CALL THE TELSTRA BUSINESS
TECHNICAL HELPDESK ON 1800 066 594
VISIT TELSTRA.COM/BUSINESS

APR 10
CODE

BUSINESS

CISCO USER GUIDE

WELCOME TO TELSTRA BUSINESS BROADBAND EQUIPMENT – CISCO® 877W AND 1812[1] ROUTER

You have purchased Telstra Business Broadband Equipment Extras – Cisco® Customer premises equipment. The Cisco user guide will help you to configure and setup your new router, so you can get more out of your Telstra Business Broadband service.

ADSL CUSTOMERS

If you have purchased our Telstra Broadband Equipment Extras with Cisco ADSL Customer Premises Equipment (CPE), your included router is the Cisco 877W–K9. It has wireless capability.

ETHERNET CUSTOMERS

The Cisco 1812–K9 router does not have built-in wireless capability. If you require wireless capability, please consult your IT specialist or contact 1800 655 744 for information on our range of IT support options, available through Telstra Business Support Extras .

1. ABOUT THIS DOCUMENT – ABOUT SECURITY DEVICE MANAGER (SDM)

This is a step-by-step guide to help you configure your Cisco router with the Security Device Manager (SDM), so that it can be used with your Telstra Business Broadband ADSL or Ethernet service.

It will guide you through the basic steps to set up the configuration and features for the Cisco 877W or 1812 router supplied with your Telstra Business Broadband Equipment Extras.

The user guide requires the reader to have a basic working knowledge of Cisco equipment, and should be used to supplement the Cisco 850, Cisco 870 and 1800 Series Access Routers Cabling and Quick Start Guide, which is included in your Telstra Business Broadband Equipment kit.

To help make the set up of the basic and standard configurations easier, we recommend customers familiarise themselves with the Security Device Manager (your SDM software is included in this Extras package).

Customers requiring more advanced router configuration or Local Area Network (LAN) settings should use the Command Line Interface (CLI)[2].

If you do not have the expertise to do this, please consult your IT specialist, Account Representative or call 1800 655 744 for more information on our range of IT support options, available through the Business Support Extras[3].

2. THINGS TO NOTE BEFORE YOU START

a. Please ensure you have read the minimum systems requirements and compatibility criteria.

b. Ensure that all hardware meets minimum system requirements as per section 3.

c. Please store this user guide in a secure place, for quick and easy reference.

d. You can access the router in two ways:

   1. Command Line Interface[4] (for advanced configuration & LAN settings)

   2. Security Device Manager (recommended).

e. All the commonly requested features noted in section 10 and 11 have been made available on your supplied router (877W or 1812)[5]; this document will guide you through how to enable these features using the SDM.

f. Please ensure you have read the Cisco 850 & Cisco 870 Series or the 1800 Series Access Routers Cabling and Quick Start Guide for connecting your Cisco router to the Telstra Business Broadband ADSL or Ethernet service. This Quick Start Guide is included in the kit.

g. We recommend you change or reset your router default password as soon as possible after you have installed and configured your supplied Cisco router.

3. MINIMUM SYSTEMS REQUIREMENTS

A. SDM

The following table defines the minimum system requirements to install the SDM on your computer.

COMPUTER	OPERATING SYSTEM	REQUIREMENTS
Computer with a Pentium®-class processor or greater	• Windows Vista® (Business Edition) • Windows® XP Professional • Windows 2003 Server (Standard Edition) • Windows 2000 Professional with Service Pack 4 Windows 2000 Advanced Server is not supported	• Microsoft TCP/IP installed (confirm via Start > Settings > Control Panel > Network > Protocols orConfiguration) • 9 MB hard disk space • RAM: – 128 MB for Windows XP (256 MB recommended) – 64 MB for Windows 2000 (128 MB recommended)

Web browser versions

Cisco SDM can be used with the following browsers:

- Firefox® 1.0.6 and later versions
  Please note: if you have Firefox set as your default web browser and would like to continue to use it, you will need to note the following:
  – ensure that the pop-up blocker is switched off
  – you will not be able to connect using https or secure mode.
- Internet Explorer® 5.5 and later versions.
- Netscape® 7.1, 7.2, and 9.0.

Java™ Run Time Environment (JRE)

Cisco SDM requires Sun Java™ Runtime Environment (JRE). The Java Run Time Environment can be downloaded from the following webpage: **www.java.com/getjava/**

B. Wireless

Please ensure you check the following requirements for using WPA wireless protocol.

- Your wireless card must support WPA or WEP.
- Make sure you have the most current drivers for your wireless card.
- Your computer must have Windows XP service pack 2 installed and all the latest updates (you can download them through the Windows update site at **windowsupdate.microsoft.com**).

Important first step:

- Windows XP users must install a Microsoft update to enable WPA support before continuing.
- The update can be downloaded at **support.microsoft.com/kb/893357**
- You will need to restart your computer after downloading and installing the update.
- Wireless Access is supported via Mac OS® X 10.3.3 or later with AirPort® software 3.3 or later.

C. Cisco VPN Client

The following table indicates the system requirements to install the Cisco VPN Client on each of the supported platforms.[6]

COMPUTER	OPERATING SYSTEM	REQUIREMENTS
Computer with a Pentium®-class processor or greater, including Tablet PC (Cisco VPN Client version 5.0.03.560)	Windows Vista (all released versions) Windows XP Windows 2000[7] TabletPC 2004/2005 **Note** For all Windows operating systems, only 32-bit platforms are supported	Microsoft TCP/IP installed (confirm via Start > Settings > Control Panel > Network > Protocols or Configuration). 50 MB hard disk space RAM: – 128 MB for Windows XP (256 MB recommended) – 64 MB for Windows 2000 (128 MB recommended) – 32 MB for Windows 98 (see note under Operating Systems) – 64 MB for Windows NT and Windows ME (see note under Operating Systems)
Apple® computer (Cisco VPN Client version 4.9.00.0050)	Mac OS® X, Version 10.4 or later	50 MB hard disk space PPC only. None of the Release 4.9.00.0050 Mac OS® X 10.4 and higher on both Power PC (PPC) and Intel processors Not supported on Mac OS® X 10.3.9 and earlier

Cisco VPN Client for Windows Vista, release 5.0.03.560, does **NOT** support the following features:

- System upgraded from Windows XP or earlier Windows operating systems to Vista. **Please note**: Clean OS installation if required.
- Start Before Logon.
- SmartCard authentication.
- Integrated firewall.
- InstallShield.
- Auto Update.

Advisory about Connection Time on Windows

Using the VPN Client to connect to a Windows Vista system might take longer than the time needed to connect to a Windows 2000 or Windows XP system.

The actual time it takes to connect may vary for each customer.

4. SECURITY DEVICE MANAGER

The Security Device Manager is a software program provided by Cisco to allow users to configure router IOS, Security and Network connection features via a web based Graphical User Interface (GUI).

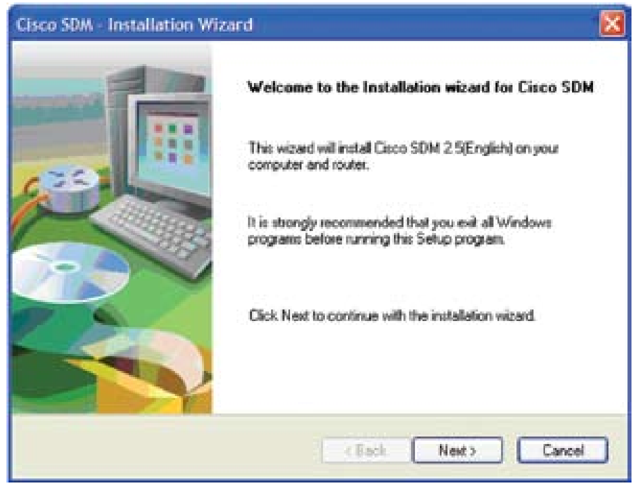
5. WAYS TO ACCESS THE SDM OFF CD OR GUI

We recommend users access the SDM GUI by opening up a web browser and typing in: **https://10.10.10.1**

Please note: An internet connection does not need to be open in order to access this site as it operates at the router level.

6. INSTALLING THE SECURITY DEVICE MANAGER (SDM VERSION 2.5)

It is recommended that users install the Security Device Manager directly to the PC or desktop.



Welcome to the Installation wizard for Cisco SDM

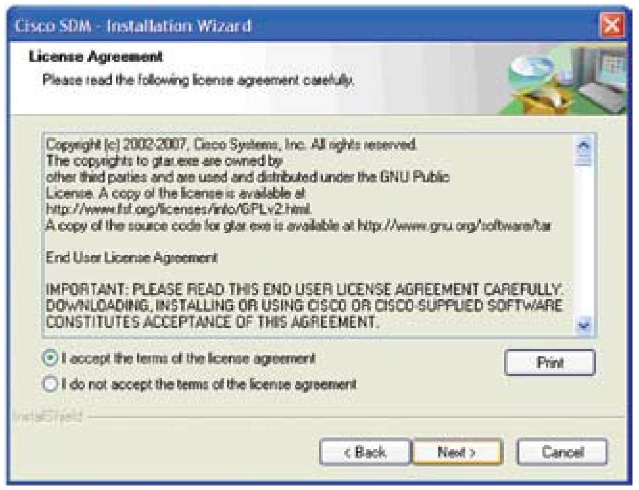
This wizard will install Cisco SDM 2.5(English) on your computer and router.

It is strongly recommended that you exit all Windows programs before running this Setup program.

Click Next to continue with the installation wizard.

STEPS:

1. Insert the SDM CD into your CD Drive.
2. Download the SDM zip file to the PC.
3. Extract the SDM zip file. Go to SDM installer folder and click **setup.exe**. The installation wizard will start as shown above.
4. Click **Next**.



License Agreement

Please read the following license agreement carefully.

Copyright (c) 2002-2007, Cisco Systems, Inc. All rights reserved.
The copyrights to gtar.exe are owned by
other third parties and are used and distributed under the GNU Public
License. A copy of the license is available at
http://www.fsf.org/licenses/info/GPLv2.html.
A copy of the source code for gtar.exe is available at http://www.gnu.org/software/tar

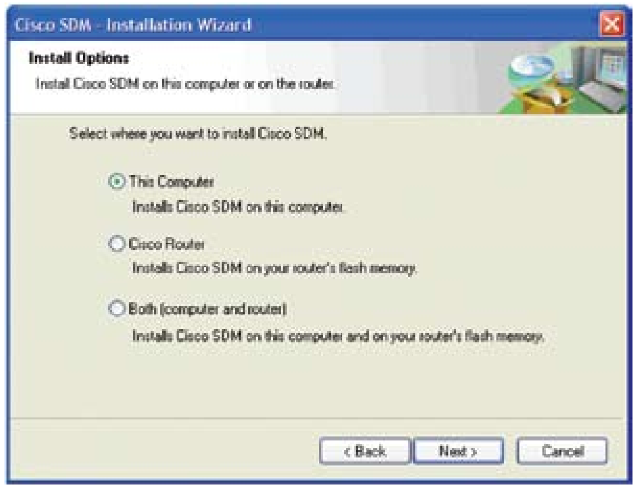
End User License Agreement

IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.

● I accept the terms of the license agreement

○ I do not accept the terms of the license agreement

5. Select **I accept the terms of the license agreement as shown above**.
6. Click **Next**.



Install Options

Install Cisco SDM on this computer or on the router.

Select where you want to install Cisco SDM.

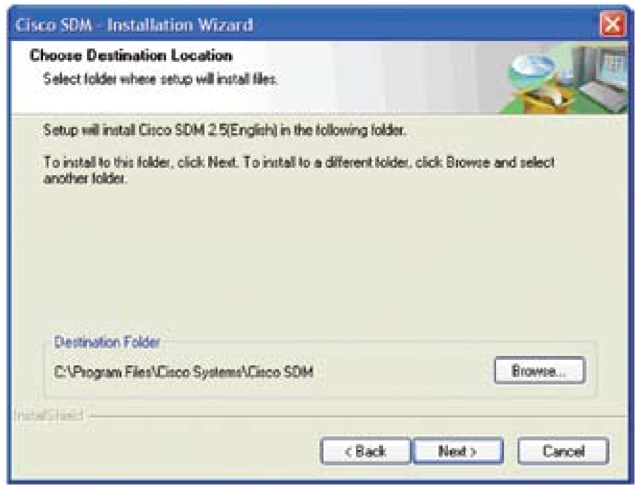
● This Computer
Installs Cisco SDM on this computer.

○ Cisco Router
Installs Cisco SDM on your router's flash memory.

○ Both (computer and router)
Installs Cisco SDM on this computer and on your router's flash memory.

7. Select **This Computer** – as shown above

8. Click **Next**.



Choose Destination Location

Select folder where setup will install files.

Setup will install Cisco SDM 2.5(English) in the following folder.

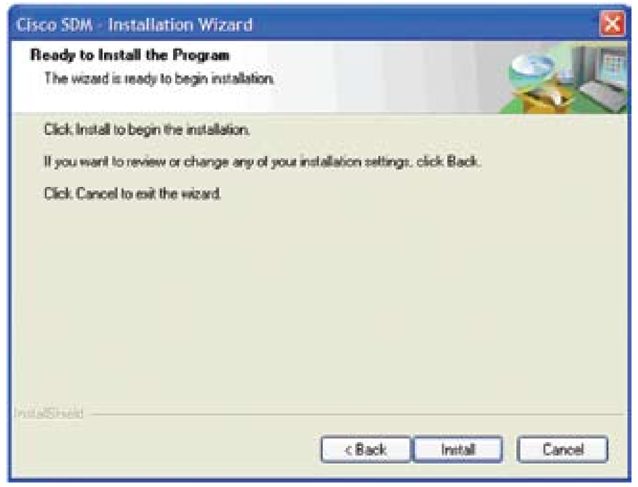
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder
C:\Program Files\Cisco Systems\Cisco SDM

9. Accept the default destination folder – as show above

10. Click **Next**.

You are now ready to install:



Ready to Install the Program

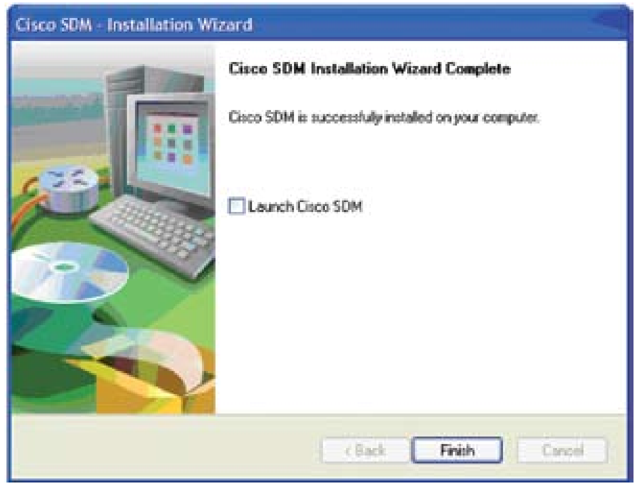
The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back.

Click Cancel to exit the wizard.

11. Click **Install**.



Cisco SDM Installation Wizard Complete

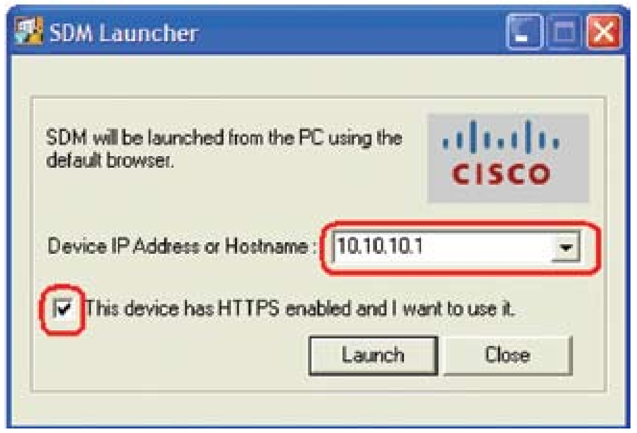
Cisco SDM is successfully installed on your computer.

□ Launch Cisco SDM

12. Click **Finish** after successful installation – as shown above.

STEPS:

1. Go to Start – All Programs – Cisco Systems – Cisco SDM – Cisco SDM. You will then be prompted with the below text box.


SDM Launcher

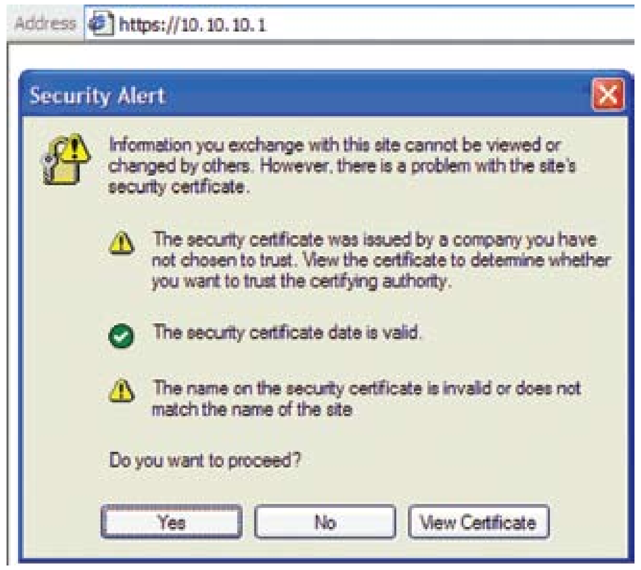
SDM will be launched from the PC using the default browser.

Device IP Address or Hostname : 10.10.10.1

☑ This device has HTTPS enabled and I want to use it.

2. Enter the **Device IP address** of the router. Telstra default shown above 10.10.10.1.
3. Select **This device has HTTPS enabled and I want to use it**.
4. Click **Launch**.

A Security Alert will appear as per below:


Address https://10. 10. 10. 1

Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

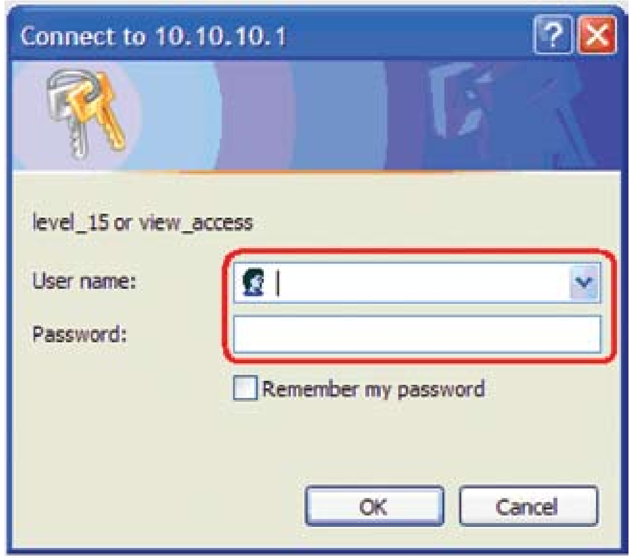
The security certificate date is valid.

The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

5. Click **Yes**.

You will be prompted to enter the user name and password.


