AlliedWare^{TM} OS

How To | Create a VPN between an Allied Telesis and a SonicWALL Router, with NAT-T

Today's network managers often need to incorporate other vendors' equipment into their networks, as companies change and grow. To support this challenge, Allied Telesis routers are designed to inter-operate with a wide range of equipment.

This How To Note details one of the inter-operation solutions from Allied Telesis: creating virtual private networks between Allied Telesis and SonicWALL routers. It shows you how to configure a VPN between a local Allied Telesis router and a remote SonicWALL router, step-by-step. On the Allied Telesis router, it uses the Site-To-Site VPN wizard for the VPN configuration.

The wizard runs on selected AR400 Allied Telesis routers from the router's web-based GUI (graphical user interface). It asks you to enter a few details and from those it configures the following settings:

- encryption to protect traffic over the VPN
- ISAKMP with a pre-shared key to manage the VPN
- the firewall, to protect the LANs and to allow traffic to use the VPN
- Network Address Translation (NAT), so that you can access the Internet from the private LAN through a single public IP address. This Internet access does not interfere with the VPN solution
- (in this example) NAT-Traversal because one end of the VPN tunnel is behind a separate NAT device

What information will you find in this document?

This How To Note begins with the following information:

Then it describes the configuration, in the following sections:

Related How To Notes

Allied Telesis offers How To Notes with a wide range of VPN solutions, from quick and simple solutions for connecting home and remote offices, to advanced multi-feature setups. Notes also describe how to create a VPN between an Allied Telesis router and equipment from a number of other vendors.

For a complete list of VPN How To Notes, see the *Overview of VPN Solutions in How To Notes* in the How To Library at www.alliedtelesis.com/resources/literature/howto.aspx.

Which products and software version does it apply to?

The VPN wizard is available on the following Allied Telesis routers, running Software Version 2.9.1 or later:

- AR415S
- AR440S, AR441S, AR442S

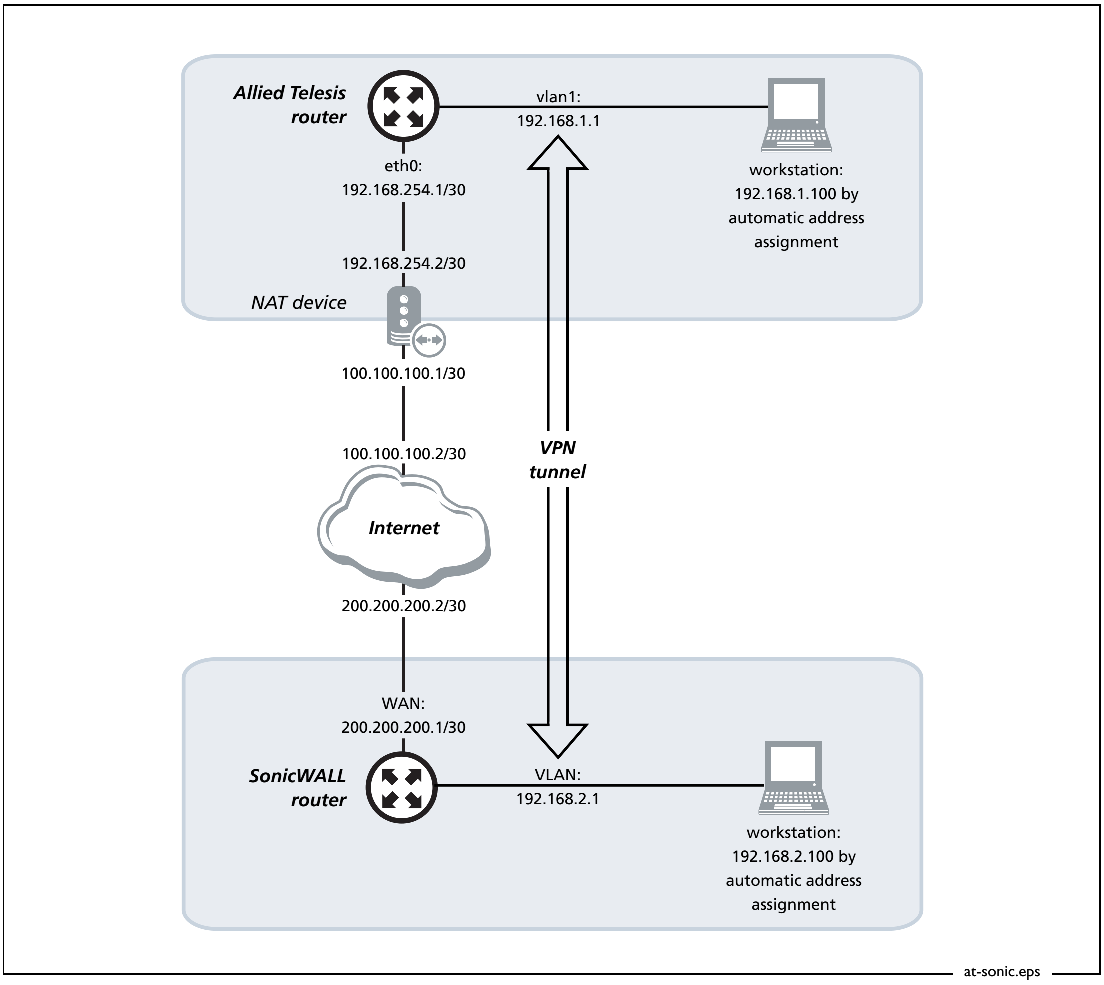
You can use the command line to set up an equivalent configuration on AR700 and other AR400 Series routers. See "How to use the CLI instead of the GUI" on page 30 for the necessary commands.

We created this example with a SonicWALL TZ 170, running SonicOS Enhanced 2.5.1.1-65e. SonicOS Standard does not support NAT-T draft 3, so this solution requires SonicOS Enhanced.

The screenshots in this Note are from an Internet Explorer 6.0 browser running on Windows XP.

The network

This example illustrates a NAT-T solution, which you need when one or both of the routers are behind a NAT device such as some xDSL and cable modems. In this example, an Allied Telesis AR415S router is behind a NAT device. The following diagram shows the LANs and their interfaces and addresses.



Note: You can still use this example if you have no NAT device between the Allied Telesis router and the Internet, or if you have a NAT device between the SonicWALL router and the Internet, with slight alterations. See "Appendix: Using this example if you don't have a NAT device in the same position" on page 31 for details.

Initiating the tunnel from either end

In this example, you can only initiate the tunnel from the Allied Telesis end, not the SonicWALL end. If you want to let the SonicWALL initiate the VPN too, you have to configure your NAT device to allow it. To do this, set up pinholes (allow rules) on the NAT device to allow through UDP traffic on ports 500 and 4500.

How to configure the Allied Telesis router

Before you start

1. Install and configure the NAT device.
2. Access the router via its GUI.
3. Customise the router and set up vlan1 as the LAN interface. The site-to-site VPN wizard always uses vlan1 as the local LAN for the VPN connection, so you must make sure an IP interface is configured on vlan1 before running the wizard.
4. Create a security officer. If you use the Basic Setup wizard to customise the router, this creates one security officer, with a username of "secoff".
5. Set up the WAN interface. This example uses a fixed IP address on the WAN interface—modify it to use an appropriate interface for your network.

The router setup of steps 2-5 is described in *How To Use the Allied Telesis GUI to Customise the Router and Set Up An Internet Connection*, which is available from www.alliedtelesis.com/resources/literature/howto.aspx.

