.