Connect to 10.10.10.1

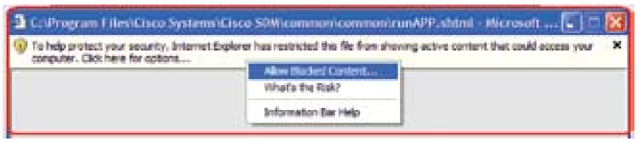
level_15 or view_access

User name:

Password:

□ Remember my password

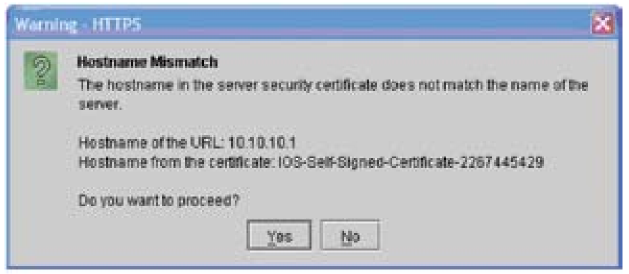
6. Enter **User name** and **Password**. A default administrator user name and password "advantage/advantage" has been pre-configured into the router configuration. For your network and router security, you are advised to change your user name and password. See section 8 (F) – **Adding User name and Password**.


C:\Program Files\Cisco Systems\Cisco SDM\common\common\runAPP.shtml - Microsoft ...

To help protect your security, Internet Explorer has restricted this file from showing active content that could access your computer. Click here for options...

7. An error may occur such as the one shown above. To unblock the SDM popup page, move your mouse cursor over the yellow bar and right click the mouse and select **Allow Blocked Content**.

THE popup screen will then Appear: "Warning – HTTPS"


Warning - HTTPS

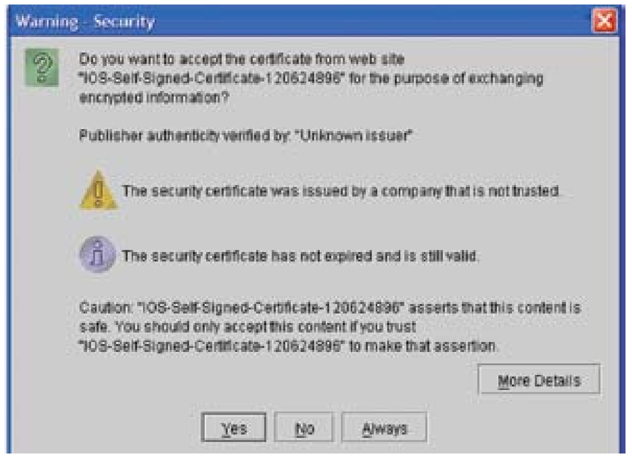
Hostname Mismatch

The hostname in the server security certificate does not match the name of the server.

Hostname of the URL: 10.10.10.1
Hostname from the certificate: IOS-Self-Signed-Certificate-2267445429

Do you want to proceed?

8. This is a self signed certificate by the router, so the publisher will be unknown. This is the correct behaviour, Click **Yes**.


Warning - Security

Do you want to accept the certificate from web site "IOS-Self-Signed-Certificate-120624896" for the purpose of exchanging encrypted information?

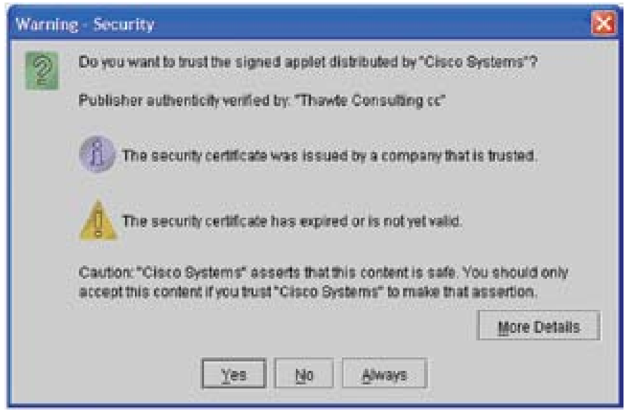
Publisher authenticity verified by: "Unknown issuer"

The security certificate was issued by a company that is not trusted.

The security certificate has not expired and is still valid.

Caution: "IOS-Self-Signed-Certificate-120624896" asserts that this content is safe. You should only accept this content if you trust "IOS-Self-Signed-Certificate-120624896" to make that assertion.

9. A pop up screen will now show with **Warning – Security** as above. Click **Yes**.


Warning - Security

Do you want to trust the signed applet distributed by "Cisco Systems"?

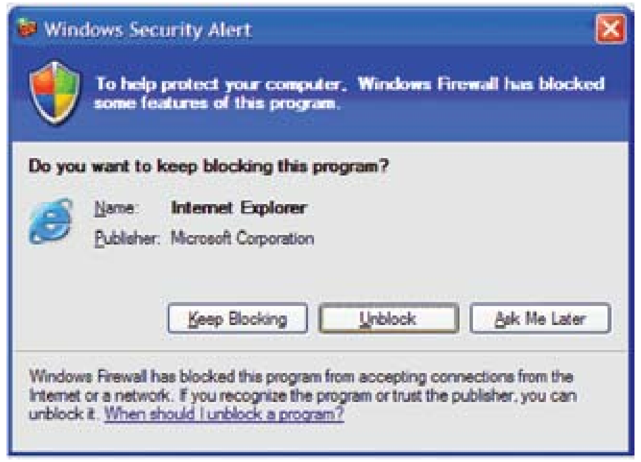
Publisher authenticity verified by: "Thawte Consulting cc"

The security certificate was issued by a company that is trusted.

The security certificate has expired or is not yet valid.

Caution: "Cisco Systems" asserts that this content is safe. You should only accept this content if you trust "Cisco Systems" to make that assertion.

10. A warning will then appear, Click **Yes**.


Windows Security Alert

To help protect your computer, Windows Firewall has blocked some features of this program.

Do you want to keep blocking this program?

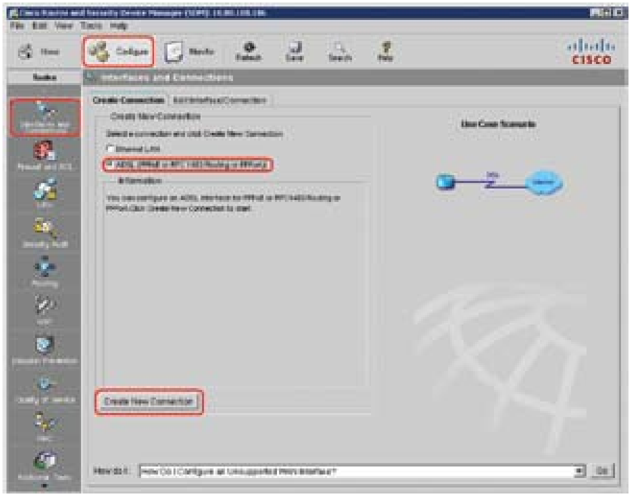
Name: **Internet Explorer**
Publisher: Microsoft Corporation

Windows Firewall has blocked this program from accepting connections from the Internet or a network. If you recognize the program or trust the publisher, you can unblock it. When should I unblock a program?

11. Windows Security Alert may pop up. Click **Unblock**.

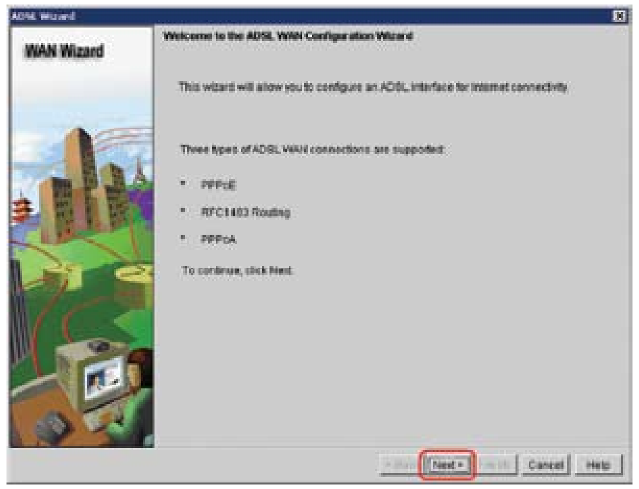
A. Configuring Interfaces:

1. Configuring your ADSL (WAN) Interface



STEPS:

1. Click **Configure**.
2. Click **Interfaces and Connections** in the **Tasks** section.
3. Select **ADSL (PPPoE or RFC 1483 Routing or PPPoA)**.
4. Click **Create New Connection**.


ADSL Wizard

WAN Wizard

Welcome to the ADSL WAN Configuration Wizard

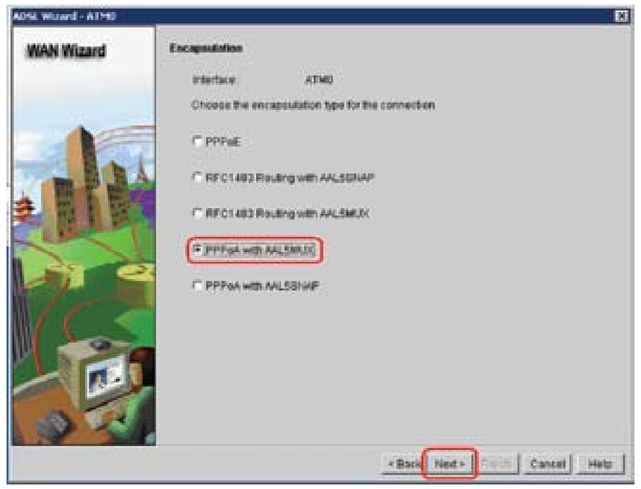
This wizard will allow you to configure an ADSL interface for internet connectivity

Three types of ADSL WAN connections are supported:

- PPPoE
- RFC1483 Routing
- PPPoA

To continue, click Next.

5. Click **Next**.


ADSL Wizard - ATM0

WAN Wizard

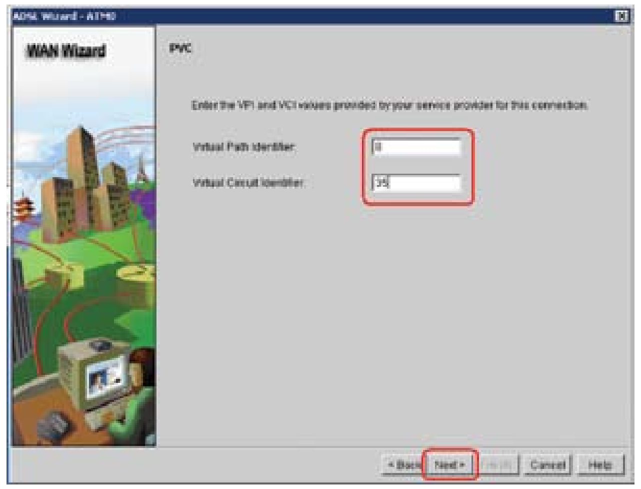
Encapsulation

Interface: ATM0

Choose the encapsulation type for the connection

○ PPPoE
○ RFC1483 Routing with AAL5SNAP
○ RFC1483 Routing with AAL5MUX
● PPPoA with AAL5MUX
○ PPPoA with AAL5SNAP

6. Select **PPPoA with AAL5MUX**.
7. Click **Next**.


ADSL Wizard - ATM0

WAN Wizard

PVC

Enter the VPI and VCI values provided by your service provider for this connection.

Virtual Path Identifier: 8

Virtual Circuit Identifier: 35

8. Enter values for **Virtual Path Identifier** (VPI) and **Virtual Circuit Identifier** (VCI). The VPI and VCI are obtained from the **Configuration Advice** from Telstra.
9. Click **Next** (if successful, move on to step 10).

Please note:

If the previous steps fail at this point, we recommend you take the following action:

a. Click **Configure** – as per steps on page 11.

b. Click **Interfaces and Connections** from the **Tasks** section.

c. Click **Edit Interface/Connection**.

d. Highlight **ATM0.1**

e. Double Click on **Username** on the bottom half of the screen.

f. Click **Authentication** in the pop up box that appears.

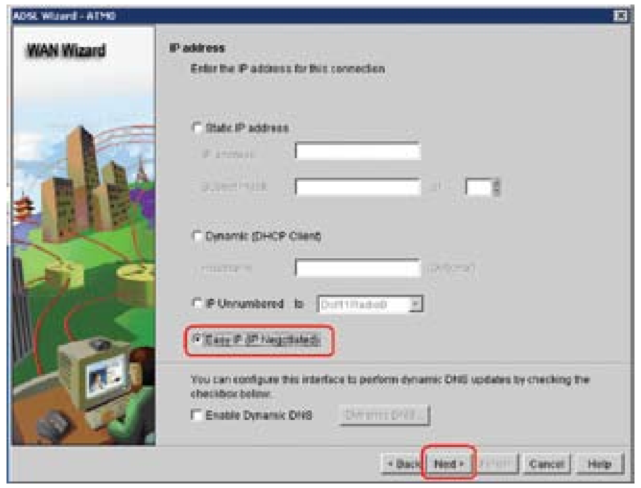
g. Populate **Username, New Password** and **Confirm new Password** fields, caps authentication should already be selected.

h. Click **OK**.

i. Click **OK** again.

j. Click **File/Write to Startup config**

k. Click **Yes** when prompted to continue with the copy process


ADSL Wizard - ATM0

WAN Wizard

IP address

Enter the IP address for this connection

○ Static IP address

IP address:

Subnet mask:

○ Dynamic (DHCP Client)

Hostname: (optional)

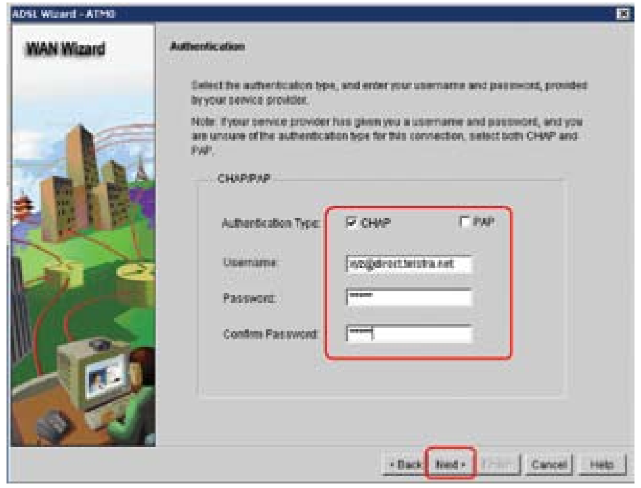
○ IP Unnumbered to Dot11Radio0

● Easy IP (IP Negotiated)

You can configure this interface to perform dynamic DNS updates by checking the checkbox below.

□ Enable Dynamic DNS

10. Select **Easy IP (IP Negotiated)** as shown above.
11. Click **Next**.


ADSL Wizard - ATM0

WAN Wizard

Authentication

Select the authentication type, and enter your username and password, provided by your service provider.

Note: If your service provider has given you a username and password, and you are unsure of the authentication type for this connection, select both CHAP and PAP.

CHAP/PAP

Authentication Type: ☑ CHAP □ PAP

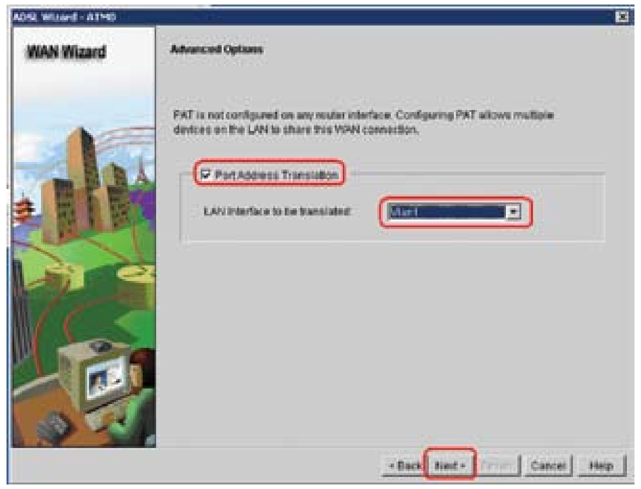
Username: xyz@direct.telstra.net

Password: *****

Confirm Password: *****

12. **Authentication Type** – Select **CHAP**.
13. Enter the **Username** and **Password** from the **Configuration Advice** provided by Telstra.
14. Click **Next**.

Please note: The above is provided as an example.


ADSL Wizard - ATM0

WAN Wizard

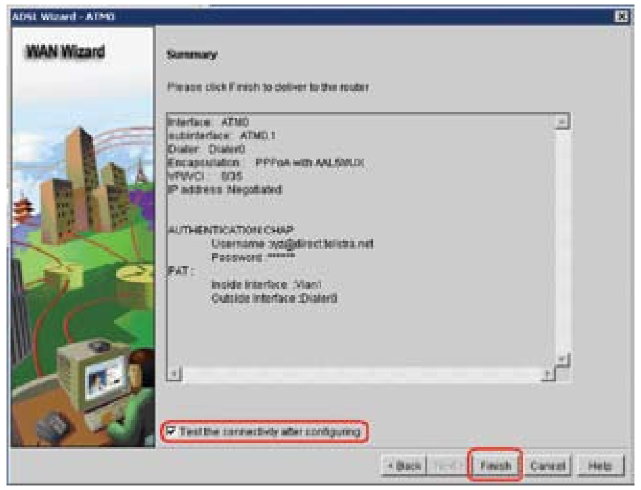
Advanced Options

PAT is not configured on any router interface. Configuring PAT allows multiple devices on the LAN to share this WAN connection.

☑ Port Address Translation

LAN interface to be translated: Vlan1

15. Select **Port Address Translation**.
16. **LAN interface to be translated** – Click drop down menu and select your LAN interface.
17. Click **Next**.



ADSL Wizard - ATM0

WAN Wizard

Summary

Please click Finish to deliver to the router

Interface: ATM0
subinterface: ATM0.1
Dialer: Dialer0
Encapsulation: PPPoA with AAL5MUX
VPI/VCI: 8/35
IP address: Negotiated

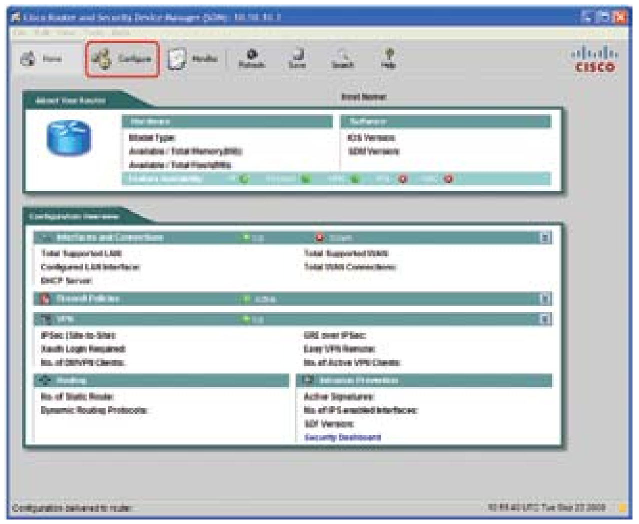
AUTHENTICATION CHAP
Username: xyz@directtelstra.net
Password: ******
PAT :
Inside Interface: Vlan1
Outside Interface: Dialer0

☑ Test the connectivity after configuring

18. Select **Test the connection after configuring**.

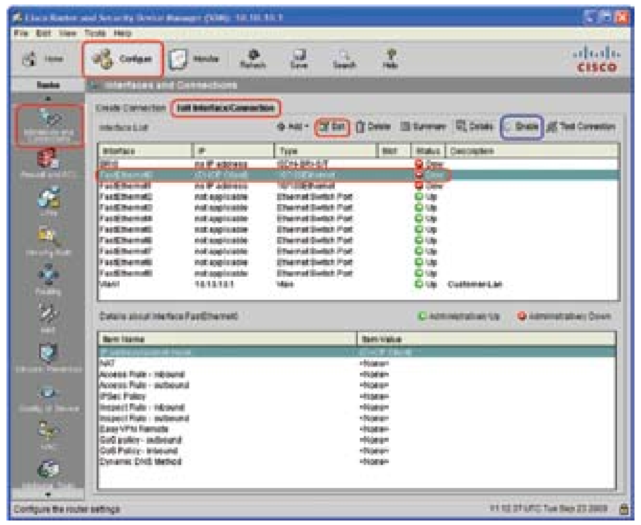
19. Click **Finish**.