In this example, the Allied Telesis router has the following settings:

	Interface	**Address**	**Mask**
Allied Telesis router LAN	vlan1	192.168.1.1	255.255.255.0
Allied Telesis router WAN	eth0	192.168.254.1	255.255.255.252
Remote site's WAN settings		200.200.200.1	
Remote site's LAN settings		192.168.2.1	255.255.255.0

The NAT device has the following settings:

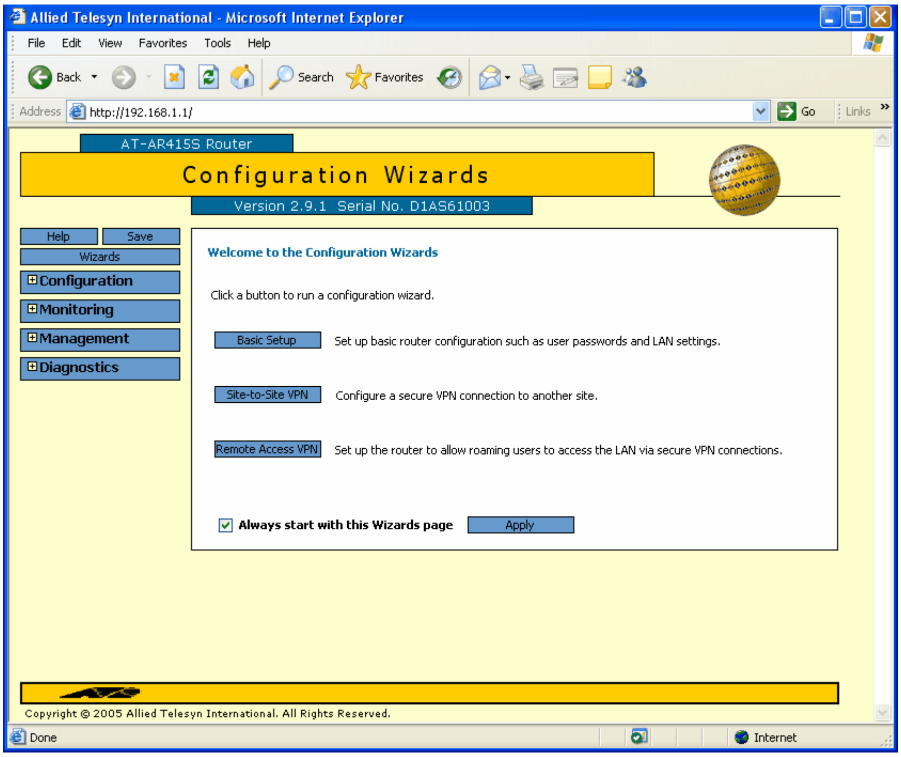
	Interface	**Address**	**Mask**
Private interface (towards the router)	eth1	192.168.254.2	255.255.255.252
Public interface (towards the Internet)	eth0	100.100.100.1	255.255.255.252

Create the VPN tunnel

1. Open the Configuration Wizards page

Log in as either the manager or the security officer. If you log in as the manager, the router changes to secure mode when you finish the VPN wizard and at that stage prompts you to log in again as the security officer.

The Site-To-Site VPN wizard is one of the options on the Configuration Wizards page. Make sure your browser's pop-up blocker is disabled—the wizard needs to open pop-ups. If you access the Internet through a proxy server, make sure your browser bypasses the proxy for this address.


Allied Telesyn International - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.1.1/
Go Links
AT-AR415S Router
Configuration Wizards
Version 2.9.1 Serial No. D1AS61003
Help Save
Wizards
Configuration
Monitoring
Management
Diagnostics

Welcome to the Configuration Wizards

Click a button to run a configuration wizard.

Basic Setup — Set up basic router configuration such as user passwords and LAN settings.

Site-to-Site VPN — Configure a secure VPN connection to another site.

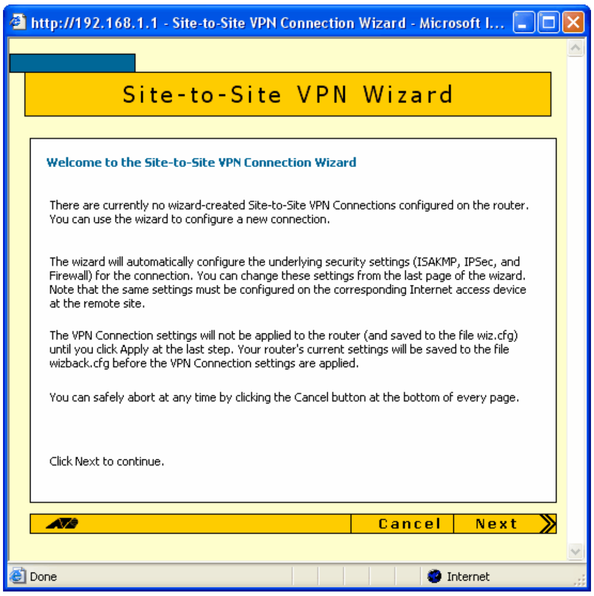
Remote Access VPN — Set up the router to allow roaming users to access the LAN via secure VPN connections.

☑ Always start with this Wizards page — Apply

Copyright © 2005 Allied Telesyn International. All Rights Reserved.
Done
Internet

The GUI opens at this page the first time you configure your router. After initial configuration it may open at the System Status page instead. If so, click on the Wizards button in the left-hand menu to open the Configuration Wizards page.

2. Start the Site-to-Site VPN wizard


http://192.168.1.1 - Site-to-Site VPN Connection Wizard - Microsoft I...
Site-to-Site VPN Wizard
Cancel
Next
Done
Internet

Welcome to the Site-to-Site VPN Connection Wizard

There are currently no wizard-created Site-to-Site VPN Connections configured on the router. You can use the wizard to configure a new connection.

The wizard will automatically configure the underlying security settings (ISAKMP, IPSec, and Firewall) for the connection. You can change these settings from the last page of the wizard. Note that the same settings must be configured on the corresponding Internet access device at the remote site.

The VPN Connection settings will not be applied to the router (and saved to the file wiz.cfg) until you click Apply at the last step. Your router's current settings will be saved to the file wizback.cfg before the VPN Connection settings are applied.

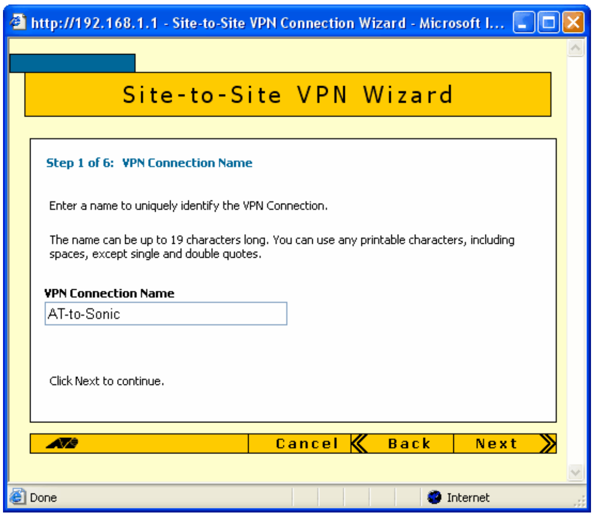
You can safely abort at any time by clicking the Cancel button at the bottom of every page.

Click Next to continue.

Click on the Site-to-Site VPN button. The wizard starts by displaying a welcome message.

Click the Next button.

3. Name the VPN connection


http://192.168.1.1 - Site-to-Site VPN Connection Wizard - Microsoft I...
Site-to-Site VPN Wizard
Cancel
Back
Next
Done
Internet

Step 1 of 6: VPN Connection Name

Enter a name to uniquely identify the VPN Connection.

The name can be up to 19 characters long. You can use any printable characters, including spaces, except single and double quotes.

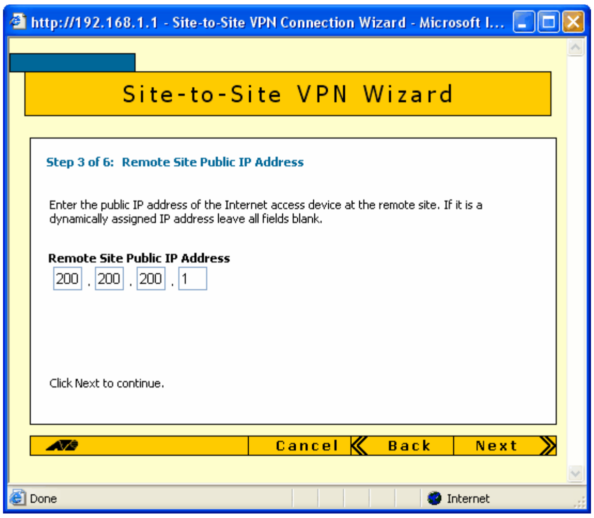
VPN Connection Name
AT-to-Sonic

Click Next to continue.

Enter an appropriate VPN connection name.

Click the Next button. If you have multiple possible WAN interfaces configured on the router, the wizard next lets you select the appropriate interface. In this example there is only one WAN interface, so the wizard selects it automatically and moves directly to the remote site settings.