2. Configuring Ethernet/Static Interface



STEPS:

1. Select **Configure** as shown above.



2. Click **Interfaces and Connections** from the **Tasks** section.

3. Click **Edit Interface/Connection**.

4. Highlight **Fastethernet0** interface.

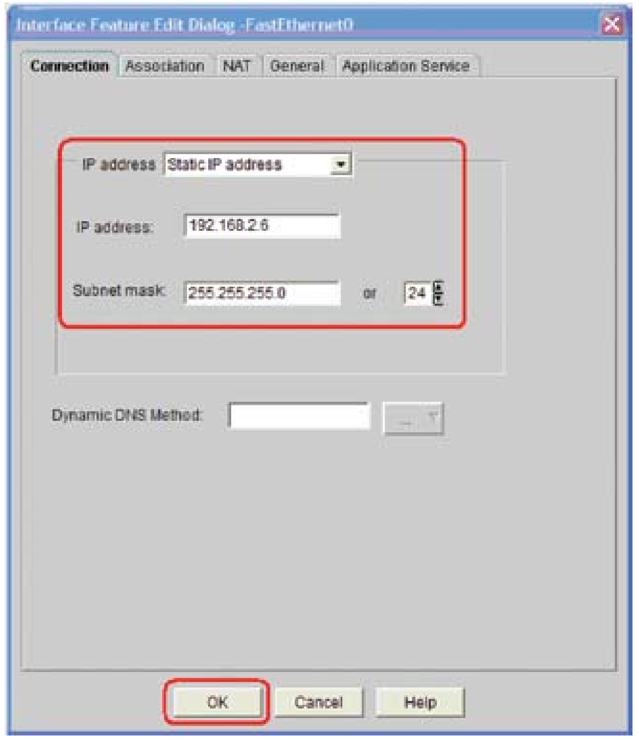
5. Click **Enable**. The status column should now change from **Down** to **Up**.

6. Click **Edit Interface Connection** tab.

7. Click and highlight Interface and click **Edit**

   Please note: The **Edit** tab may not always be active. If this does not work, please use/follow the **create connection** wizard.

You will be provided with the following dialogue box:



Interface Feature Edit Dialog -FastEthernet0

IP address: Static IP address

IP address: 192.168.2.6

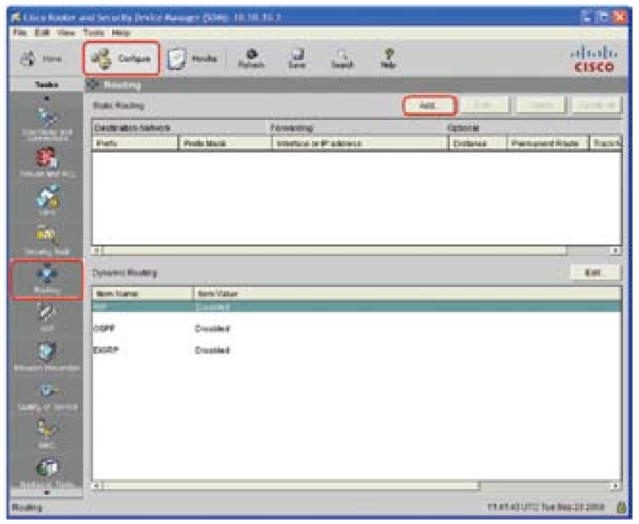
Subnet mask: 255.255.255.0 or 24

Dynamic DNS Method:

8. Fill in the details as shown above and click **OK**.

Please note: the above **IP address** is used as an example only – the actual static **IP address** is detailed in your configuration email for Telstra Business Broadband.

B. Configuring Static Route



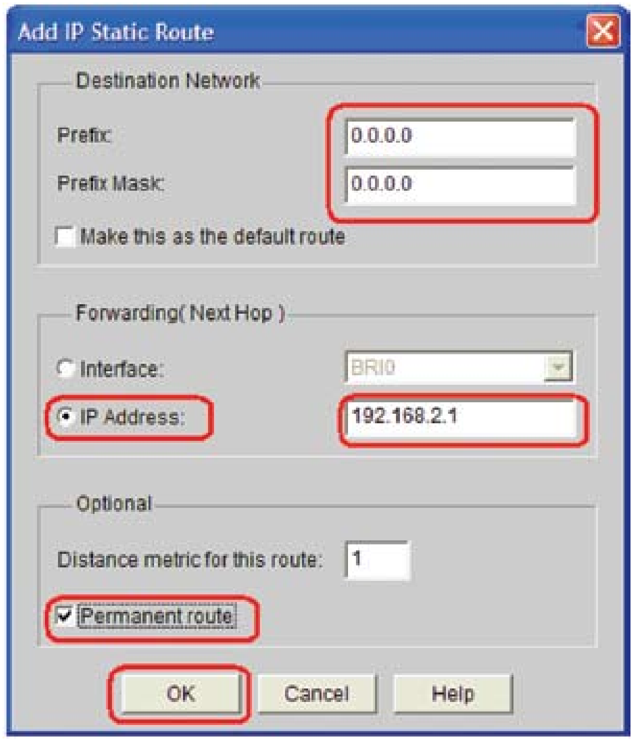
STEPS:

1. Click **Configure**.

2. Click **Routing** from the **Tasks** section – on the left hand side of the screen.

3. Click **Add** as shown above.

You will be provided with the following screen to add your static route:



Add IP Static Route

Destination Network

Prefix: 0.0.0.0

Prefix Mask: 0.0.0.0

□ Make this as the default route

Forwarding(Next Hop)

○ Interface: BRI0

● IP Address: 192.168.2.1

Optional

Distance metric for this route: 1

☑ Permanent route

Fill in the details as shown above.

4. Select **IP Address** radio button.

5. Enter your default route address.

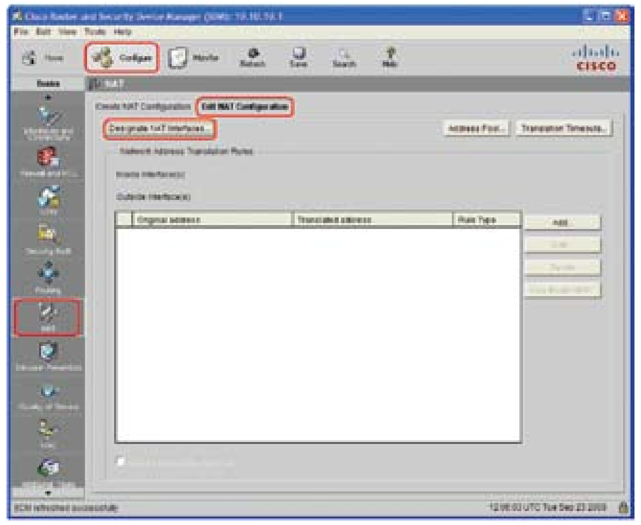
6. Select **Permanent route**.

7. Click **OK**

Please note: The above shows a sample default route.

C. Network Address Translation (NAT)/Port Address Translation (PAT)

1. Defining Trusted and Untrusted Interface



STEPS:

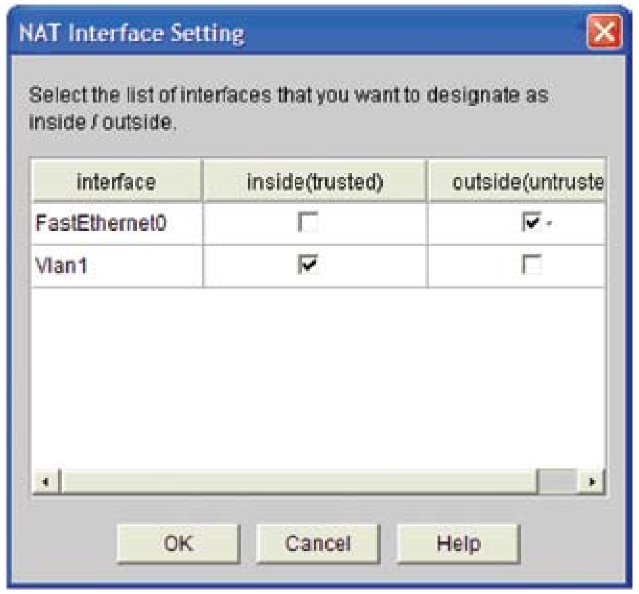
1. Click **Configure**.

2. Click **NAT** from the **Tasks** section.

3. Select **Edit NAT Configuration** tab.

4. Click **Designated NAT Interfaces**.

The following dialogue box will appear:



NAT Interface Setting

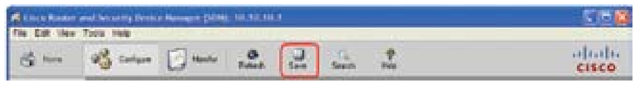
Select the list of interfaces that you want to designate as inside / outside.

interface	inside(trusted)	outside(untruste
FastEthernet0	□	☑
Vlan1	☑	□

5. Select appropriate boxes for **trusted** and **untrusted** interfaces – as shown above.

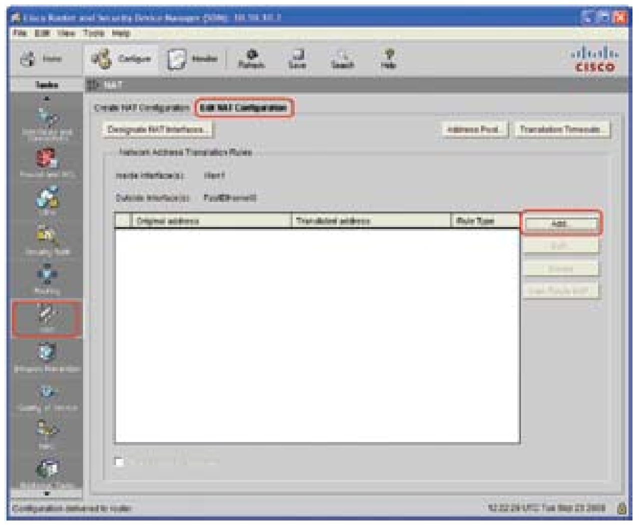
Please note: The above WAN interface is provided as an example for Ethernet set up (ie **FastEthernet0**), for ADSL customers please use **dialler0**.

6. Click **OK**.



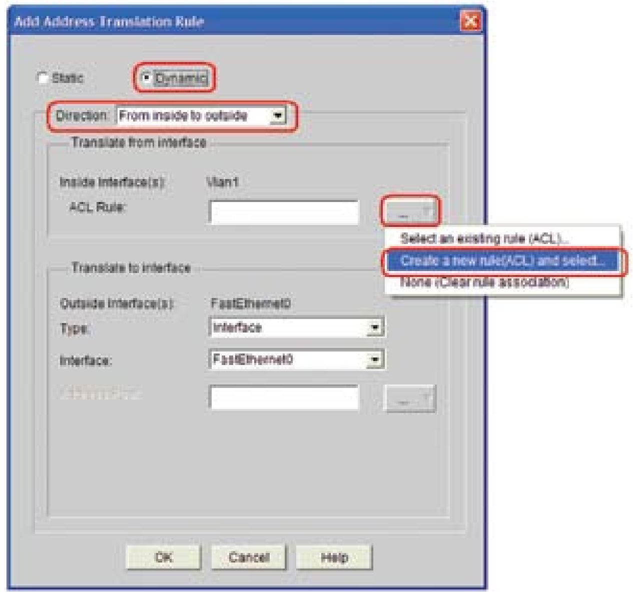
7. Click **Save**.

2. Dynamic Port Address Translation



STEPS:

1. Click **Configure** – as shown above.
2. Click **NAT** from the **Tasks** section.
3. Select **Edit NAT Configuration** tab.
4. Click **Add**.



Add Address Translation Rule

○ Static ● Dynamic

Direction: From inside to outside

Translate from interface

Inside Interface(s): Vlan1

ACL Rule:

Select an existing rule (ACL)...
Create a new rule(ACL) and select...
None (Clear rule association)

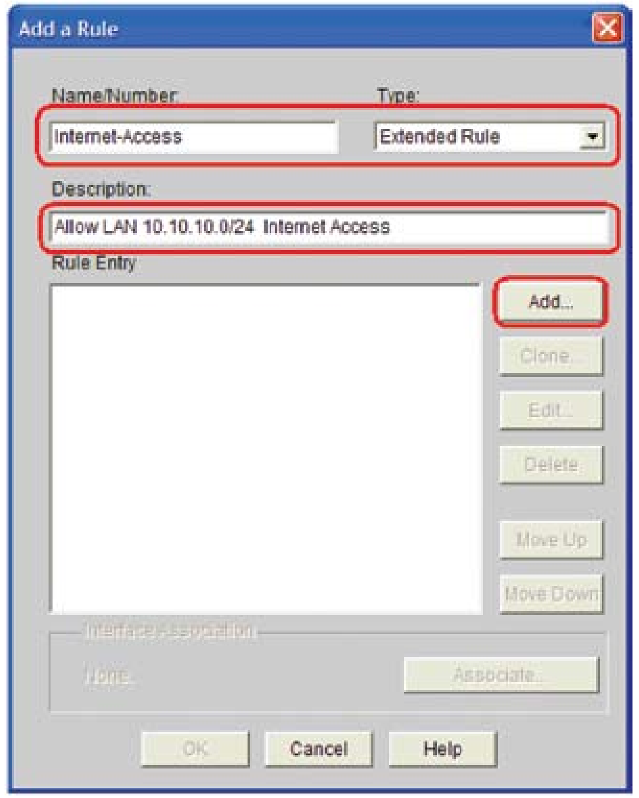
Translate to interface

Outside Interface(s): FastEthernet0

Type: Interface

Interface: FastEthernet0

5. Select **Dynamic**.
6. In the **Direction** drop down menu: select **From Inside to outside**.
7. Click pull down menu and select **Create a new rule (ACL) and select...**



Add a Rule

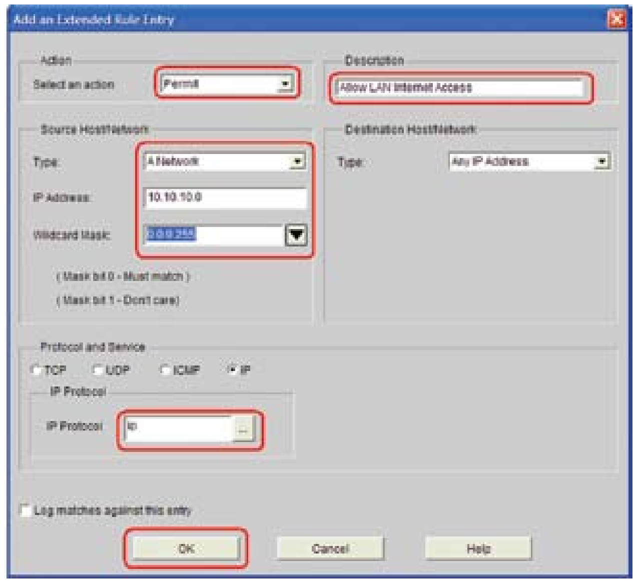
Name/Number: Internet-Access

Type: Extended Rule

Description: Allow LAN 10.10.10.0/24 Internet Access

Rule Entry

8. Fill in Name, Type and **Description** as appropriate.
9. Click **Add**



Add an Extended Rule Entry

Action

Select an action: Permit

Description: Allow LAN Internet Access

Source Host/Network

Type: A Network

IP Address: 10.10.10.0

Wildcard Mask: 0.0.0.255

(Mask bit 0 - Must match)

(Mask bit 1 - Don't care)

Destination Host/Network

Type: Any IP Address

Protocol and Service

○ TCP ○ UDP ○ ICMP ● IP

IP Protocol

IP Protocol: ip

□ Log matches against this entry

Complete the following fields:

10. Action.

11. Description (optional).

12. Source Host/Network source.

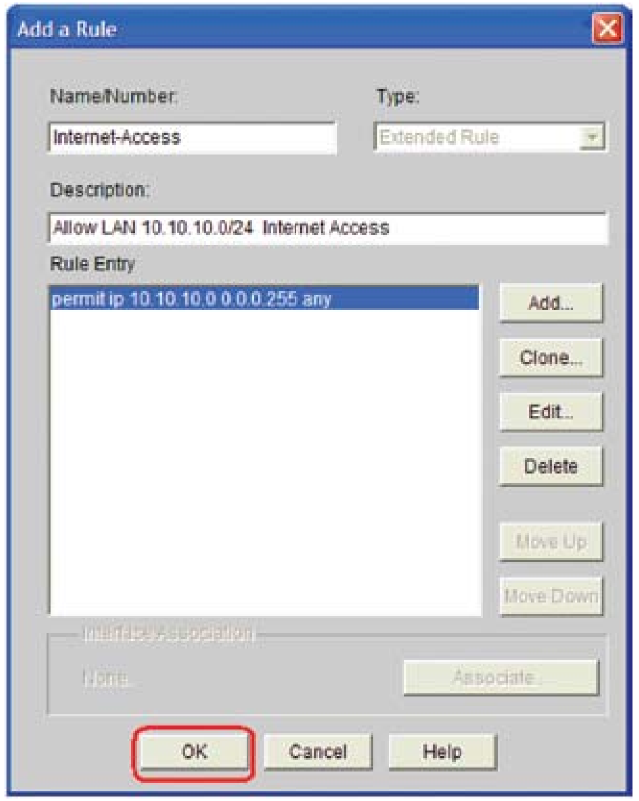
13. Protocol and Service.

14. Select **IP** in the **IP Protocol**.

15. Click **OK**.

Please note: The source should be the trusted network.

The following screen will be provided:



Add a Rule

Name/Number: Internet-Access

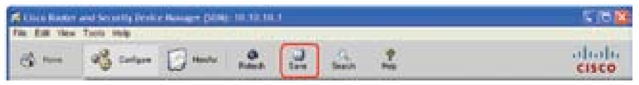
Type: Extended Rule

Description: Allow LAN 10.10.10.0/24 Internet Access

Rule Entry

permit ip 10.10.10.0 0.0.0.255 any

16. Click **OK**.

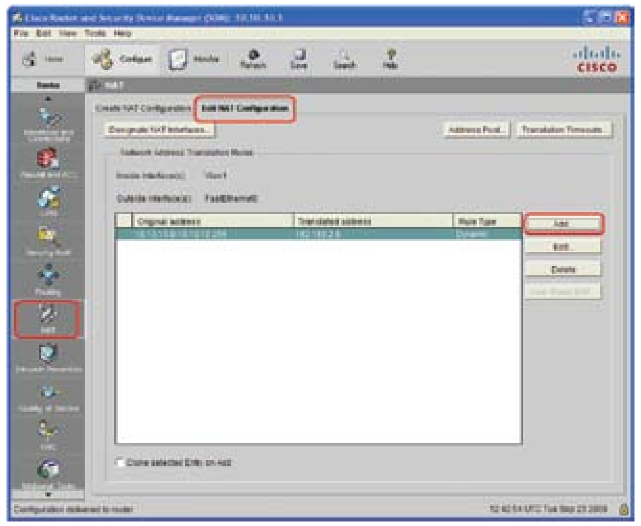


17. Click on **Save**.

D. Static Port Address Translation (Static PAT)

Static port address translation is required if the customer has a web server located within their LAN which they would like to give internet users access to. This assumes the customer has appropriate security measures on the server before configuring this feature, if you are unsure please consult your IT specialist or contact your Account Representative for more information on our IT Services solutions.