4. Enter the remote site's WAN IP address


http://192.168.1.1 - Site-to-Site VPN Connection Wizard - Microsoft I...

Site-to-Site VPN Wizard

Step 3 of 6: Remote Site Public IP Address

Enter the public IP address of the Internet access device at the remote site. If it is a dynamically assigned IP address leave all fields blank.

Remote Site Public IP Address
200 . 200 . 200 . 1

Click Next to continue.

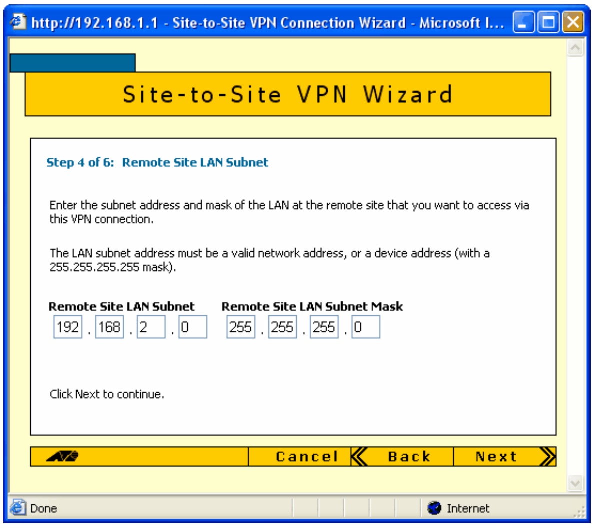
Cancel
Back
Next
Done
Internet

Enter the public IP address of the other end of the tunnel. In this example, this is 200.200.200.1, which is the IP address of the SonicWALL WAN interface.

Note that you can use the Tab key to move between fields when entering the address, but should not use the . key (the period).

Click the Next button.

5. Enter the remote site's LAN IP address


http://192.168.1.1 - Site-to-Site VPN Connection Wizard - Microsoft I...

Site-to-Site VPN Wizard

Step 4 of 6: Remote Site LAN Subnet

Enter the subnet address and mask of the LAN at the remote site that you want to access via this VPN connection.

The LAN subnet address must be a valid network address, or a device address (with a 255.255.255.255 mask).

Remote Site LAN Subnet
192 . 168 . 2 . 0

Remote Site LAN Subnet Mask
255 . 255 . 255 . 0

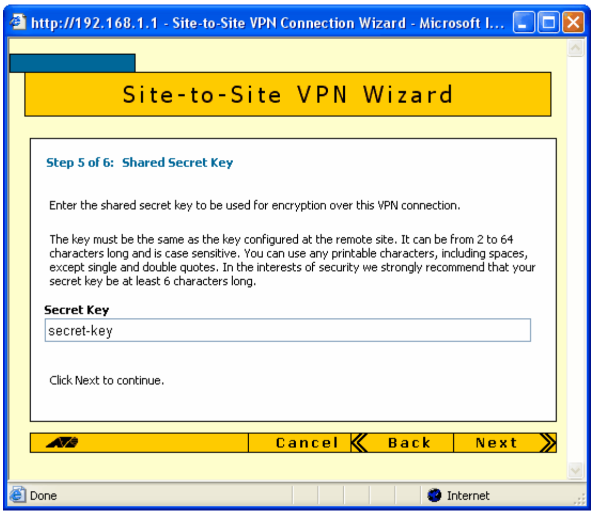
Click Next to continue.

Cancel
Back
Next
Done
Internet

Enter the SonicWALL router's LAN subnet address and mask. In this example, this is 192.168.2.0 and a mask of 255.255.255.0.

Click the Next button.

6. Enter the shared secret key



http://192.168.1.1 - Site-to-Site VPN Connection Wizard - Microsoft I...
Site-to-Site VPN Wizard
Cancel
Back
Next
Done
Internet

Step 5 of 6: Shared Secret Key

Enter the shared secret key to be used for encryption over this VPN connection.

The key must be the same as the key configured at the remote site. It can be from 2 to 64 characters long and is case sensitive. You can use any printable characters, including spaces, except single and double quotes. In the interests of security we strongly recommend that your secret key be at least 6 characters long.

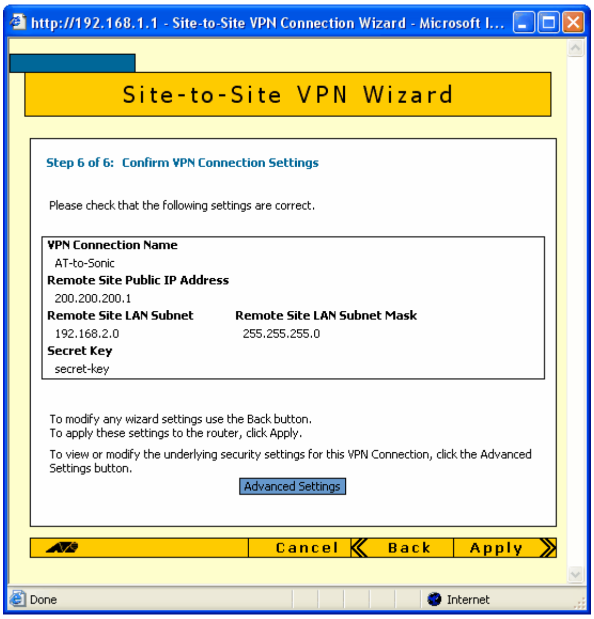
Secret Key: secret-key

Click Next to continue.

Enter the secret key, which is an alphanumeric string between 2 and 64 characters long. Both routers must use the same secret key. On the SonicWALL router, this is the Site-to-Site Policy’s preshared key.

Click the Next button.

7. Check the settings



http://192.168.1.1 - Site-to-Site VPN Connection Wizard - Microsoft I...
Site-to-Site VPN Wizard
Advanced Settings
Cancel
Back
Apply
Done
Internet

Step 6 of 6: Confirm VPN Connection Settings

Please check that the following settings are correct.

VPN Connection Name: AT-to-Sonic

Remote Site Public IP Address: 200.200.200.1

Remote Site LAN Subnet: 192.168.2.0

Remote Site LAN Subnet Mask: 255.255.255.0

Secret Key: secret-key

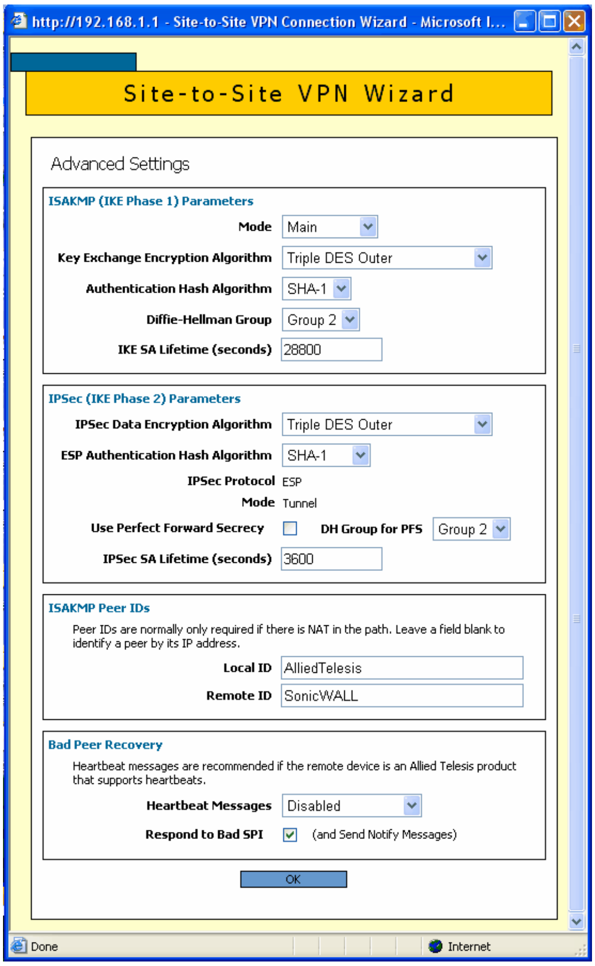
To modify any wizard settings use the Back button.
To apply these settings to the router, click Apply.

To view or modify the underlying security settings for this VPN Connection, click the Advanced Settings button.

Check the summary. If necessary, use the wizard’s Back button to return and correct any settings you want to change.