The following screens show how to configure PAT for web (port 80)



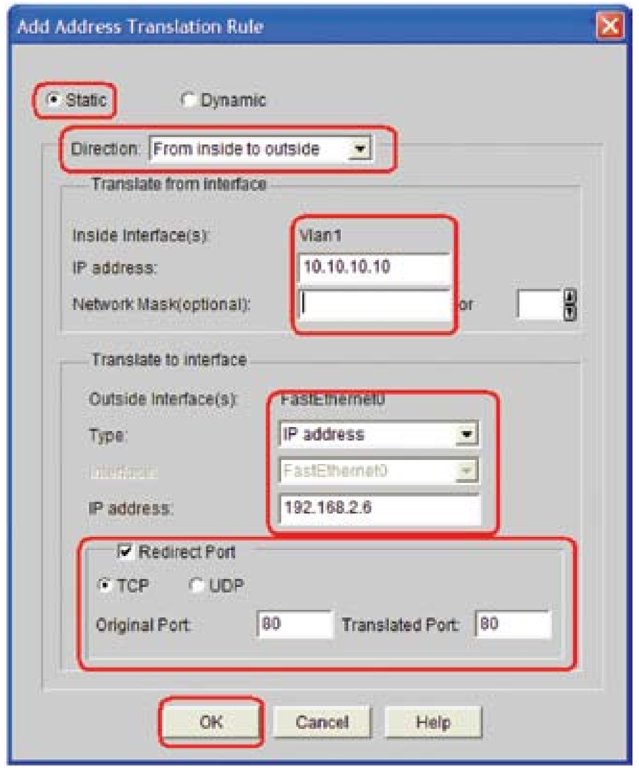
STEPS:

1. Click **Configure** – as shown above.

2. Click **NAT** from the **Tasks** section.

3. Select **Edit NAT Configuration** tab.

4. Click **Add**.



Add Address Translation Rule

● Static ○ Dynamic

Direction: From inside to outside

Translate from interface

Inside Interface(s): Vlan1

IP address: 10.10.10.10

Network Mask(optional): or

Translate to interface

Outside Interface(s): FastEthernet0

Type: IP address

Interface: FastEthernet0

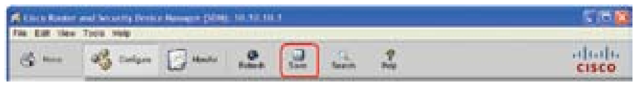
IP address: 192.168.2.6

☑ Redirect Port

● TCP ○ UDP

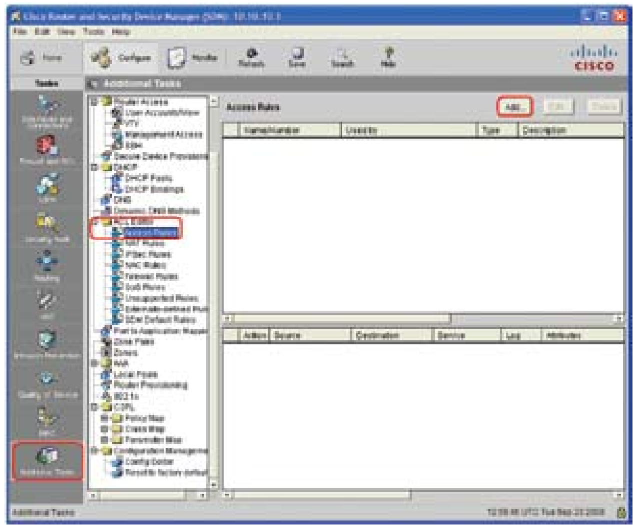
Original Port: 80 Translated Port: 80

5. Select **Static** – as shown above.
6. In the **Direction** drop down menu – select **From inside to outside**.
7. In the **Translate from Interface** enter the **IP address** and subnet mask of the Web sever on the LAN.
8. In **Translate to interface**, enter the public IP address in the **IP address** field.
9. Ensure that the **Redirect Port** is selected.
10. Select **TCP**.
11. **Original Port** and **Translated Port** are set to **80**.
12. Click **OK**.



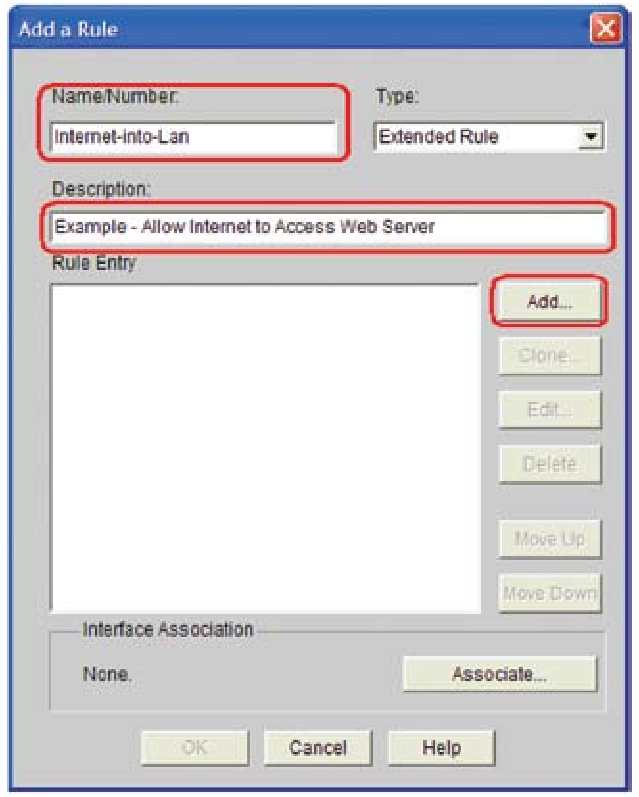
13. Click **Save**.

E. Creating Access Control List



STEPS:

1. Click **Configure** – as shown above.
2. Click **Additional Tasks** from the **Tasks** section.
3. Select **Edit NAT Configuration** tab.
4. Click **Add**.



Add a Rule

Name/Number: Internet-into-Lan

Type: Extended Rule

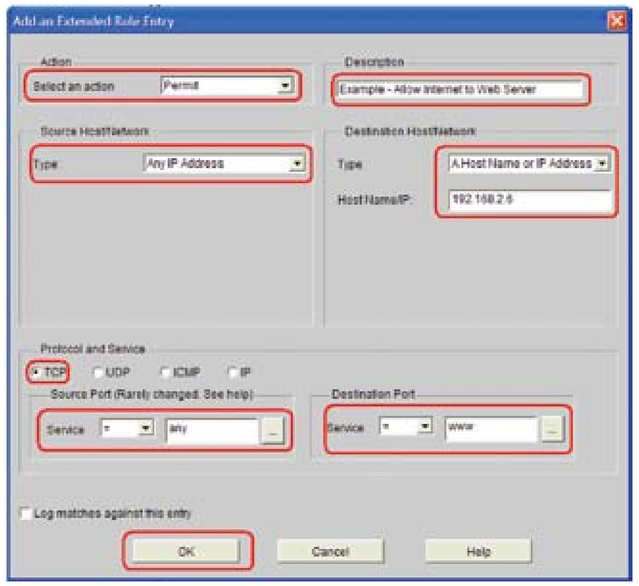
Description: Example - Allow Internet to Access Web Server

Rule Entry

Interface Association

None.

5. Complete the fields **Name/Number** and **Description**.
6. Click **Add**.



Add an Extended Rule Entry

Action

Select an action: Permit

Description

Example - Allow Internet to Web Server

Source Host/Network

Type: Any IP Address

Destination Host/Network

Type: A Host Name or IP Address

Host Name/IP: 192.168.2.6

Protocol and Service

● TCP ○ UDP ○ ICMP ○ IP

Source Port (Rarely changed. See help)

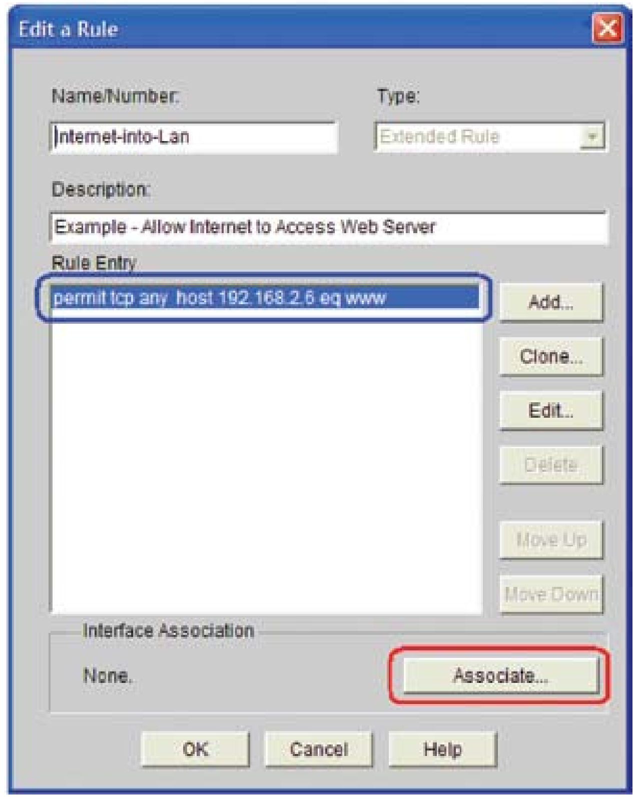
Service: = any

Destination Port

Service: = www

□ Log matches against this entry

7. The above examples shows any user (source) allowed to access the public address of the web server. Access has been restricted to port 80 only.
8. Once you have added the rule, click **OK**.



Edit a Rule

Name/Number: Internet-into-Lan

Type: Extended Rule

Description: Example - Allow Internet to Access Web Server

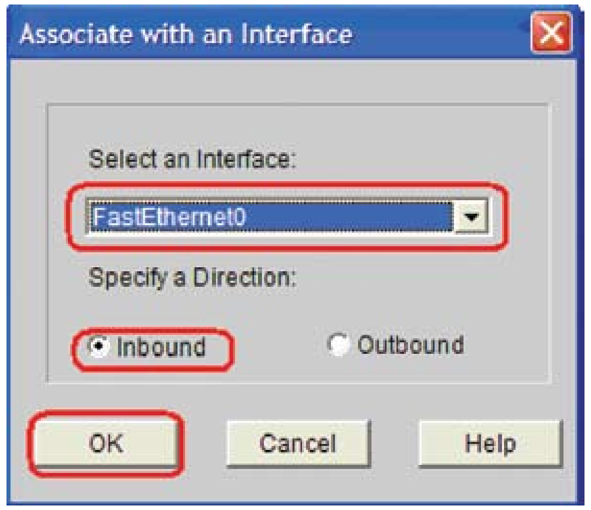
Rule Entry

permit tcp any host 192.168.2.6 eq www

Interface Association

None.

9. The above will be shown to verify the rule which was configured.
10. To apply the rule, click **Associate**.



Associate with an Interface

Select an Interface: FastEthernet0

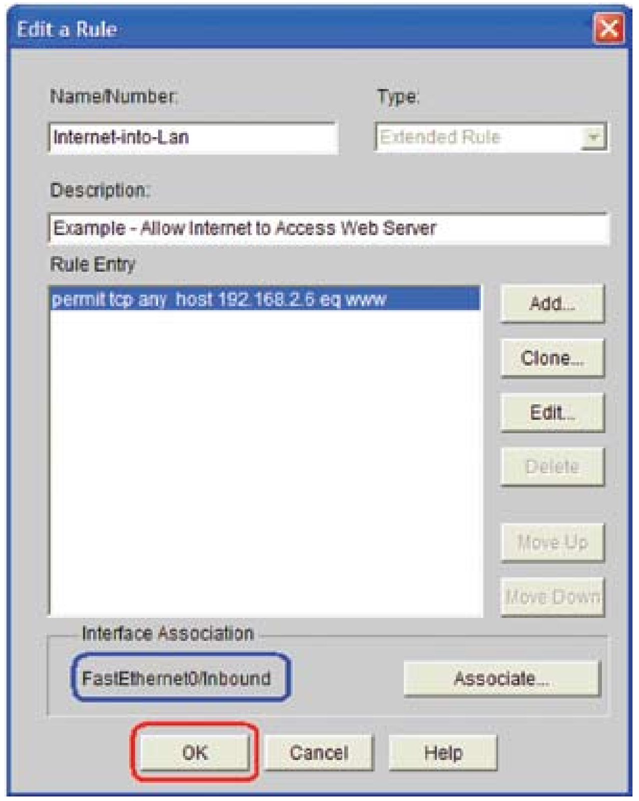
Specify a Direction:

● Inbound ○ Outbound

11. As the example allows internet users to access a web server in the LAN, select an Interface (example **FastEthernet0**) and specify **Inbound** direction.

Please note: This is provided as an example only – for Ethernet set up use ie **FastEthernet** and ADSL set up please use ie **dialler0**.

12. Click **OK**.


Edit a Rule

Name/Number: Internet-into-Lan

Type: Extended Rule

Description: Example - Allow Internet to Access Web Server

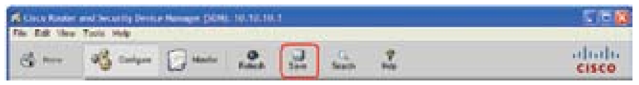
Rule Entry: permit tcp any host 192.168.2.6 eq www

Interface Association: FastEthernet0/Inbound

13. You will be provided with this screen, which will confirm the interface association and direction.

Please note: The the WAN interface is provided as an example for Ethernet set up (ie **FastEthernet**), for ADSL customers this should indicate **dialler0**.

14. Click **OK** to finish.

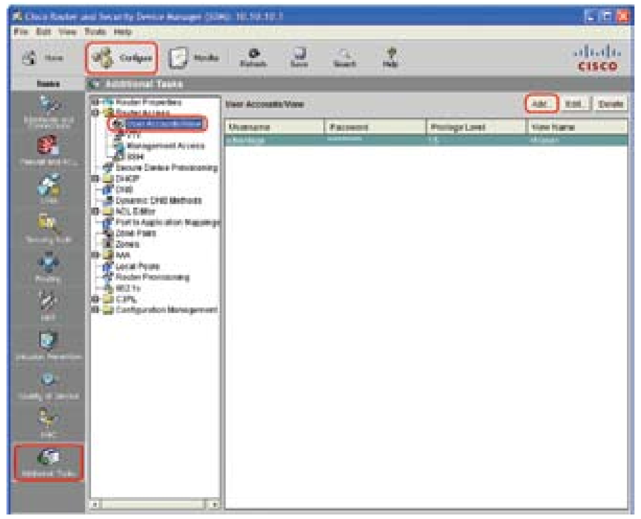


15. Click **Save**.

F. Adding/modifying/Removing Username and Password

1. Adding UserNAME and Password

The following instructions show how to add new users with passwords.



STEPS:

1. Click **Configure** as shown above.

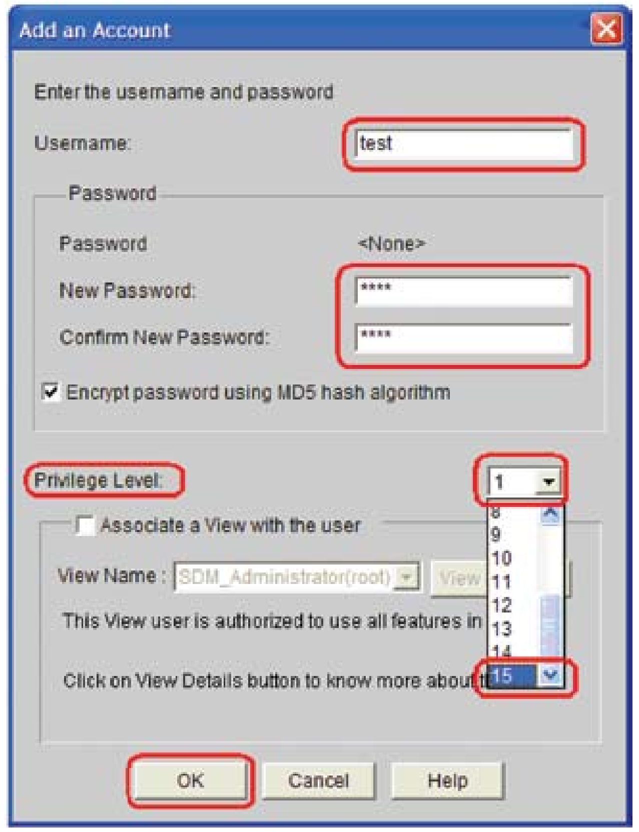
2. Click **Additional Tasks** in the **Tasks** section.

3. Click **Router Access**.

4. Click **User Accounts/view**.

5. Click **Add** or click **Edit** if you wish to modify username and/or password.

You will be provided with the following screen:


Add an Account

Enter the username and password

Username: test

Password

Password <None>

New Password: ****

Confirm New Password: ****

☑ Encrypt password using MD5 hash algorithm

Privilege Level: 1

□ Associate a View with the user

View Name : SDM_Administrator(root)

This View user is authorized to use all features in

Click on View Details button to know more about t

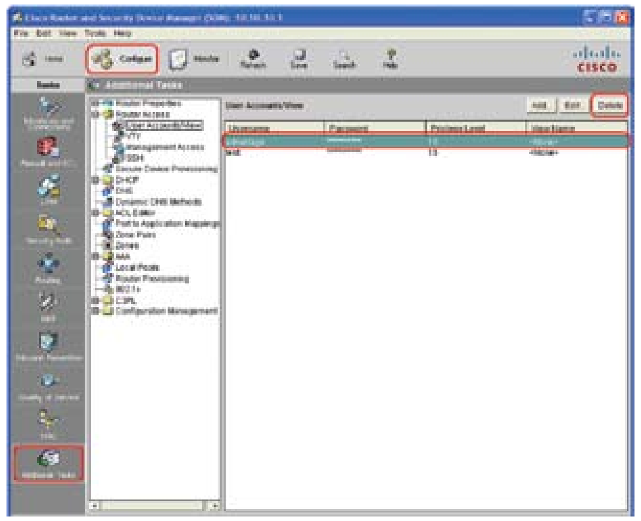
6. Fill in the **Username**, **New Password** and **Confirm New Password** fields.

7. For **Privilege Level**, only administrators should be marked with **15** and all other users should be marked with **1**

8. Click **OK**.

9. Click **File** and **Write** (File toolbar) to start up Configure **– THIS IS VERY IMPORTANT AND IS REQUIRED TO SAVE THE CHANGES INTO THE ROUTER IN CASE OF A POWER FAILURE/POWER CYCLE.**

2. Removing Telstra Administrator Account



STEPS:

1. Click **Configure** as shown above.

2. Click **Additional Tasks** in the **Tasks** section.

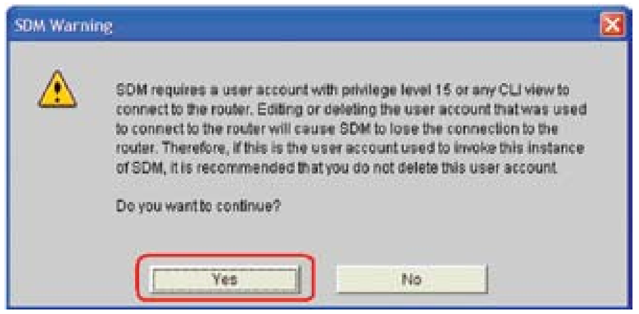
3. Click **User Account/View**.