Once you are happy with the settings, click the Advanced Settings button to modify Peer ID settings.

8. Specify Peer IDs



http://192.168.1.1 - Site-to-Site VPN Connection Wizard - Microsoft I...

Site-to-Site VPN Wizard

Advanced Settings

ISAKMP (IKE Phase 1) Parameters

Mode	Main
Key Exchange Encryption Algorithm	Triple DES Outer
Authentication Hash Algorithm	SHA-1
Diffie-Hellman Group	Group 2
IKE SA Lifetime (seconds)	28800

IPSec (IKE Phase 2) Parameters

IPSec Data Encryption Algorithm	Triple DES Outer
ESP Authentication Hash Algorithm	SHA-1
IPSec Protocol	ESP
Mode	Tunnel
Use Perfect Forward Secrecy	□ DH Group for PFS: Group 2
IPSec SA Lifetime (seconds)	3600

ISAKMP Peer IDs

Peer IDs are normally only required if there is NAT in the path. Leave a field blank to identify a peer by its IP address.

Local ID	AlliedTelesis
Remote ID	SonicWALL

Bad Peer Recovery

Heartbeat messages are recommended if the remote device is an Allied Telesis product that supports heartbeats.

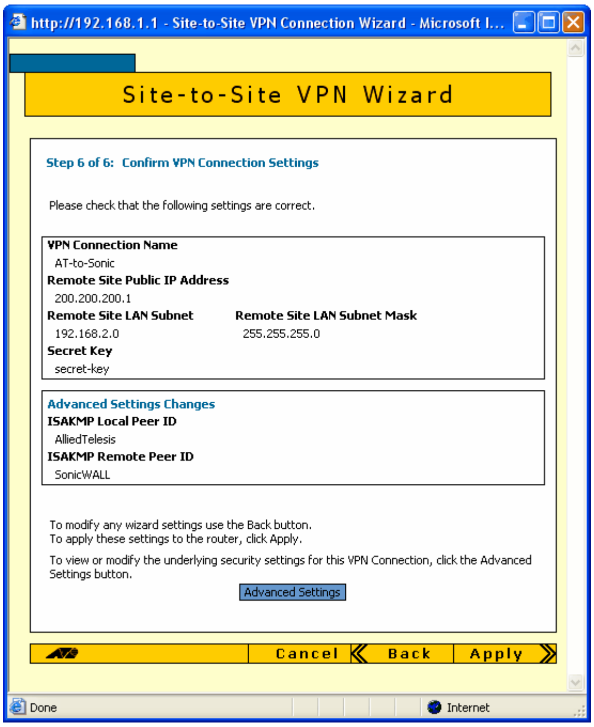
Heartbeat Messages	Disabled
Respond to Bad SPI	☑ (and Send Notify Messages)

Peer IDs enable the routers to identify each other when they exchange secret key information. By default, the Peer IDs are the router IP addresses. This does not work when one (or both) routers are behind a separate NAT device, because the NAT device changes the IP addresses.

Towards the bottom of the Advanced Settings page, enter a local ID (to identify this router) and a remote ID (to identify the router at the other end of the link). It does not matter what text you use as the IDs, so long as each ID is different.

Then click the OK button.

9. Check the settings again


http://192.168.1.1 - Site-to-Site VPN Connection Wizard - Microsoft I...
Site-to-Site VPN Wizard

Step 6 of 6: Confirm VPN Connection Settings

Please check that the following settings are correct.

VPN Connection Name
AT-to-Sonic
Remote Site Public IP Address
200.200.200.1
Remote Site LAN Subnet **Remote Site LAN Subnet Mask**
192.168.2.0 255.255.255.0
Secret Key
secret-key

Advanced Settings Changes
ISAKMP Local Peer ID
AlliedTelesis
ISAKMP Remote Peer ID
SonicWALL

To modify any wizard settings use the Back button.
To apply these settings to the router, click Apply.

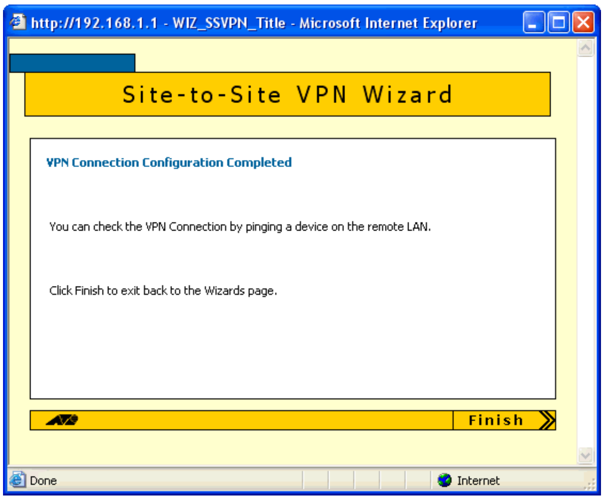
To view or modify the underlying security settings for this VPN Connection, click the Advanced Settings button.

Check the summary. It now includes the Peer ID settings. If necessary, correct any settings you want to change.

When all the settings are correct, click the Apply button.

10. Finish the wizard

Security officer


http://192.168.1.1 - WIZ_SSVPN_Title - Microsoft Internet Explorer
Site-to-Site VPN Wizard

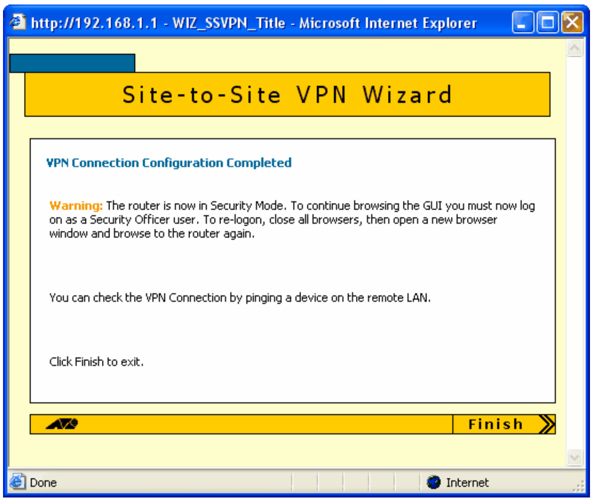
VPN Connection Configuration Completed

You can check the VPN Connection by pinging a device on the remote LAN.

Click Finish to exit back to the Wizards page.

If you are logged in as the security officer, the GUI displays a completion message. Click the Finish button to finish the Wizard and save the VPN settings.

Manager


http://192.168.1.1 - WIZ_SSVPN_Title - Microsoft Internet Explorer
Site-to-Site VPN Wizard
Finish
Done
Internet

VPN Connection Configuration Completed

Warning: The router is now in Security Mode. To continue browsing the GUI you must now log on as a Security Officer user. To re-logon, close all browsers, then open a new browser window and browse to the router again.

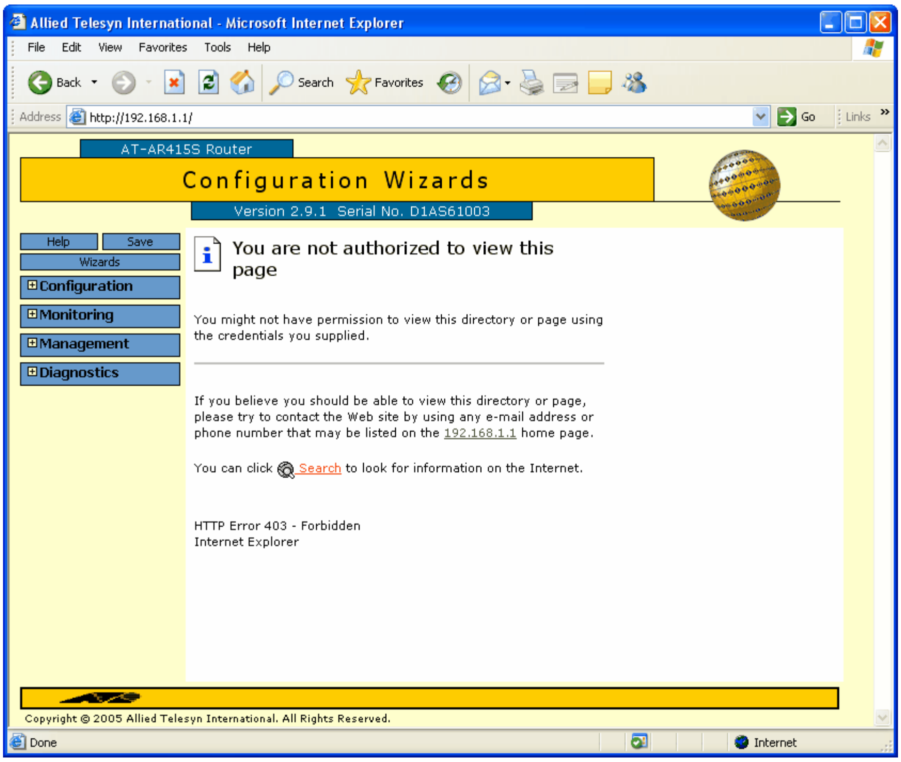
You can check the VPN Connection by pinging a device on the remote LAN.

Click Finish to exit.

If you are logged in as manager, the GUI displays a message to warn you that you will need to close your browser and re-login as a security officer (see below) once you have finished the wizard.

Click the Finish button to finish the Wizard and save the VPN settings.

The browser now indicates that you no longer have permission to view the GUI.


Allied Telesyn International - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address http://192.168.1.1/
Go
Links
AT-AR415S Router
Configuration Wizards
Version 2.9.1 Serial No. D1AS61003
Help
Save
Wizards
Configuration
Monitoring
Management
Diagnostics
Copyright © 2005 Allied Telesyn International. All Rights Reserved.
Done
Internet

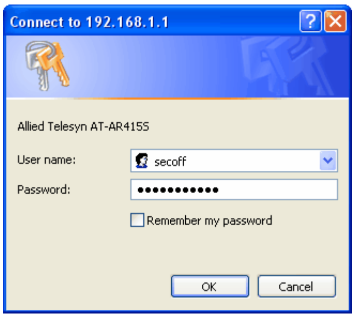
You are not authorized to view this page

You might not have permission to view this directory or page using the credentials you supplied.

If you believe you should be able to view this directory or page, please try to contact the Web site by using any e-mail address or phone number that may be listed on the 192.168.1.1 home page.

You can click Search to look for information on the Internet.

HTTP Error 403 - Forbidden
Internet Explorer



Allied Telesyn AT-AR415S

User name: secoff

Password: ●●●●●●●●●●●

□ Remember my password

The router configuration is now complete. If required, you can log in to the router again for further configuration or monitoring. To do this, close your browser, open it again, and browse to the router's IP address.

If you used the Basic Setup wizard to configure the LAN settings, the router will have one security officer, with a username of "secoff".

Login as the security officer.

How to configure the SonicWALL router

To configure the SonicWALL router, perform the steps in the following sections:

1. "Access the Router" on page 12
2. "Customise the router and set up the network" on page 15
3. "Define the LAN subnet of the peer" on page 20
4. "Create the VPN" on page 23
5. "Set the VPN IKE IDs and use Main Mode" on page 27

Access the Router

By default, SonicWALL TZ 170 routers start up with a LAN interface IP address of 192.168.168.168 and mask of 255.255.255.0.

Resetting to factory defaults

If you have difficulty accessing your SonicWALL, you may need to reset it to its factory defaults. To do this:

1. Give your PC an address in the subnet 192.168.168.0 (but not 192.168.168.168).
2. Power up the SonicWALL.
3. Press the Reset button—the pinhole button beside the console port—until the “test” light on the front flashes orange. This puts the router in SafeMode.
4. Connect the PC's NIC to any of the SonicWALL LAN ports and browse to 192.168.168.168.
5. Make sure any pop-up blocker is disabled for that address.
6. Click on the button that allows you to boot up with “Current firmware with Factory Default Settings”
7. Wait for the GUI to re-display the login screen. If it has not done so after about a minute, refresh your browser to force the GUI to refresh.
8. Log in using the factory defaults of:

   username: admin

   password: password

1. Connect a PC to the router

Select a standalone PC to configure the router from—a PC that is not connected into any existing LAN.

Connect a NIC card on the PC to any of the router’s LAN ports.

2. Set the PC’s IP address

Give your PC an address in the 192.168.168.0 subnet.

3. Browse to the router's management GUI

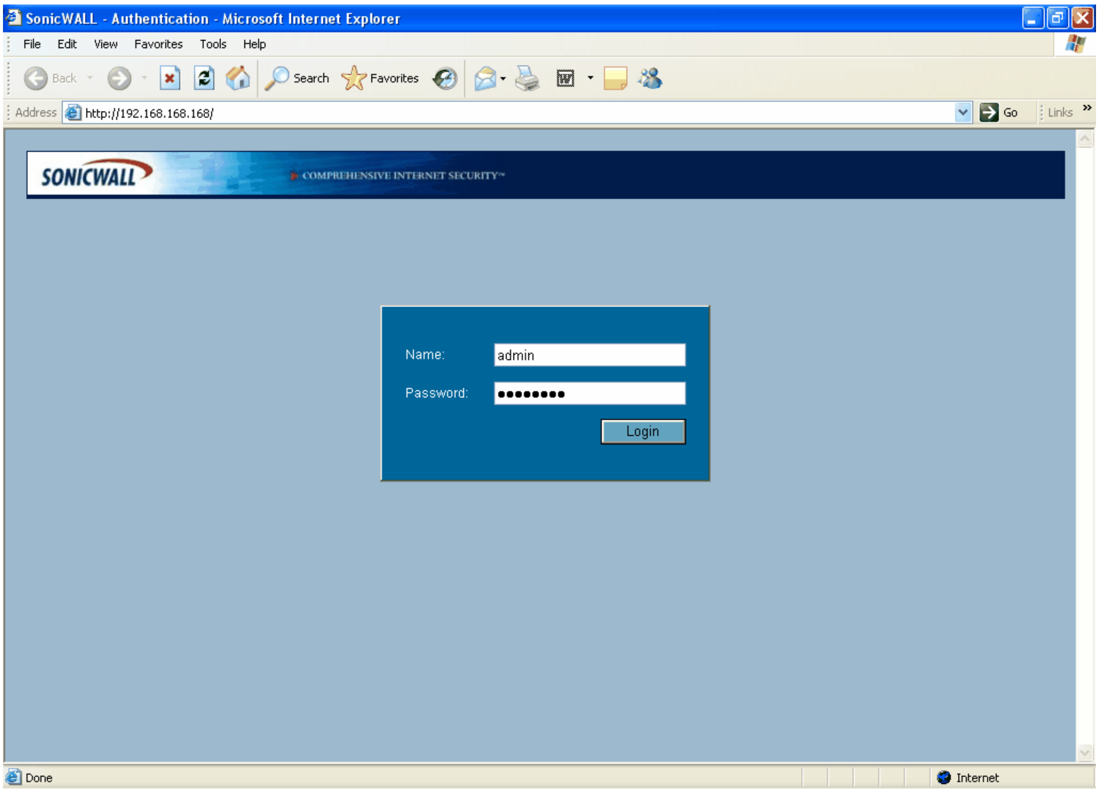
Browse to 192.168.168.168. If you are using a pop-up blocker, disable it for this address. If you access the Internet through a proxy server, set your browser to bypass the proxy for this address.

The login dialog box opens.