4. Click and highlight **advantage** or the administrator username.

5. Click **Delete**.

Please note:

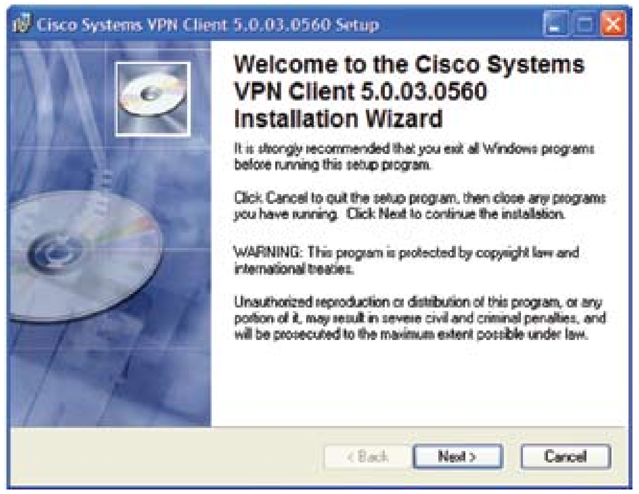
The following prompt – **SDM Warning** will be shown, this will warn the administrator. Before this default account is deleted, make sure a NEW Username and Password with **Privilege Level 15** has been configured.


SDM Warning

SDM requires a user account with privilege level 15 or any CLI view to connect to the router. Editing or deleting the user account that was used to connect to the router will cause SDM to lose the connection to the router. Therefore, if this is the user account used to invoke this instance of SDM, it is recommended that you do not delete this user account.

Do you want to continue?

6. Click **Yes** to initiate the Administrator Account deletion.



Welcome to the Cisco Systems VPN Client 5.0.03.0560 Installation Wizard

It is strongly recommended that you exit all Windows programs before running this setup program.

Click Cancel to quit the setup program, then close any programs you have running. Click Next to continue the installation.

WARNING: This program is protected by copyright law and international treaties.

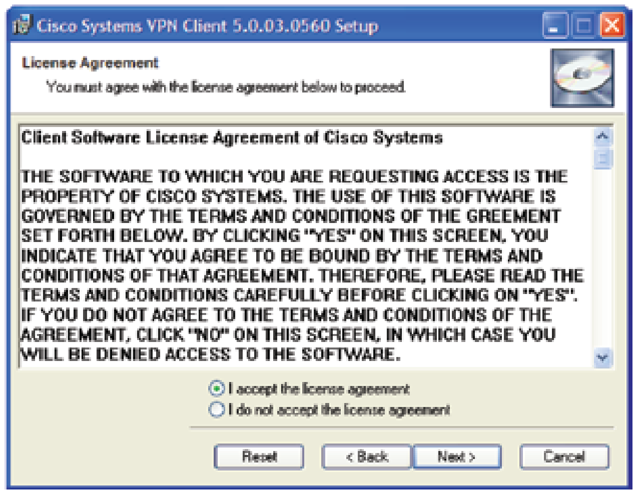
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

STEPS:

1. Download the Cisco VPN client to the PC (This feature/client is only available to customers who have purchased our Router Support Service Extra).

2. Extract the Cisco Client zip file. Go to Cisco VPN Client installer folder and click **setup.exe**. The installation wizard will start as shown above.

3. Click **Next**.



License Agreement

You must agree with the license agreement below to proceed.

Client Software License Agreement of Cisco Systems

THE SOFTWARE TO WHICH YOU ARE REQUESTING ACCESS IS THE PROPERTY OF CISCO SYSTEMS. THE USE OF THIS SOFTWARE IS GOVERNED BY THE TERMS AND CONDITIONS OF THE GREEMENT SET FORTH BELOW. BY CLICKING "YES" ON THIS SCREEN, YOU INDICATE THAT YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS OF THAT AGREEMENT. THEREFORE, PLEASE READ THE TERMS AND CONDITIONS CAREFULLY BEFORE CLICKING ON "YES". IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THE AGREEMENT, CLICK "NO" ON THIS SCREEN, IN WHICH CASE YOU WILL BE DENIED ACCESS TO THE SOFTWARE.

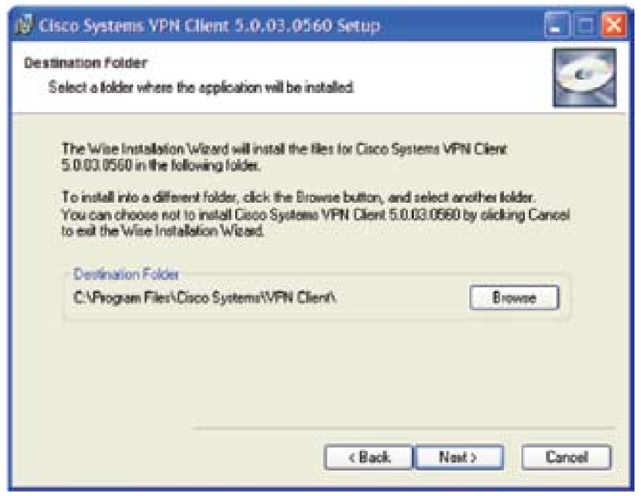
● I accept the license agreement

○ I do not accept the license agreement

4. A **License Agreement** will appear.

5. Select **I accept the license agreement**.

6. Click **Next**.



Destination Folder

Select a folder where the application will be installed.

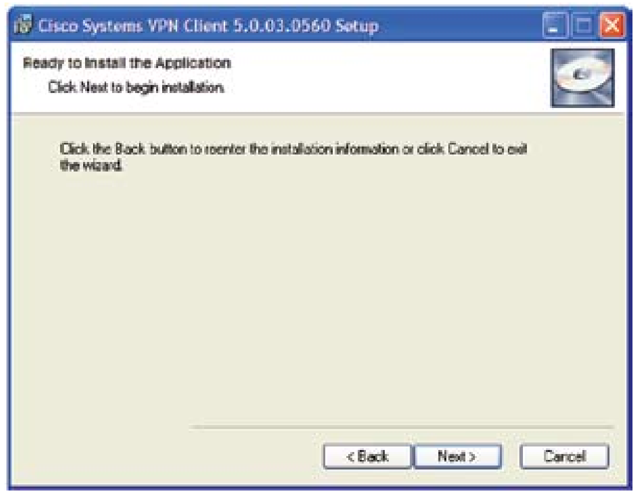
The Wise Installation Wizard will install the files for Cisco Systems VPN Client 5.0.03.0560 in the following folder.

To install into a different folder, click the Browse button, and select another folder. You can choose not to install Cisco Systems VPN Client 5.0.03.0560 by clicking Cancel to exit the Wise Installation Wizard.

Destination Folder

C:\Program Files\Cisco Systems\VPN Client\

7. Accept default destination folder and click **Next**.

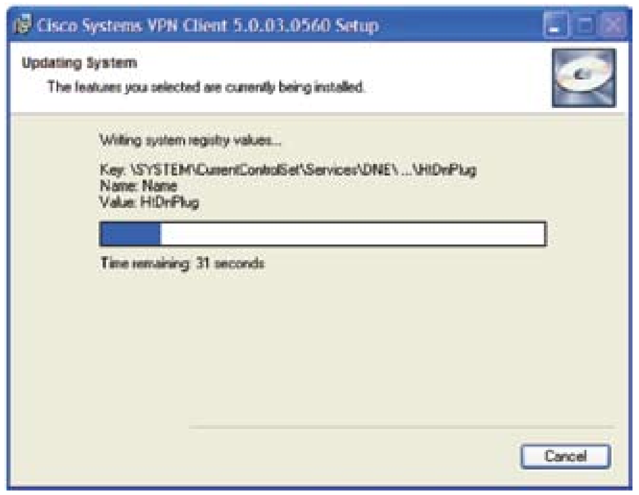


Ready to Install the Application

Click Next to begin installation.

Click the Back button to reenter the installation information or click Cancel to exit the wizard.

8. Click **Next**.



Updating System

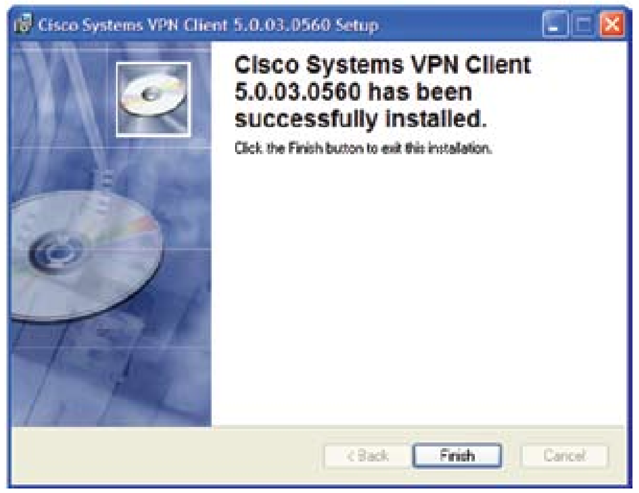
The features you selected are currently being installed.

Writing system registry values...

Key: \SYSTEM\CurrentControlSet\Services\DNE\ ...\HIDnPlug
Name: Name
Value: HIDnPlug

Time remaining: 31 seconds

9. The installation will start as shown above.



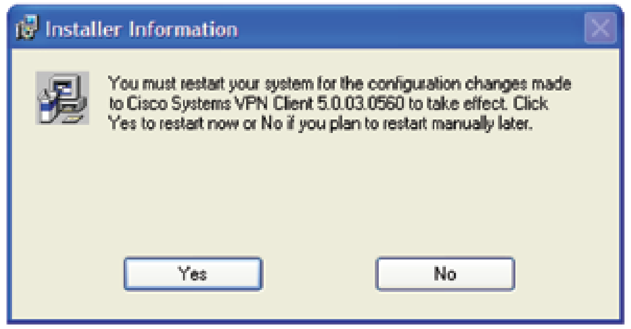
Cisco Systems VPN Client 5.0.03.0560 has been successfully installed.

Click the Finish button to exit this installation.

Cisco VPN install successful:

10. Click **Finish** when the installation is complete.

You will be prompted to reboot your computer for installation to take effect:



You must restart your system for the configuration changes made to Cisco Systems VPN Client 5.0.03.0560 to take effect. Click Yes to restart now or No if you plan to restart manually later.

11. To reboot computer, click **Yes**.

A. Wireless

Wired Equivalent Privacy (WEP) and WiFi Protected Access (WPA) are the two security protocol options available for encrypting wireless communications on the router.

We recommend customers use WPA – the stronger of the two encryption methods.

WPA is the second generation wireless encryption protocol and designed to overcome the security flaws that were evident in WEP. WPA is available in WPA2 (Enterprise) and WPA-PSK (Personal).

We recommend you use WPA as your method for Wireless Encryption.

WPA-PSK is easier to setup than WPA2 (enterprise) since it uses a pre-shared key, compared to certificates in an enterprise environment. The minimum length is 8 characters; with maximum 63 characters, we recommend a minimum length of 20 characters. Values can be alpha-numeric.

To use either WEP or WPA both the wireless devices and the operating system must be able to support it.

Please note: Some older operating systems may not support WPA and will require WEP. It is not possible to mix WPA and WEP.

If one device on the network is limited to WEP, then either that device needs to be replaced or the entire network is to be limited to using WEP.

B. Remote Access

The routers support various remote access applications, such as SDM, telnet, and SSH to allow remote management.

SDM can either use http or https. However, the SDM software needs to be installed on the PC.

Telnet and SSH are network protocols which allow remote interactive TCP sessions to the router. Telnet is less secure since the TCP session is all in clear text while SSH is more secure, it uses encryption to protect the data between the client and the router.

C. Remote Access VPN (IPSec VPN)

Remote Access VPN allows mobile workers (Tele-workers) to securely access the corporate network from anywhere in the world.

To securely access the corporate network, the router needs to be setup to accept and terminate the IPSec VPN tunnel and the Cisco VPN client software needs to be installed on the PC to initiate the request.

When the IPSec tunnel is established, it offers the user comprehensive security by encrypting the data between the client PC and the router.

Important note:

This feature is available through Telstra if you have purchased the Telstra Business Broadband Extras 'Router Support Service (RSS)'. For more information on this Telstra Business Broadband Extras, please contact your Telstra Account Representative or call **1800 655 744**.

D. Dynamic Host Control Protocol (DHCP)

The DHCP protocol allows a server to dynamically assign IP addresses and DNS addresses to the PC TCP/IP software stack. The IP addresses are assigned from an arbitrary IP address pool.

E. Integrated Firewall

In its simplest form, a firewall prevents unauthorized access from an untrusted source to a trusted network. The Zone Base Firewall (ZBF) feature is a sophisticated form of firewall introduced in Cisco IOS version 12.4(6)T which provides stateful inspection.

Stateful inspection offers better security by keeping track of the packets traversing the router by "inspecting" the packet up to the application layer information. This allows the router to distinguish legitimate packets for different types of connections.

F. Network Address Translation (NAT)/Port Address Translation (PAT)

The concept of NAT and PAT allows internal devices with unregistered (private) address to access the internet by having the router re-write and replace the internal address with an internet (public) valid IP Address.

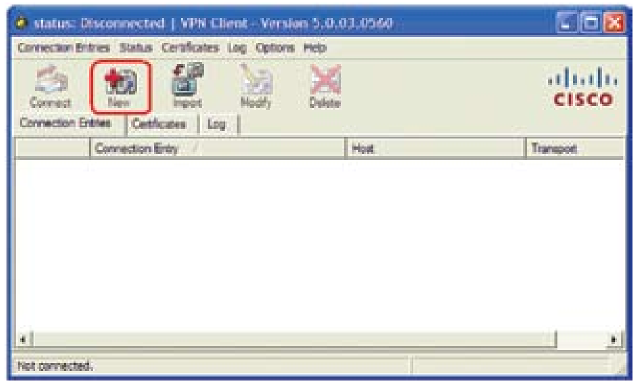
NAT allows the router to allocate one public IP address to one internal private IP address while PAT allows the router to share one public IP address amongst many internal private IP addressed devices.

It should be noted that some protocols may break when used in conjunction with NAT/PAT since some protocols may have embedded IP addresses in the payload itself.

It is assumed the customer will only encounter standard well known protocols.

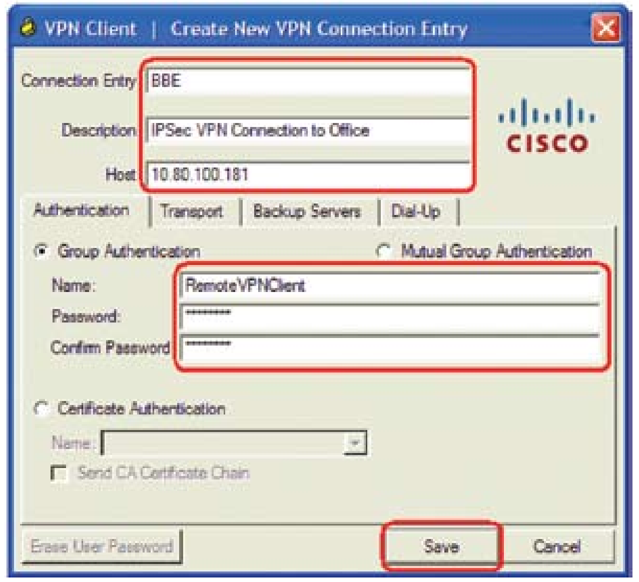
A. Cisco VPN Client Configuration

This feature is available through Telstra if you have purchased the Telstra Business Broadband Extras 'Router Support Service (RSS)'. For more information on this Telstra Business Broadband Extras, please contact your Telstra Account Representative or call **1800 655 744**.


status: Disconnected | VPN Client - Version 5.0.03.0560
Connection Entries Status Certificates Log Options Help
Connect
New
Import
Modify
Delete
CISCO
Connection Entries
Certificates
Log
Connection Entry
Host
Transport
Not connected.

STEPS:

1. Start the Cisco VPN Client.
2. Click **New**.



Connection Entry: BBE

Description: IPSec VPN Connection to Office

Host: 10.80.100.181

● Group Authentication ○ Mutual Group Authentication

Name: RemoteVPNClient

Password: ********

Confirm Password: ********

○ Certificate Authentication

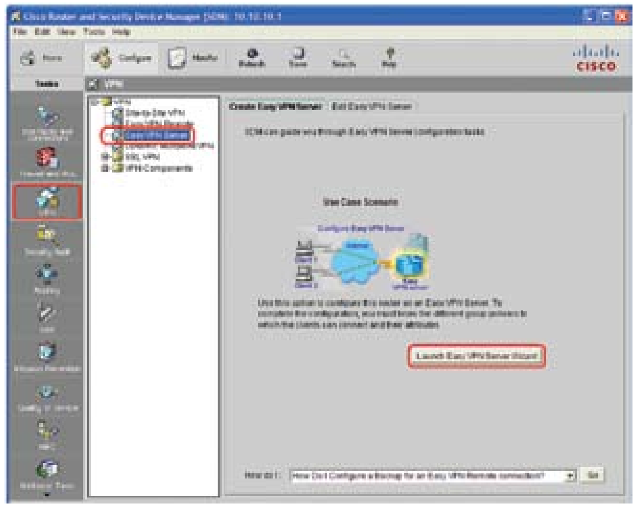
Name:

□ Send CA Certificate Chain

3. **Connection Entry** – is the name of this particular profile.
4. **Description** – a meaningful description of the profile.
5. **Host** – the public IP address of the router.
6. **Group Authentication:**
   - **Name** – user defined, this group name MUST be the same as the one defined in section 11(B) step 18.
   - **Password** – user defined.

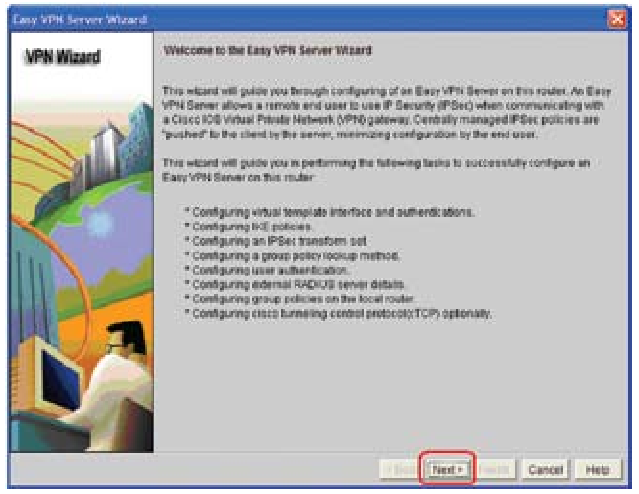
B. Configuring an IPSec VPN on the Router

This section shows how to configure the router to act as an IPSec VPN termination point to allow remote users who have installed Cisco VPN Client on their personal computer, to securely connect to the corporate local area network. This feature is available through Telstra if you have purchased the Telstra Business Broadband Extras 'Router Support Service (RSS)'. For more information on this Telstra Business Broadband Extras, please contact your Telstra Account Representative or call **1800 655 744**.



STEPS:

1. Click **Configure**.
2. Click **VPN** in the **Tasks** section.
3. Click **Easy VPN Server**.
4. Click **Launch Easy VPN Server Wizard**.