4. Log on

The defaults are

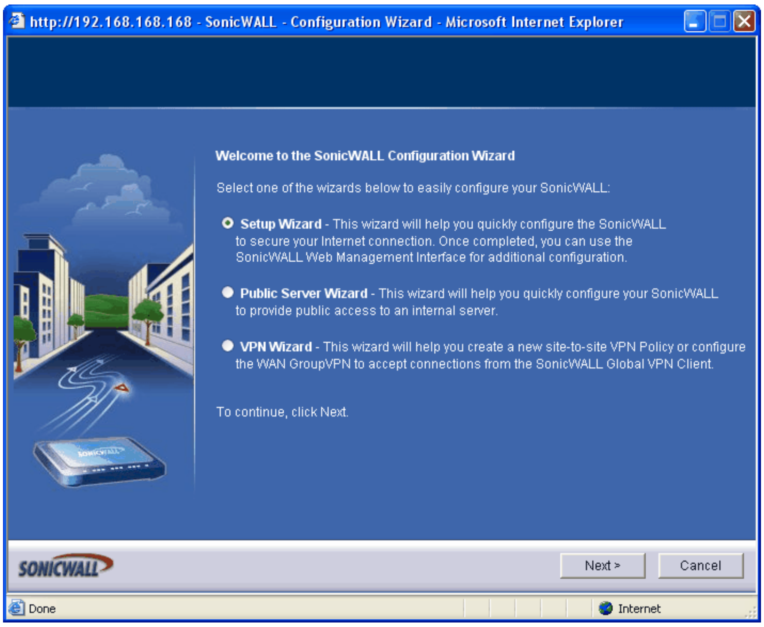
username:	admin
password:	password


SonicWALL - Authentication - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go
Links
SONICWALL
COMPREHENSIVE INTERNET SECURITY
Login
Done
Internet

http://192.168.168.168/

Name: admin

Password: ●●●●●●●●



http://192.168.168.168 - SonicWALL - Configuration Wizard - Microsoft Internet Explorer

Welcome to the SonicWALL Configuration Wizard

Select one of the wizards below to easily configure your SonicWALL:

● **Setup Wizard** - This wizard will help you quickly configure the SonicWALL to secure your Internet connection. Once completed, you can use the SonicWALL Web Management Interface for additional configuration.

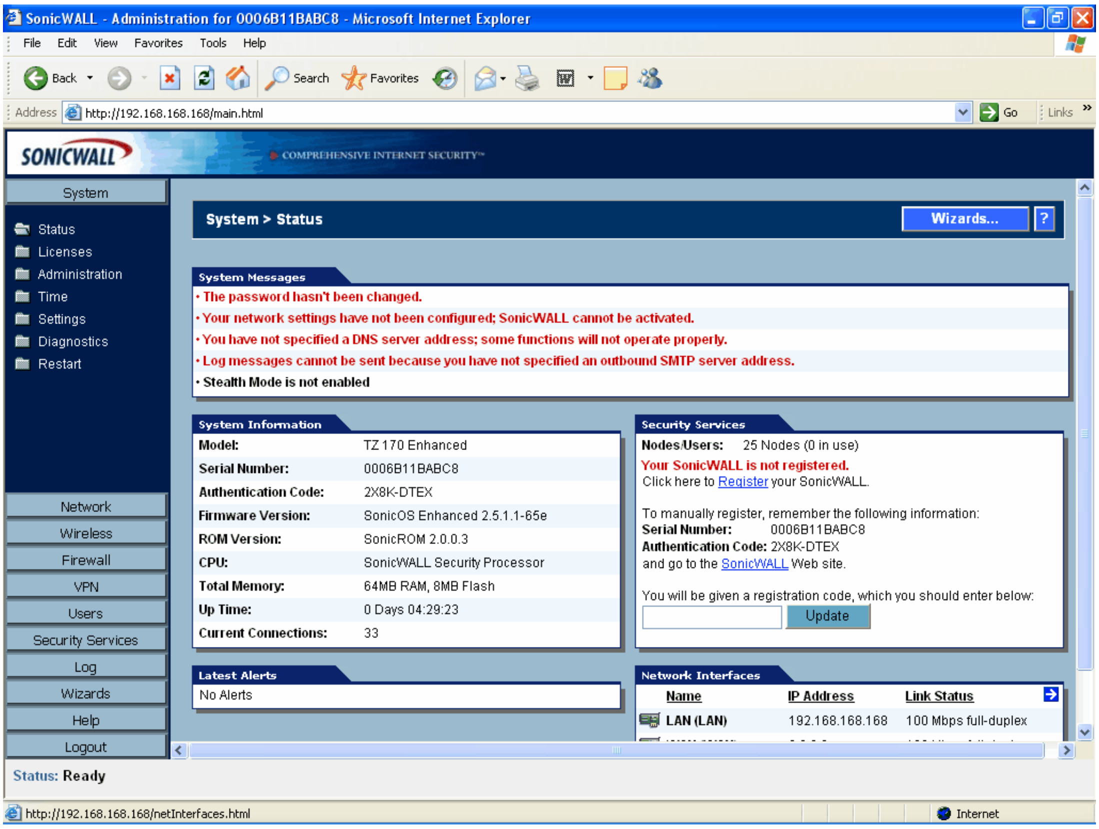
○ **Public Server Wizard** - This wizard will help you quickly configure your SonicWALL to provide public access to an internal server.

○ **VPN Wizard** - This wizard will help you create a new site-to-site VPN Policy or configure the WAN GroupVPN to accept connections from the SonicWALL Global VPN Client.

To continue, click Next.

The first time you configure your router, the GUI opens at the Configuration Wizard page.

After initial configuration, when you browse to the SonicWALL it may open at the System > Status page instead of the Configuration Wizard page.



SonicWALL - Administration for 0006B11BABC8 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address http://192.168.168.168/main.html
Go
Links
SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Status
Licenses
Administration
Time
Settings
Diagnostics
Restart
Network
Wireless
Firewall
VPN
Users
Security Services
Log
Wizards
Help
Logout
Wizards...
?

System > Status

System Messages

- The password hasn't been changed.
- Your network settings have not been configured; SonicWALL cannot be activated.
- You have not specified a DNS server address; some functions will not operate properly.
- Log messages cannot be sent because you have not specified an outbound SMTP server address.
- Stealth Mode is not enabled

System Information

Model:	TZ 170 Enhanced
Serial Number:	0006B11BABC8
Authentication Code:	2X8K-DTEX
Firmware Version:	SonicOS Enhanced 2.5.1.1-65e
ROM Version:	SonicROM 2.0.0.3
CPU:	SonicWALL Security Processor
Total Memory:	64MB RAM, 8MB Flash
Up Time:	0 Days 04:29:23
Current Connections:	33

Security Services

Nodes/Users: 25 Nodes (0 in use)

Your SonicWALL is not registered.
Click here to Register your SonicWALL.

To manually register, remember the following information:
Serial Number: 0006B11BABC8
Authentication Code: 2X8K-DTEX
and go to the SonicWALL Web site.

You will be given a registration code, which you should enter below:

Update

Latest Alerts

No Alerts

Network Interfaces

Name	IP Address	Link Status
LAN (LAN)	192.168.168.168	100 Mbps full-duplex

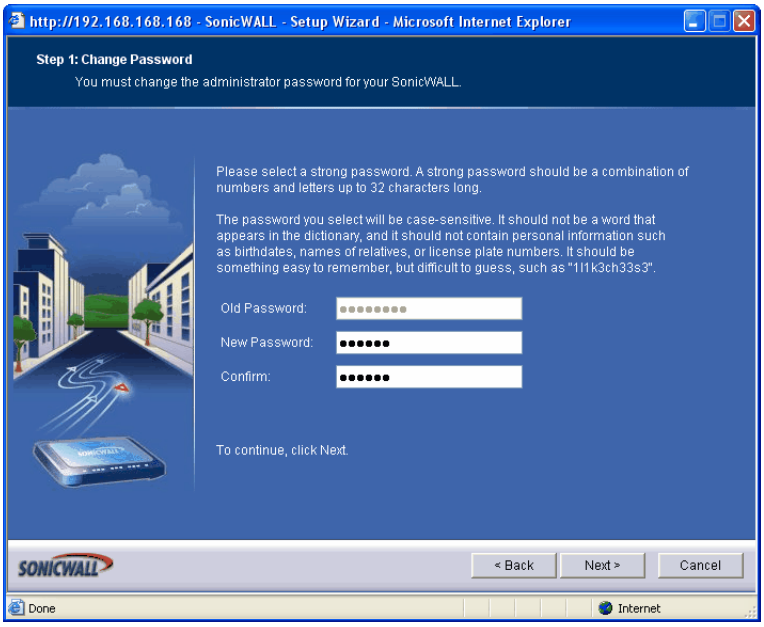
Status: Ready

Click on the Wizards button in the left-hand menu to open the Configuration Wizard page.

Customise the router and set up the network

The following steps use the Setup wizard to begin configuring your router.

1. Change the administrator password



http://192.168.168.168 - SonicWALL - Setup Wizard - Microsoft Internet Explorer

Step 1: Change Password

You must change the administrator password for your SonicWALL.

Please select a strong password. A strong password should be a combination of numbers and letters up to 32 characters long.

The password you select will be case-sensitive. It should not be a word that appears in the dictionary, and it should not contain personal information such as birthdates, names of relatives, or license plate numbers. It should be something easy to remember, but difficult to guess, such as "1l1k3ch33s3".