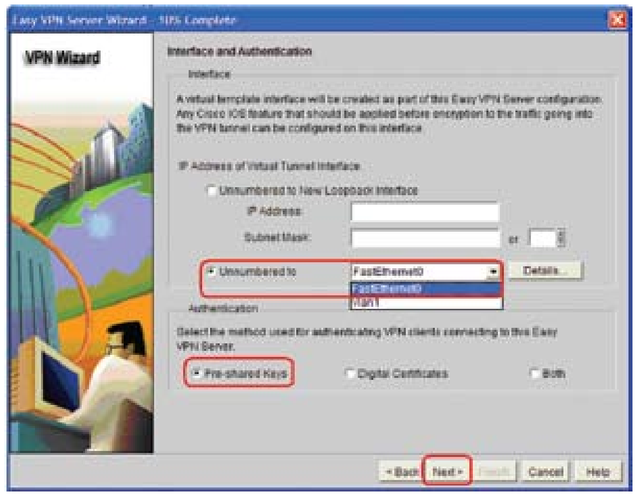
Welcome to the Easy VPN Server Wizard

This wizard will guide you through configuring of an Easy VPN Server on this router. An Easy VPN Server allows a remote end user to use IP Security (IPSec) when communicating with a Cisco IOS Virtual Private Network (VPN) gateway. Centrally managed IPSec policies are "pushed" to the client by the server, minimizing configuration by the end user.

This wizard will guide you in performing the following tasks to successfully configure an Easy VPN Server on this router:

* Configuring virtual template interface and authentications.
* Configuring IKE policies.
* Configuring an IPSec transform set.
* Configuring a group policy lookup method.
* Configuring user authentication.
* Configuring external RADIUS server details.
* Configuring group policies on the local router.
* Configuring cisco tunneling control protocol(cTCP) optionally.

5. Click **Next**.



Interface and Authentication

Interface

A virtual template interface will be created as part of this Easy VPN Server configuration. Any Cisco IOS feature that should be applied before encryption to the traffic going into the VPN tunnel can be configured on this interface.

IP Address of Virtual Tunnel Interface

○ Unnumbered to New Loopback Interface

IP Address:

Subnet Mask: or

● Unnumbered to FastEthernet0

FastEthernet0
Vlan1

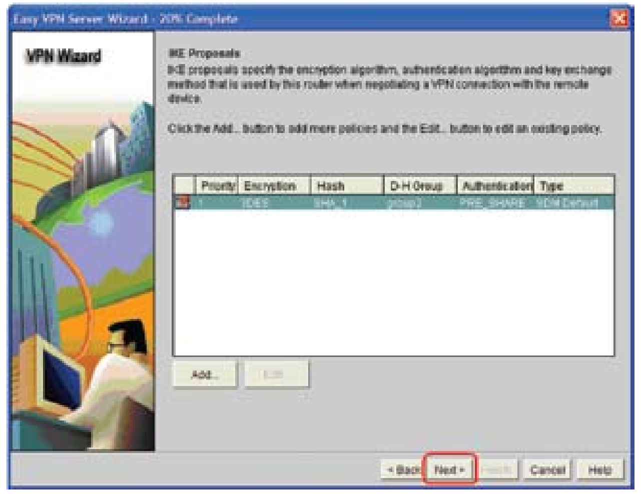
Authentication

Select the method used for authenticating VPN clients connecting to this Easy VPN Server.

● Pre-shared Keys ○ Digital Certificates ○ Both

6. Click **Unnumbered to**.
7. Click the drop down menu and choose the interface which faces the internet.
8. For **Authentication**, select **Pre-shared Keys**.
9. Click **Next**.

You will be provided with the following screen.



Easy VPN Server Wizard - 20% Complete

VPN Wizard

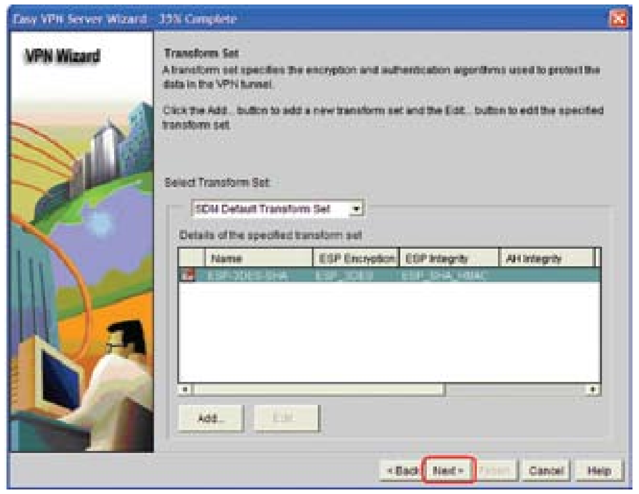
IKE Proposals

IKE proposals specify the encryption algorithm, authentication algorithm and key exchange method that is used by this router when negotiating a VPN connection with the remote device.

Click the Add... button to add more policies and the Edit... button to edit an existing policy.

	Priority	Encryption	Hash	D-H Group	Authentication	Type
	1	3DES	SHA_1	group2	PRE_SHARE	SDM Default

10. Click **Next**.



Easy VPN Server Wizard - 35% Complete

VPN Wizard

Transform Set

A transform set specifies the encryption and authentication algorithms used to protect the data in the VPN tunnel.

Click the Add... button to add a new transform set and the Edit... button to edit the specified transform set.

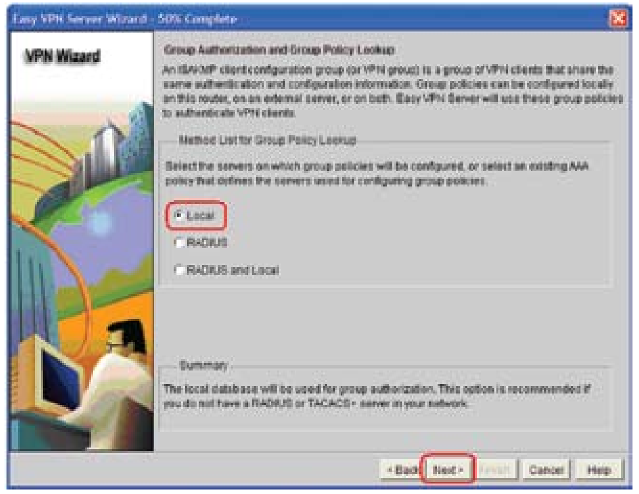
Select Transform Set:

SDM Default Transform Set

Details of the specified transform set

	Name	ESP Encryption	ESP Integrity	AH Integrity
	ESP-3DES-SHA	ESP_3DES	ESP_SHA_HMAC	

11. Click **Next**.



Easy VPN Server Wizard - 50% Complete

VPN Wizard

Group Authorization and Group Policy Lookup

An ISAKMP client configuration group (or VPN group) is a group of VPN clients that share the same authentication and configuration information. Group policies can be configured locally on this router, on an external server, or on both. Easy VPN Server will use these group policies to authenticate VPN clients.

Method List for Group Policy Lookup

Select the servers on which group policies will be configured, or select an existing AAA policy that defines the servers used for configuring group policies.

● Local

○ RADIUS

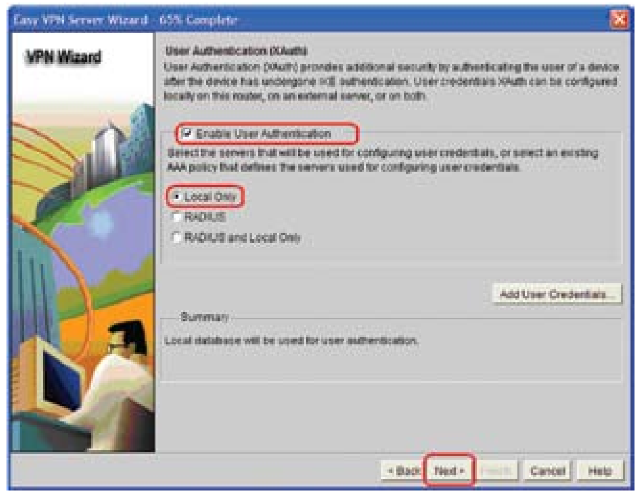
○ RADIUS and Local

Summary

The local database will be used for group authorization. This option is recommended if you do not have a RADIUS or TACACS+ server in your network.

12. Select **Local**.

13. Click **Next**.



Easy VPN Server Wizard - 65% Complete

VPN Wizard

User Authentication (XAuth)

User Authentication (XAuth) provides additional security by authenticating the user of a device after the device has undergone IKE authentication. User credentials XAuth can be configured locally on this router, on an external server, or on both.

☑ Enable User Authentication

Select the servers that will be used for configuring user credentials, or select an existing AAA policy that defines the servers used for configuring user credentials.

● Local Only

○ RADIUS

○ RADIUS and Local Only

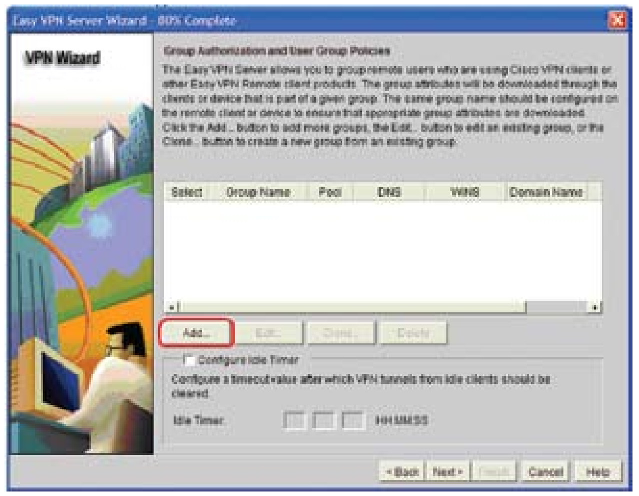
Summary

Local database will be used for user authentication.

14. Select **Enable User Authentication**.

15. Select **Local Only**.

16. Click **Next**.



Easy VPN Server Wizard - 80% Complete

VPN Wizard

Group Authorization and User Group Policies

The Easy VPN Server allows you to group remote users who are using Cisco VPN clients or other Easy VPN Remote client products. The group attributes will be downloaded through the clients or device that is part of a given group. The same group name should be configured on the remote client or device to ensure that appropriate group attributes are downloaded. Click the Add... button to add more groups, the Edit... button to edit an existing group, or the Clone... button to create a new group from an existing group.

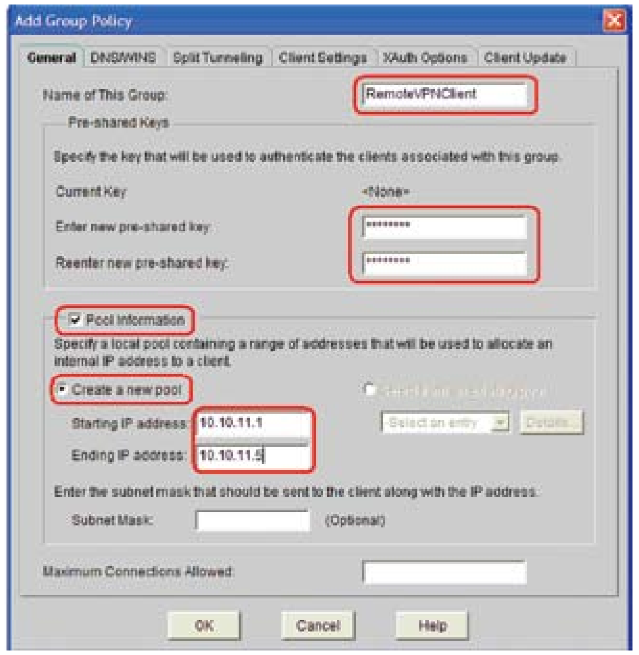
Select	Group Name	Pool	DNS	WINS	Domain Name

☐ Configure Idle Timer

Configure a timeout value after which VPN tunnels from idle clients should be cleared.

Idle Timer: HH:MM:SS

17. Click **Add**.



Add Group Policy

Name of This Group: RemoteVPNClient

Pre-shared Keys

Specify the key that will be used to authenticate the clients associated with this group.

Current Key: <None>

Enter new pre-shared key: *********

Reenter new pre-shared key: *********

☑ Pool Information

Specify a local pool containing a range of addresses that will be used to allocate an internal IP address to a client.

● Create a new pool ○ Select an existing pool

Starting IP address: 10.10.11.1

Ending IP address: 10.10.11.5

Select an entry

Enter the subnet mask that should be sent to the client along with the IP address.

Subnet Mask: (Optional)

Maximum Connections Allowed:

18. Name of This Group – define remote access policies that are common to all specific users. This group name must match the name in Section 11(A) step 6.

19. Pre-shared Keys – password for device authentication.

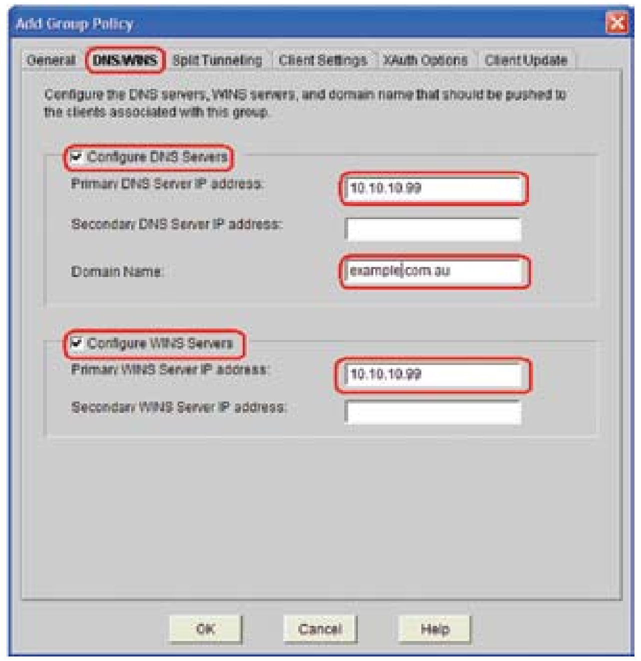
20. Pool Information – range of IP addresses that can be allocated to IPSec VPN Clients. This address MUST be unique.

21. Click **OK**.

C. Other IPSec VPN settings

1. DNS/WINS

The DNS/WINS configuration page allows customers who have internal servers within the corporate network which need to be assigned to the IPSec VPN user so they can resolve private host or device names.



Add Group Policy

Configure the DNS servers, WINS servers, and domain name that should be pushed to the clients associated with this group.

☑ Configure DNS Servers

Primary DNS Server IP address: 10.10.10.99

Secondary DNS Server IP address:

Domain Name: example.com.au

☑ Configure WINS Servers

Primary WINS Server IP address: 10.10.10.99

Secondary WINS Server IP address:

STEPS:

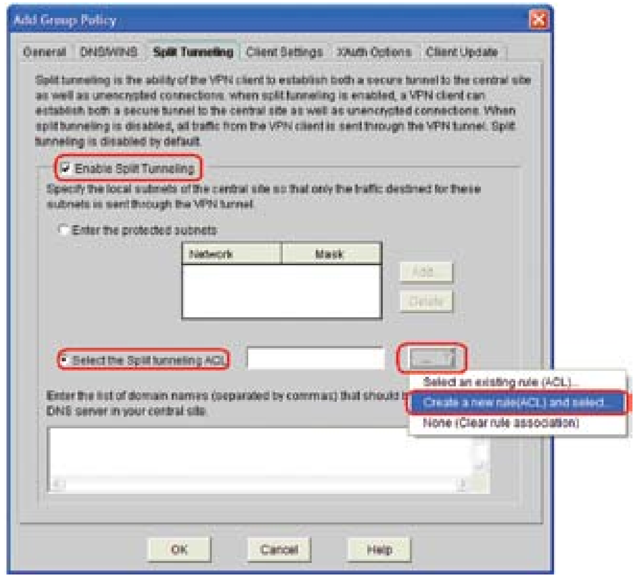
1. Click **DNS/WINS** tab.
2. Select **Configure DNS Servers** and fill in the required fields.
3. Check **Configure WINS Servers** and fill in the required fields.

2. Split Tunneling

Split tunneling allows administrators to configure the router to allow remote users (Cisco VPN Clients) to have secure access to the company network while at the same time allowing unsecure access to the internet.

Split tunneling can pose a security risk when configured. Since VPN Clients have unsecured access to the internet, they can be compromised by an attacker. That attacker is then able to access the corporate LAN via the IPsec tunnel.

It is advised administrators do not enable split tunneling.



Add Group Policy

Split tunneling is the ability of the VPN client to establish both a secure tunnel to the central site as well as unencrypted connections. when split tunneling is enabled, a VPN client can establish both a secure tunnel to the central site as well as unencrypted connections. When split tunneling is disabled, all traffic from the VPN client is sent through the VPN tunnel. Split tunneling is disabled by default.

☑ Enable Split Tunneling

Specify the local subnets of the central site so that only the traffic destined for these subnets is sent through the VPN tunnel.

○ Enter the protected subnets

● Select the Split tunneling ACL

Select an existing rule (ACL)...

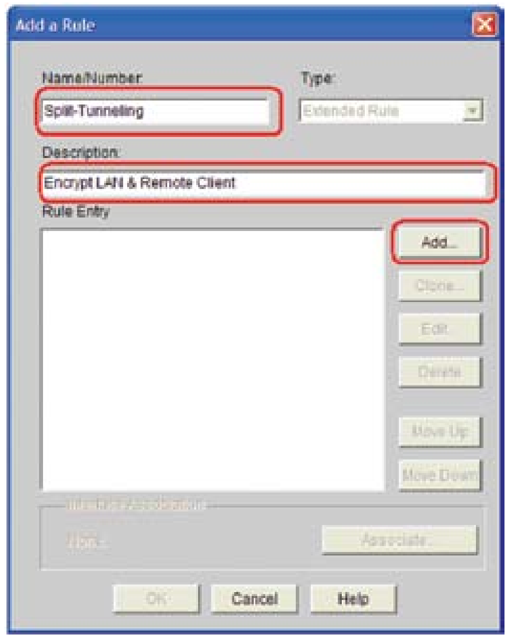
Create a new rule(ACL) and select...

None (Clear rule association)

Enter the list of domain names (separated by commas) that should be resolved by the DNS server in your central site.

STEPS:

1. Click **Split tunneling** tab – as shown above.
2. Select **Enable Split Tunneling**.
3. Select **Select the Split tunneling ACL**.
4. Click **Create a new rule (ACL) and select...**



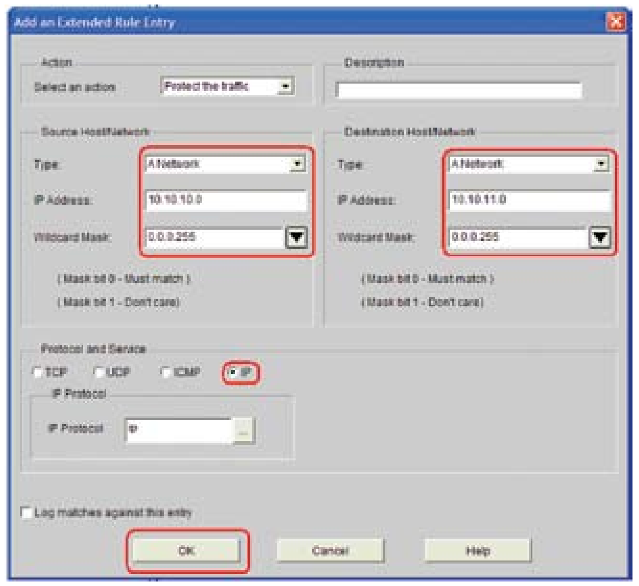
Add a Rule

Name/Number: Split-Tunneling

Type: Extended Rule

Description: Encrypt LAN & Remote Client

5. **Name/Number** – provide a meaningful name of the ACL (no spaces).
6. **Description** – provide a meaningful description.
7. Click **Add**.