Old Password: ••••••••

New Password: ••••••

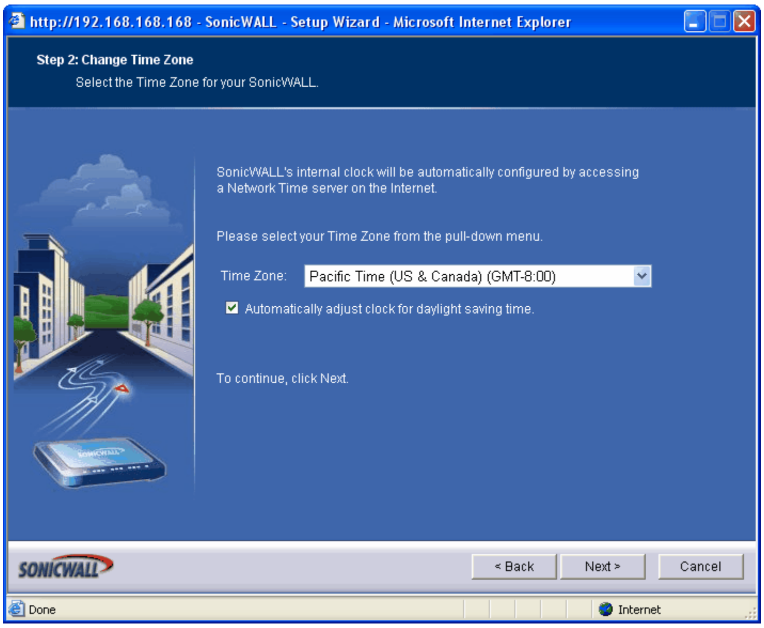
Confirm: ••••••

To continue, click Next.

The first action in the Setup wizard is to enter a suitable password for access to the GUI.

Click the Next button.

2. Set the time zone



http://192.168.168.168 - SonicWALL - Setup Wizard - Microsoft Internet Explorer

Step 2: Change Time Zone

Select the Time Zone for your SonicWALL.

SonicWALL's internal clock will be automatically configured by accessing a Network Time server on the Internet.

Please select your Time Zone from the pull-down menu.

Time Zone: Pacific Time (US & Canada) (GMT-8:00)

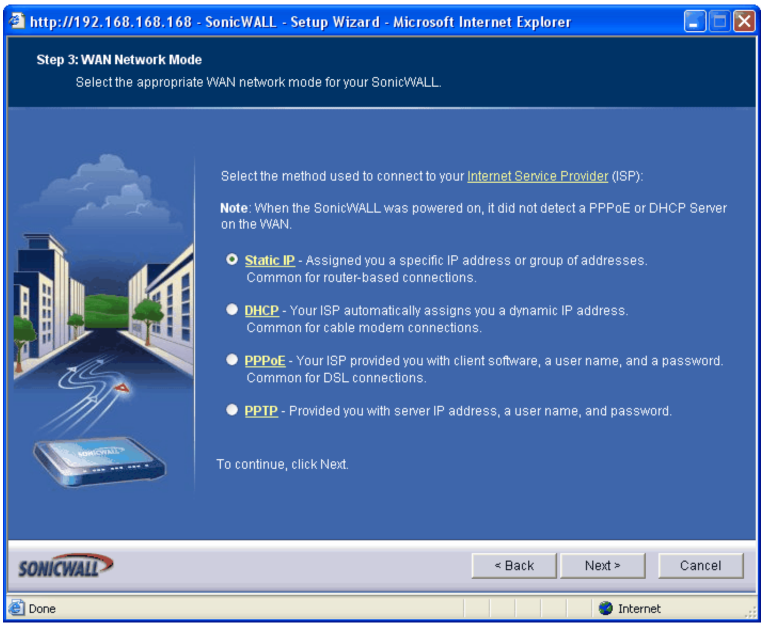
☑ Automatically adjust clock for daylight saving time.

To continue, click Next.

Select your time zone, and set the router to automatically adjust for summer time.

Click the Next button.

3. Choose the type of WAN address


http://192.168.168.168 - SonicWALL - Setup Wizard - Microsoft Internet Explorer
SONICWALL
< Back
Next >
Cancel
Done
Internet

Step 3: WAN Network Mode
Select the appropriate WAN network mode for your SonicWALL.

Select the method used to connect to your Internet Service Provider (ISP):

Note: When the SonicWALL was powered on, it did not detect a PPPoE or DHCP Server on the WAN.

● Static IP - Assigned you a specific IP address or group of addresses. Common for router-based connections.

○ DHCP - Your ISP automatically assigns you a dynamic IP address. Common for cable modem connections.

○ PPPoE - Your ISP provided you with client software, a user name, and a password. Common for DSL connections.

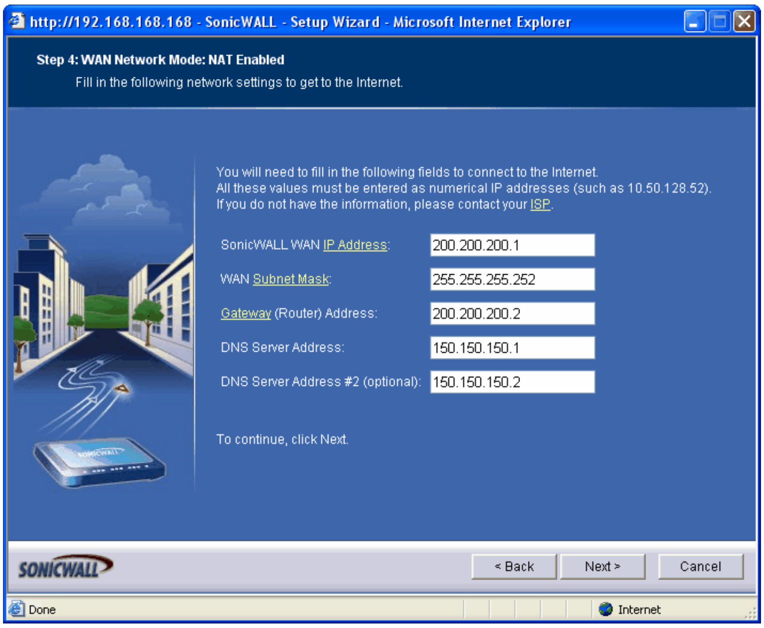
○ PPTP - Provided you with server IP address, a user name, and password.

To continue, click Next.

In this example, the SonicWALL router has a permanent fixed IP address, so select the Static IP option.

Then click the Next button.

4. Enter the WAN settings


http://192.168.168.168 - SonicWALL - Setup Wizard - Microsoft Internet Explorer
SONICWALL
< Back
Next >
Cancel
Done
Internet

Step 4: WAN Network Mode: NAT Enabled
Fill in the following network settings to get to the Internet.

You will need to fill in the following fields to connect to the Internet.
All these values must be entered as numerical IP addresses (such as 10.50.128.52).
If you do not have the information, please contact your ISP.

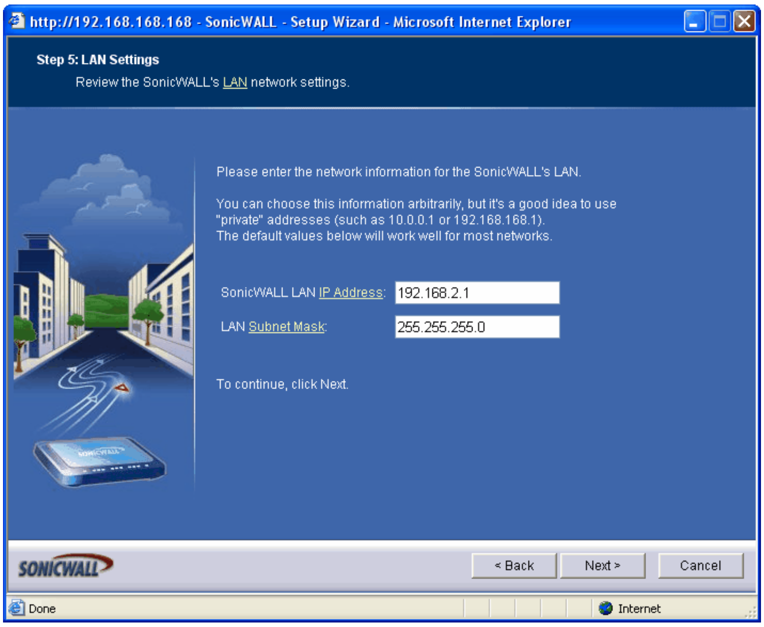
SonicWALL WAN IP Address: 200.200.200.1
WAN Subnet Mask: 255.255.255.252
Gateway (Router) Address: 200.200.200.2
DNS Server Address: 150.150.150.1
DNS Server Address #2 (optional): 150.150.150.2

To continue, click Next.