Add an Extended Rule Entry

Select an action: Protect the traffic

Source Host/Network — Type: A Network; IP Address: 10.10.10.0; Wildcard Mask: 0.0.0.255

Destination Host/Network — Type: A Network; IP Address: 10.10.11.0; Wildcard Mask: 0.0.0.255

(Mask bit 0 - Must match)

(Mask bit 1 - Don't care)

○ TCP ○ UDP ○ ICMP ● IP

IP Protocol: ip

☐ Log matches against this entry

In the Action dropdown box:

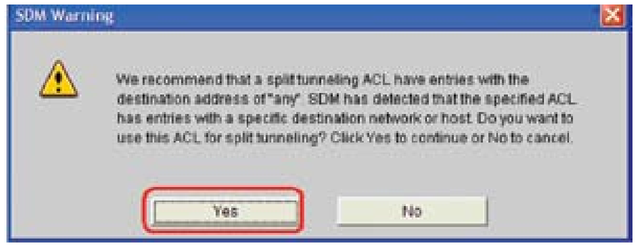
8. Click **Select an action** and select **Protect the traffic**.

In the Source Host/Network section:

9. **Type** – select **A Network**
10. **IP Address and Wildcard Mask** – this is the source subnet. Typically it is your LAN subnet.

In the Destination Host/Network section:

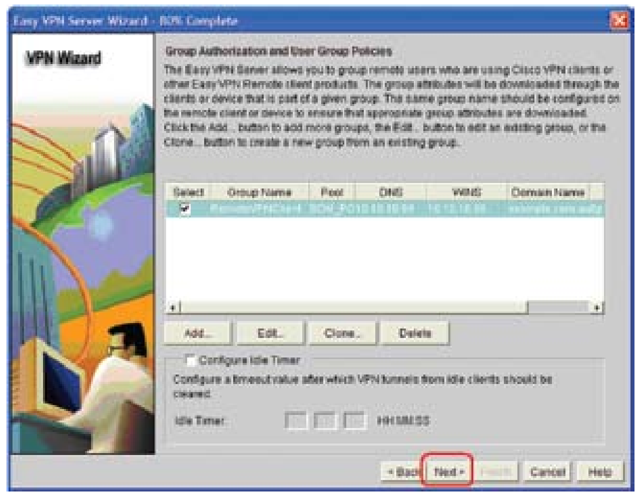
11. **Type** – select **A Network**
12. **IP Address and Wildcard Mask** – this is the destination subnet. This is your pool of IP addresses create in section 11(B) step 20 – Pool Information: – range of IP addresses that can be allocated to IPSec VPN Clients. This address MUST be unique.



SDM Warning

We recommend that a split tunneling ACL have entries with the destination address of "any". SDM has detected that the specified ACL has entries with a specific destination network or host. Do you want to use this ACL for split tunneling? Click Yes to continue or No to cancel.

13. Click **Yes**.



Easy VPN Server Wizard - 80% Complete

Group Authorization and User Group Policies

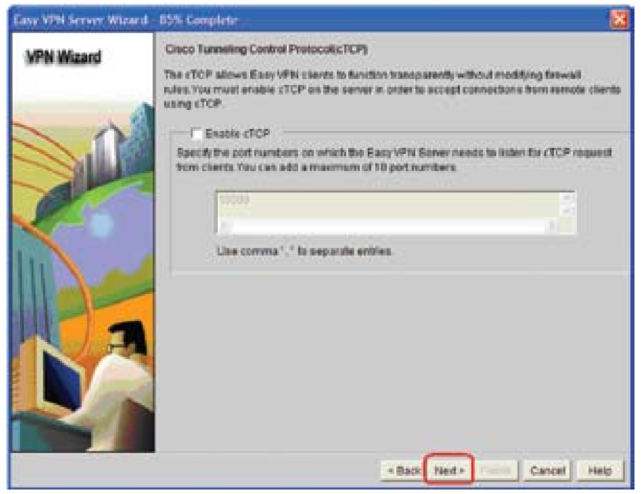
The Easy VPN Server allows you to group remote users who are using Cisco VPN clients or other Easy VPN Remote client products. The group attributes will be downloaded through the clients or device that is part of a given group. The same group name should be configured on the remote client or device to ensure that appropriate group attributes are downloaded. Click the Add... button to add more groups, the Edit... button to edit an existing group, or the Clone... button to create a new group from an existing group.

☐ Configure Idle Timer

Configure a timeout value after which VPN tunnels from idle clients should be cleared.

Idle Timer: HH:MM:SS

14. Click **Next**.



Easy VPN Server Wizard - 85% Complete

Cisco Tunneling Control Protocol(cTCP)

The cTCP allows Easy VPN clients to function transparently without modifying firewall rules. You must enable cTCP on the server in order to accept connections from remote clients using cTCP.

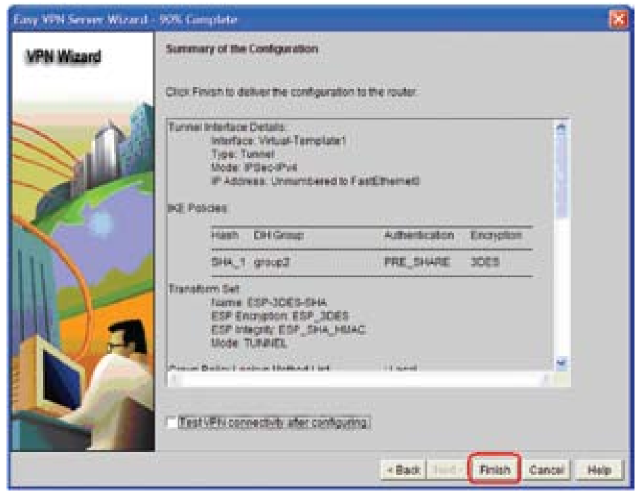
☐ Enable cTCP

Specify the port numbers on which the Easy VPN Server needs to listen for cTCP request from clients. You can add a maximum of 10 port numbers.

10000

Use comma ',' to separate entries.

15. Click **Next**.



Easy VPN Server Wizard - 90% Complete

Summary of the Configuration

Click Finish to deliver the configuration to the router.

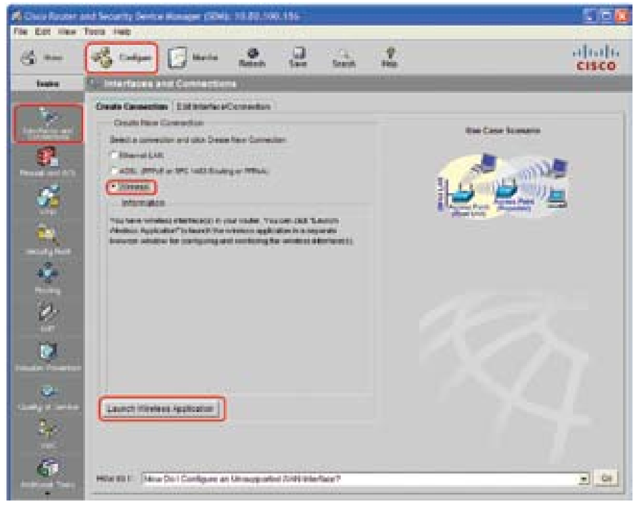
```
Tunnel Interface Details
        Interface: Virtual-Template1
        Type: Tunnel
        Mode: IPSec-IPv4
        IP Address: Unnumbered to FastEthernet0

IKE Policies
        Hash    DH Group        Authentication   Encryption
        SHA_1   group2          PRE_SHARE        3DES

Transform Set
        Name: ESP-3DES-SHA
        ESP Encryption: ESP_3DES
        ESP Integrity: ESP_SHA_HMAC
        Mode: TUNNEL
```

☐ Test VPN connectivity after configuring

16. Click **Finish**.

D. Wireless

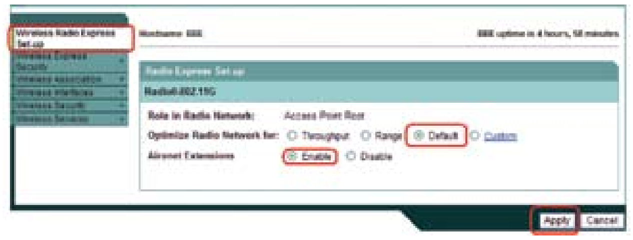
Router Wireless Configuration



STEPS:

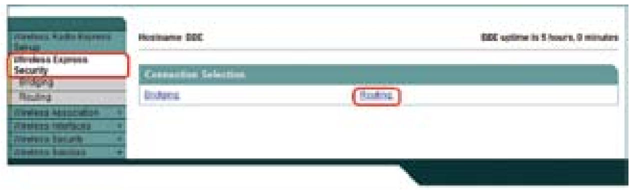
1. Click **Configure**.
2. Click **Interface and Connections** from the **Tasks** section.
3. Click **Create Connection** tab.
4. Click **Wireless** radio button.
5. Click **Launch Wireless**.

Radio Express Setup:

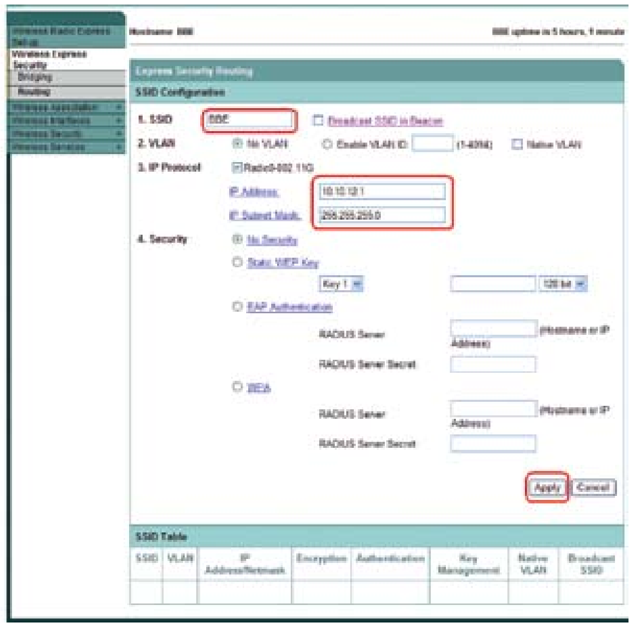


6. Click **Wireless Radio Express Setup**.
7. Select **Default** for **Optimize Radio Network for**.
8. Select **Enable** for **Aironet Extensions**.
9. Click **Apply**.

Please note: The Wireless hostname is provided as an example only.

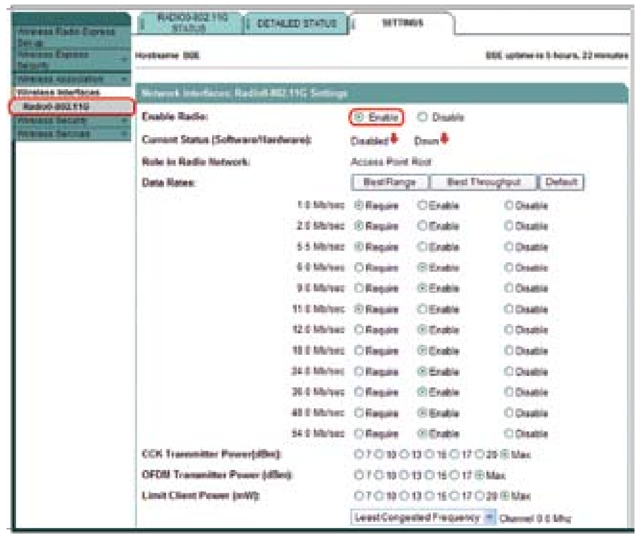


10. Click **Wireless Express Security**.
11. Select **Routing** from the **Connection Selection**.

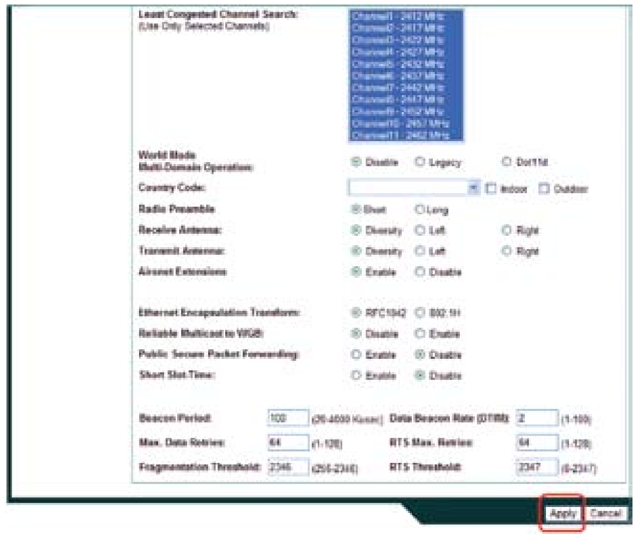


12. Fill in the following fields:
    - **SSID** (the SSID provided here is used for example purposes only).
    - **IP Address** and **IP Subnet Mask**.
13. Click **Apply**.

Configuring Wireless Interface:

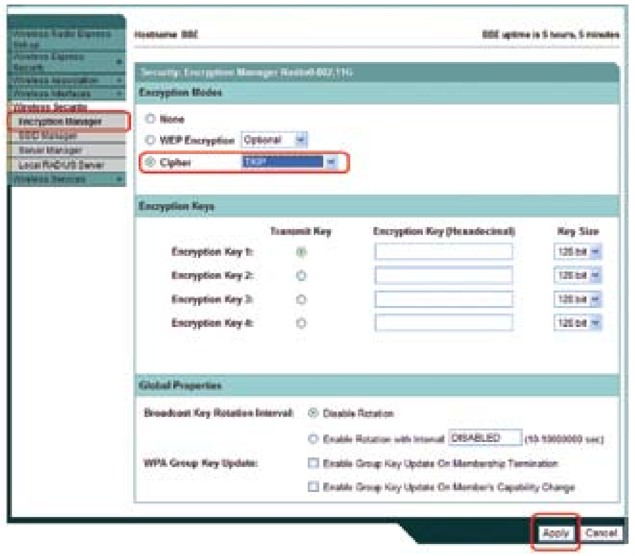


14. Click **Wireless Interface**.
15. Click **Radio 802.11G**.
16. Click **Setting** tab.
17. Select **Enable**.



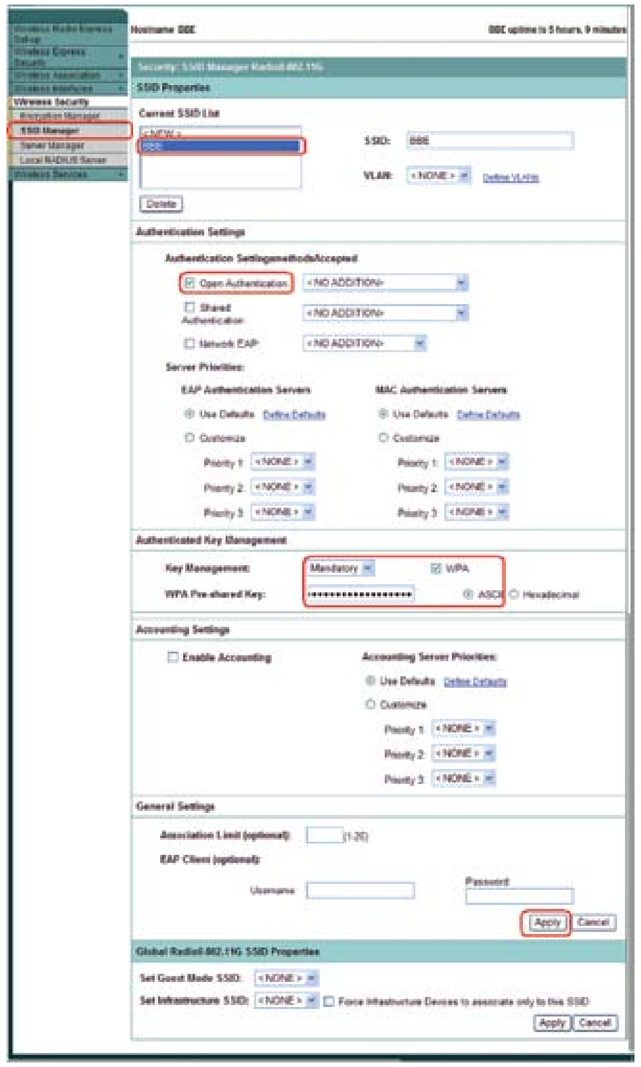
18. Click **Apply**.

Configuring Wireless Security: – Encryption Manager



19. Click **Wireless Security**.
20. Click **Encryption Manger**.
21. Select **Cipher** radio button. From the pull down menu, select **TKIP**.
22. Click **Apply**.

Configuring Wireless Security: – SSID Manager



Hostname BBE BBE uptime is 5 hours, 9 minutes

Security: SSID Manager Radio0-802.11G

SSID Properties

Current SSID List: < NEW >, BBE

SSID: BBE

VLAN: < NONE >

Authentication Settings

Authentication SettingsmethodsAccepted

☑ Open Authentication: < NO ADDITION >

☐ Shared Authentication: < NO ADDITION >

☐ Network EAP: < NO ADDITION >

Authenticated Key Management

Key Management: Mandatory ☑ WPA

WPA Pre-shared Key: •••••••••••••••••• ● ASCII ○ Hexadecimal

Accounting Settings

☐ Enable Accounting

General Settings

Association Limit (optional): (1-2K)

Global Radio0-802.11G SSID Properties

Set Guest Mode SSID: < NONE >

Set Infrastructure SSID: < NONE > ☐ Force Infrastructure Devices to associate only to this SSID

23. Click **Wireless Security**.

24. Click **SSID Manger**.

25. Click **BBE** from **Current SSID List**. The BBE SSID is an example. The user should select their custom SSID as defined in step XII – **Fill in the following fields**.

26. Select **Open Authentication** in **Authentication** Setting. From the drop down menu, select **TKIP**.

27. Under **Authenticated Key Management**:

a. Key Management, select **Mandatory** from the drop down menu.

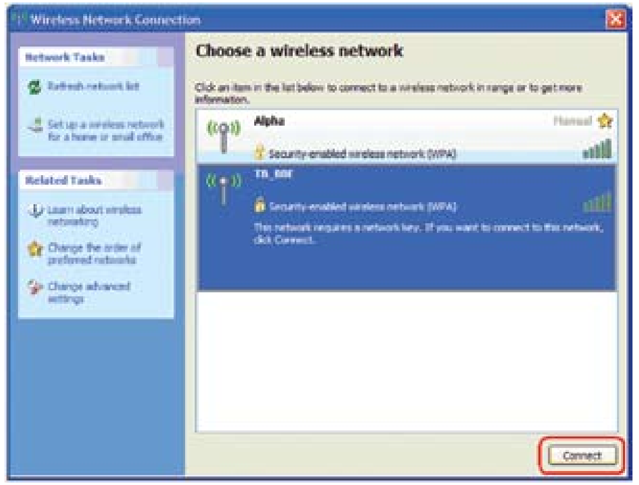
b. Select **WPA**.

c. **WPA Preshare Key** – enter WPA password, 20 to 60 characters long.

28. Click **Apply**.

29. Please refer to section 8(C) 2 **Dynamic Port Address Translation** to configure the router to allow wireless devices to access the internet.

Client Wireless Configuration



Wireless Network Connection

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

Alpha — Manual — Security-enabled wireless network (WPA)

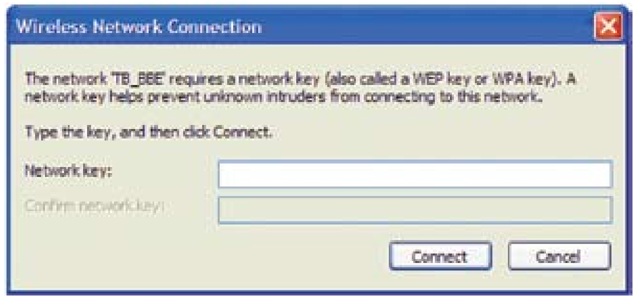
TB_BBE — Security-enabled wireless network (WPA) — This network requires a network key. If you want to connect to this network, click Connect.

Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Connect

STEPS:

1. Search for various wireless networks in the local vicinity.
2. The SSID configured will show up in the list. Select the desired SSID and click connect.

Please note: The SSID shown here is provided as an example.



Wireless Network Connection

The network 'TB_BBE' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.

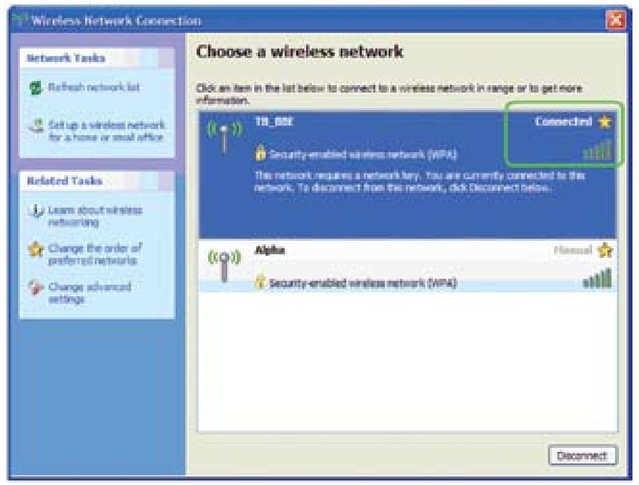
Type the key, and then click Connect.

Network key:

Confirm network key:

3. Enter the WPA shared key. This is the same key as entered in Step 27 (opposite) – Authenticated key management.
4. Re-enter the value in **Confirm network key**.
5. Click **Connect**.

You have successfully connected your client/PC to the Wireless connection as shown.



Wireless Network Connection

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

TB_BBE — Connected — Security-enabled wireless network (WPA) — This network requires a network key. You are currently connected to this network. To disconnect from this network, click Disconnect below.

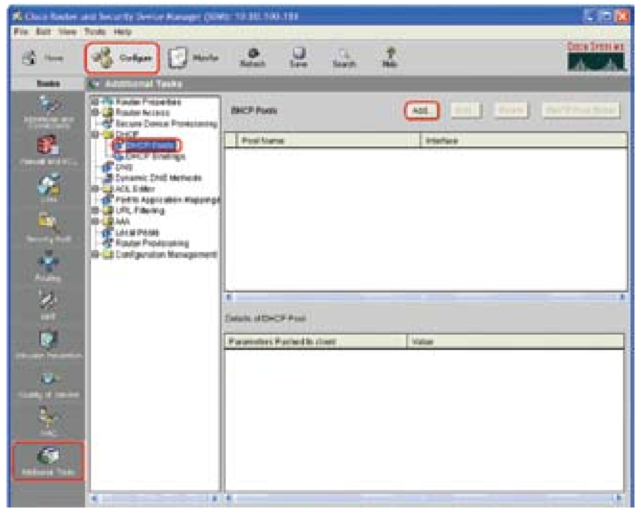
Alpha — Manual — Security-enabled wireless network (WPA)

Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Disconnect

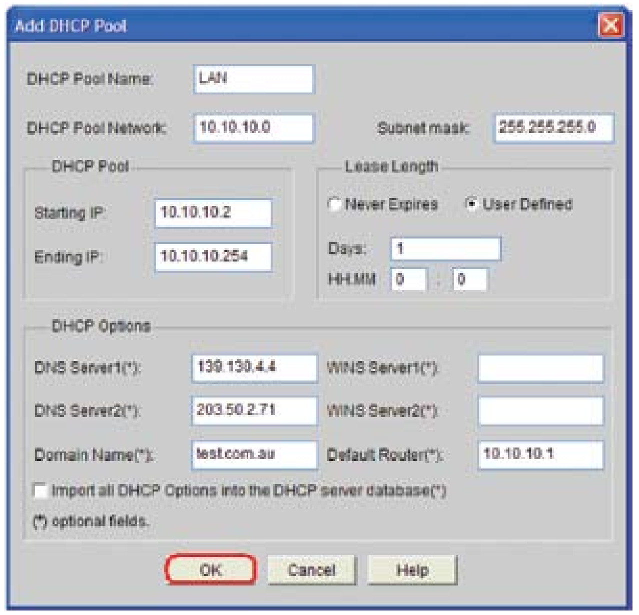
E. Configuring Router as a DHCP Server

STEPS:

1. Configure Static Interface as shown in section 8(A) 2 Configuring Ethernet/Static Interfaces.



2. Click **Configure**.
3. Click **Additional Tasks**.
4. Click **DHCP Pools**.
5. Click **Add**.



Add DHCP Pool

DHCP Pool Name: LAN

DHCP Pool Network: 10.10.10.0 Subnet mask: 255.255.255.0

DHCP Pool — Starting IP: 10.10.10.2 Ending IP: 10.10.10.254

Lease Length — ○ Never Expires ● User Defined — Days: 1 HH:MM 0 : 0

DHCP Options

DNS Server1(*): 139.130.4.4 WINS Server1(*):

DNS Server2(*): 203.50.2.71 WINS Server2(*):

Domain Name(*): test.com.au Default Router(*): 10.10.10.1

☐ Import all DHCP Options into the DHCP server database(*)

(*) optional fields.

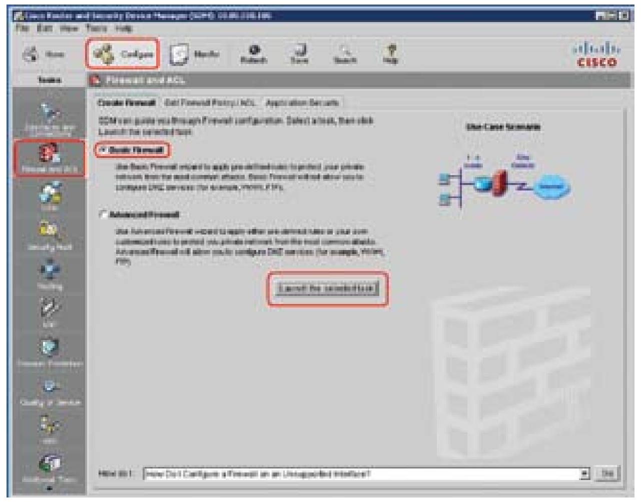
6. Fill in the fields as required for your internal network.

Please note: Domain name provided here is an example only.

F. Firewall

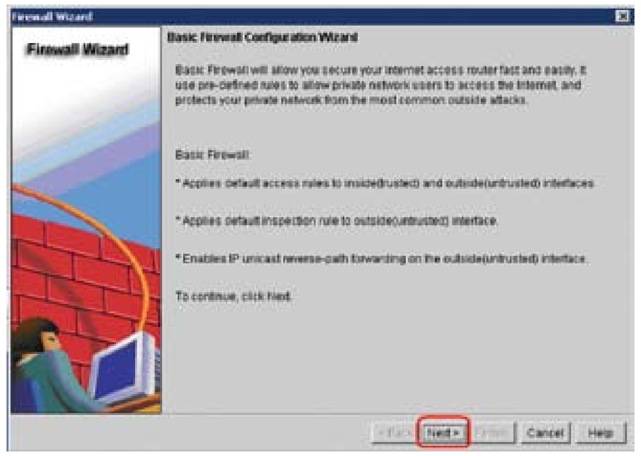
WARNING:

It is recommended that the administrator preview the commands before applying the firewall polices. Activating the firewall feature without familiarity with Cisco IOS firewall polices can cause disconnection and lock the administrator out of the router.



STEPS:

1. Click **Configure**.
2. Click **Firewall and ACL** in the **Tasks** section.
3. Click **Basic Firewall**.
4. Click **Launch Easy VPN Server Wizard**.



Basic Firewall Configuration Wizard

Basic Firewall will allow you secure your internet access router fast and easily. It use pre-defined rules to allow private network users to access the Internet, and protects your private network from the most common outside attacks.

Basic Firewall:

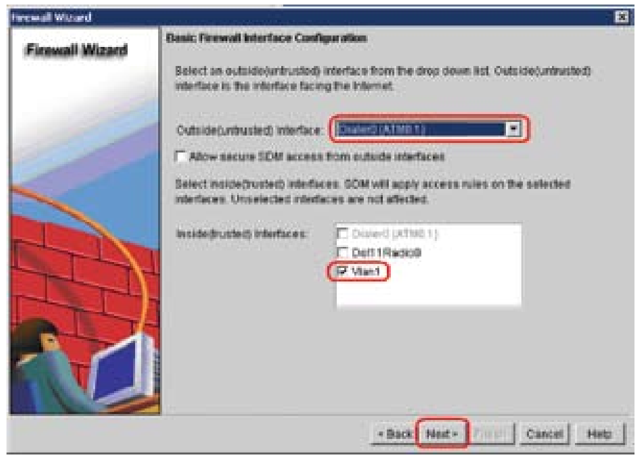
* Applies default access rules to inside(trusted) and outside(untrusted) interfaces.

* Applies default inspection rule to outside(untrusted) interface.

* Enables IP unicast reverse-path forwarding on the outside(untrusted) interface.

To continue, click Next.

5. Click **Next**.



Basic Firewall Interface Configuration

Select an outside(untrusted) interface from the drop down list. Outside(untrusted) interface is the interface facing the Internet.

Outside(untrusted) interface: Dialer0 (ATM0.1)

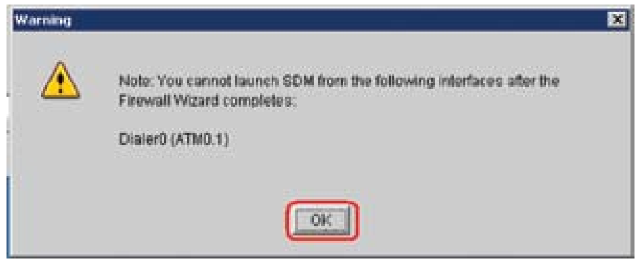
☐ Allow secure SDM access from outside interfaces

Select inside(trusted) interfaces. SDM will apply access rules on the selected interfaces. Unselected interfaces are not affected.

Inside(trusted) interfaces:
☐ Dialer0 (ATM0.1)
☐ Dot11Radio0
☑ Vlan1

6. Set **Outside (untrusted) Interface**.
7. Select **Inside (Trusted) Interface**.
8. Click **Next**.

You will be provided with the below screen to confirm the action:



Note: You cannot launch SDM from the following interfaces after the Firewall Wizard completes:

Dialer0 (ATM0.1)

9. Click **OK**.

There are three levels of Security, as described below:

Important notice to all customers selecting “High” or “Medium” Firewall policy levels.

Your Cisco device will constantly download the information it requires to enforce access controls, which may result in increased downloads which count towards the usage of your Telstra Business Broadband plan[8]. This is more likely to occur if you have set your Firewall/security policy to either “**High**” or “**Medium**” – please consult your IT specialist for further advice.

High Security:

Select this option if you want to prevent use of these applications on the network.

- The router identifies inbound and outbound Instant Messaging and drops it.
- The router checks inbound and outbound HTTP traffic and e-mail traffic for protocol compliance, and drops non-compliant traffic.
- Return traffic for other TCP and UDP applications is routed if the session was initiated inside the firewall.

Medium Security:

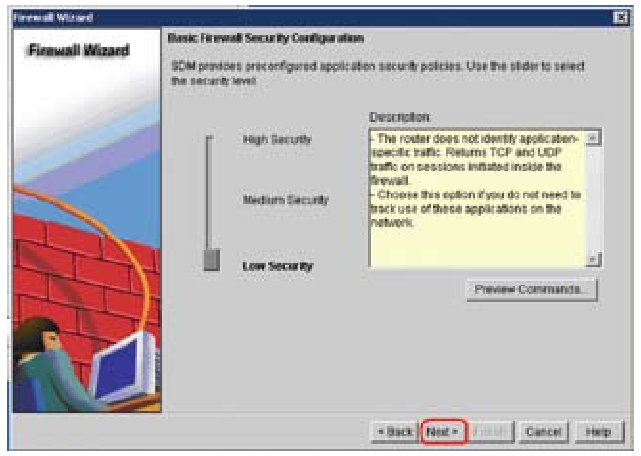
Select this option if you want to track use of these applications on the network.

- The router identifies inbound and outbound Instant Messaging, and checks inbound and outbound HTTP traffic and e-mail traffic for protocol compliance.
- Return TCP and UDP traffic on sessions initiated inside the firewall is routed.

Low Security:

Select this option if you do not need to track use of these applications on the network.

- The router does not identify application-specific traffic. Returns TCP and UDP traffic on sessions initiated inside the firewall.



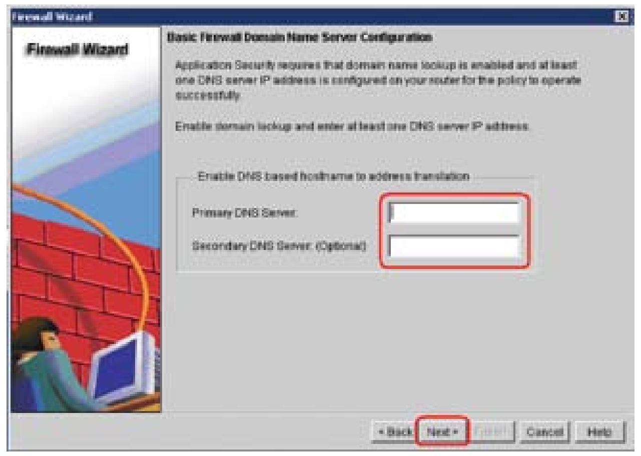
Basic Firewall Security Configuration

SDM provides preconfigured application security policies. Use the slider to select the security level.

Description:

- The router does not identify application-specific traffic. Returns TCP and UDP traffic on sessions initiated inside the firewall.
- Choose this option if you do not need to track use of these applications on the network.

10. Select the Security level required.
11. Click **Next**.



Basic Firewall Domain Name Server Configuration

Application Security requires that domain name lookup is enabled and at least one DNS server IP address is configured on your router for the policy to operate successfully.

Enable domain lookup and enter at least one DNS server IP address.

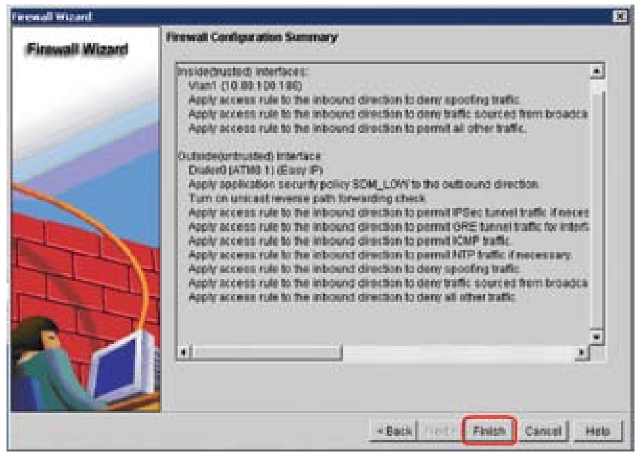
Enable DNS based hostname to address translation

Primary DNS Server:

Secondary DNS Server: (Optional)

12. Enter your Primary DNS Server address.
13. Click **Next**.

Your Firewall Configuration is now complete.



Firewall Configuration Summary

```
Inside(trusted) interfaces:
  Vlan1 (10.80.100.180)
  Apply access rule to the inbound direction to deny spoofing traffic.
  Apply access rule to the inbound direction to deny traffic sourced from broadca
  Apply access rule to the inbound direction to permit all other traffic.

Outside(untrusted) interface:
  Dialer0 (ATM0.1) (Easy IP)
  Apply application security policy SDM_LOW to the outbound direction.
  Turn on unicast reverse path forwarding check.
  Apply access rule to the inbound direction to permit IPSec tunnel traffic if neces
  Apply access rule to the inbound direction to permit GRE tunnel traffic for interf
  Apply access rule to the inbound direction to permit ICMP traffic.
  Apply access rule to the inbound direction to permit NTP traffic if necessary.
  Apply access rule to the inbound direction to deny spoofing traffic.
  Apply access rule to the inbound direction to deny traffic sourced from broadca
  Apply access rule to the inbound direction to deny all other traffic.
```

14. Click **Finish**.

12. GLOSSARY

ADSL	Asymmetric Digital Subscriber Line
Ethernet	Business Digital Subscriber Line
Telstra Business Support Extras	IT support services – PAYG options, IT Services On Demand
CLI	Command Line Interface
CPE	Customer Premise Equipment
DSL	Digital Subscriber Line
DNS	Domain Name System (Server)
DHCP	Dynamic Host Control Protocol
IOS	Internetwork Operating System
IP Address	Internet Protocol Address
IPSec	Internet Protocol Security
JRE	Java Runtime Environment
LAN	Local Area Network
NAT	Network Address Translation
PAT	Port Address Translation
Router Support Service	Subscription based service for basic router configuration changes
SSID	Service Set Identifier – the unique name given to a Wireless Network
Split Tunneling	Allows IPSec VPN users to access the internet and their LAN using the same connection
SDM	Security Device Manager
WAN	Wide Area Network
WINS	Windows Internet Name Service
VPN	Virtual Private Network
VPN Client	The application used to communicate securely with your Cisco router over the internet

13. NEED ADDITIONAL HELP?

Please contact the Telstra Business Technical Helpdesk on **1800 066 594** or visit us at **telstrabusiness.com**

The following links may be useful:

Cisco 1812:
www.cisco.com/en/US/products/ps6183/index.html

Cisco 800 Series ISR's Q&A:
www.cisco.com/en/US/prod/collateral/routers/ps380/ps6200/prod_qas0900aecd8028a982.html

Cisco Security Device Manager:
www.cisco.com/en/US/products/sw/secursw/ps5318/index.html

FOR THOSE WHO LIKE THE DETAILS, WE'VE GOT THEM HERE

1. The 1812 Router supplied is non wireless.
2. This guide does not step through the modification to Command Line Interface (CLI).
3. Additional fees and charges may apply.
4. This guide does not provide instructions on how to modify the CLI.
5. Some support exclusions apply.
6. Not available unless Router Support Service is purchased. Telstra does not support faults relating to customer initiated IPSec VPN set up, for support of this feature please contact your IT Specialist or contact us on 1800 655 744 to find out more about our Telstra Business Support Extras services.
7. The VPN Client supports both the Windows 2000 Server and the Windows 2003 Server operating systems.
8. Excess Usage charges will apply if subscribed plan is exceeded.