Enter the WAN interface's IP address and mask. For Gateway, enter the ISP's address (see "The network" on page 3). For DNS Server Address, enter the address of the DNS server that your router will access.

Then click the Next button.

5. Enter the LAN address


http://192.168.168.168 - SonicWALL - Setup Wizard - Microsoft Internet Explorer

Step 5: LAN Settings

Review the SonicWALL's LAN network settings.

Please enter the network information for the SonicWALL's LAN.

You can choose this information arbitrarily, but it's a good idea to use "private" addresses (such as 10.0.0.1 or 192.168.168.1). The default values below will work well for most networks.

SonicWALL LAN IP Address: 192.168.2.1

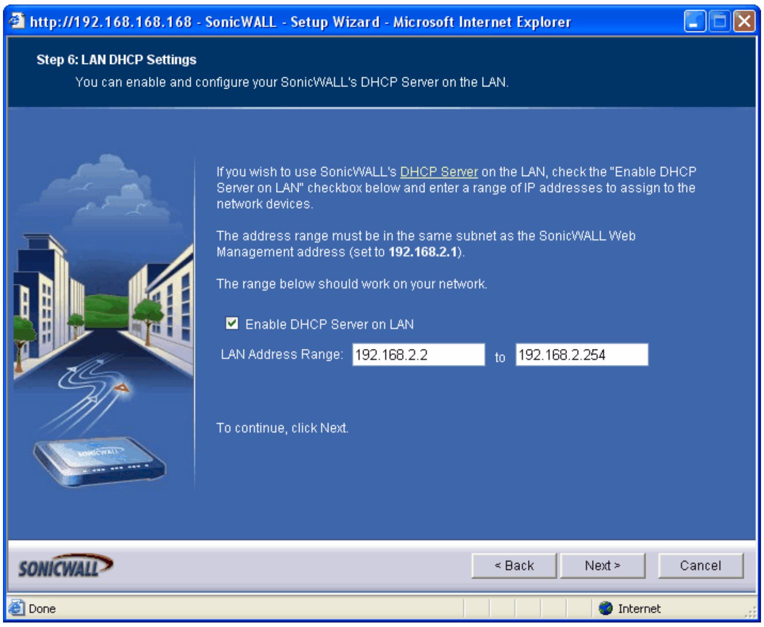
LAN Subnet Mask: 255.255.255.0

To continue, click Next.

Enter the IP address and mask of the SonicWALL's interface to the LAN.

Then click the Next button.

6. Set up the DHCP server


http://192.168.168.168 - SonicWALL - Setup Wizard - Microsoft Internet Explorer

Step 6: LAN DHCP Settings

You can enable and configure your SonicWALL's DHCP Server on the LAN.

If you wish to use SonicWALL's DHCP Server on the LAN, check the "Enable DHCP Server on LAN" checkbox below and enter a range of IP addresses to assign to the network devices.

The address range must be in the same subnet as the SonicWALL Web Management address (set to **192.168.2.1**).

The range below should work on your network.

☑ Enable DHCP Server on LAN

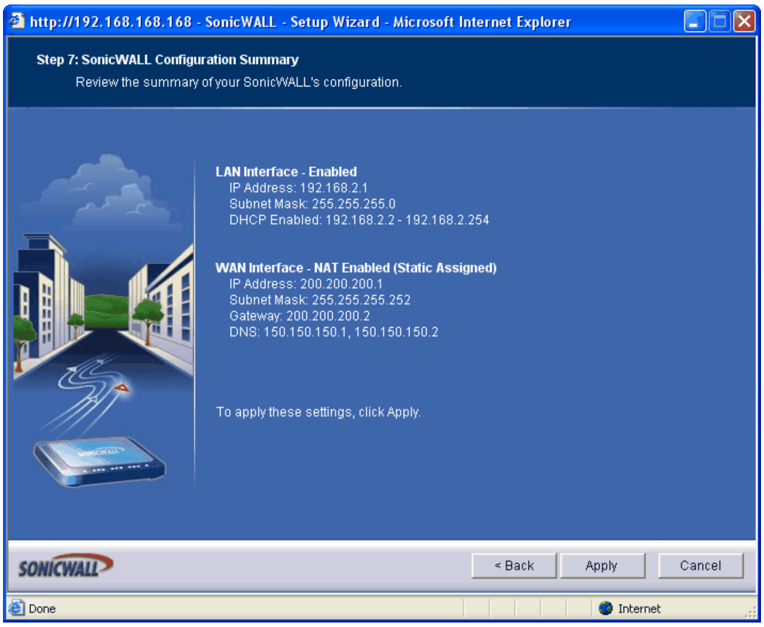
LAN Address Range: 192.168.2.2 to 192.168.2.254

To continue, click Next.

In this step, you can set up the DHCP server on this router to service the office LAN you intend to connect to. Check that the wizard has chosen an appropriate range of addresses.

Then click the Next button.

7. Check the settings


http://192.168.168.168 - SonicWALL - Setup Wizard - Microsoft Internet Explorer

Step 7: SonicWALL Configuration Summary

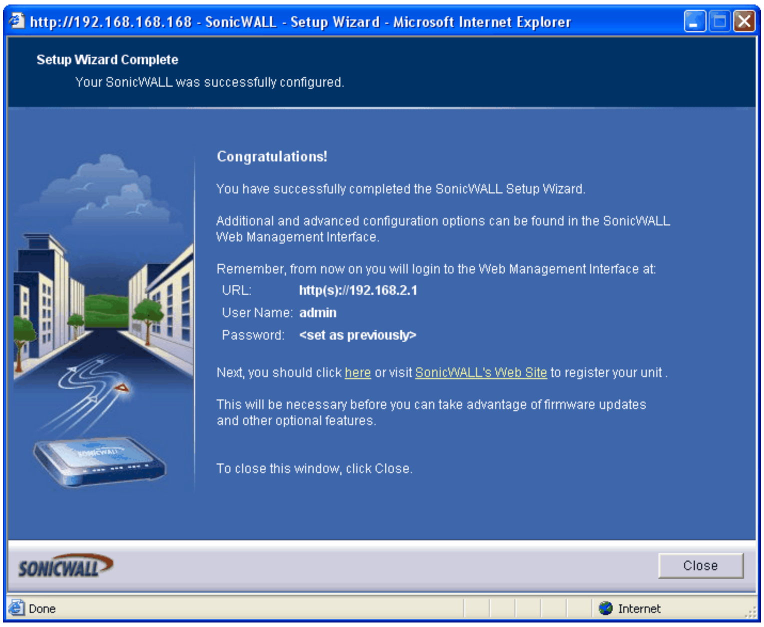
Review the summary of your SonicWALL's configuration.

LAN Interface - Enabled
IP Address: 192.168.2.1
Subnet Mask: 255.255.255.0
DHCP Enabled: 192.168.2.2 - 192.168.2.254

WAN Interface - NAT Enabled (Static Assigned)
IP Address: 200.200.200.1
Subnet Mask: 255.255.255.252
Gateway: 200.200.200.2
DNS: 150.150.150.1, 150.150.150.2

To apply these settings, click Apply.

Check the summary. If necessary, use the Back button to return and correct any settings you want to change.


http://192.168.168.168 - SonicWALL - Setup Wizard - Microsoft Internet Explorer

Setup Wizard Complete

Your SonicWALL was successfully configured.

Congratulations!

You have successfully completed the SonicWALL Setup Wizard.

Additional and advanced configuration options can be found in the SonicWALL Web Management Interface.

Remember, from now on you will login to the Web Management Interface at:
URL: **http(s)://192.168.2.1**
User Name: **admin**
Password: **<set as previously>**

Next, you should click here or visit SonicWALL's Web Site to register your unit .

This will be necessary before you can take advantage of firmware updates and other optional features.

To close this window, click Close.

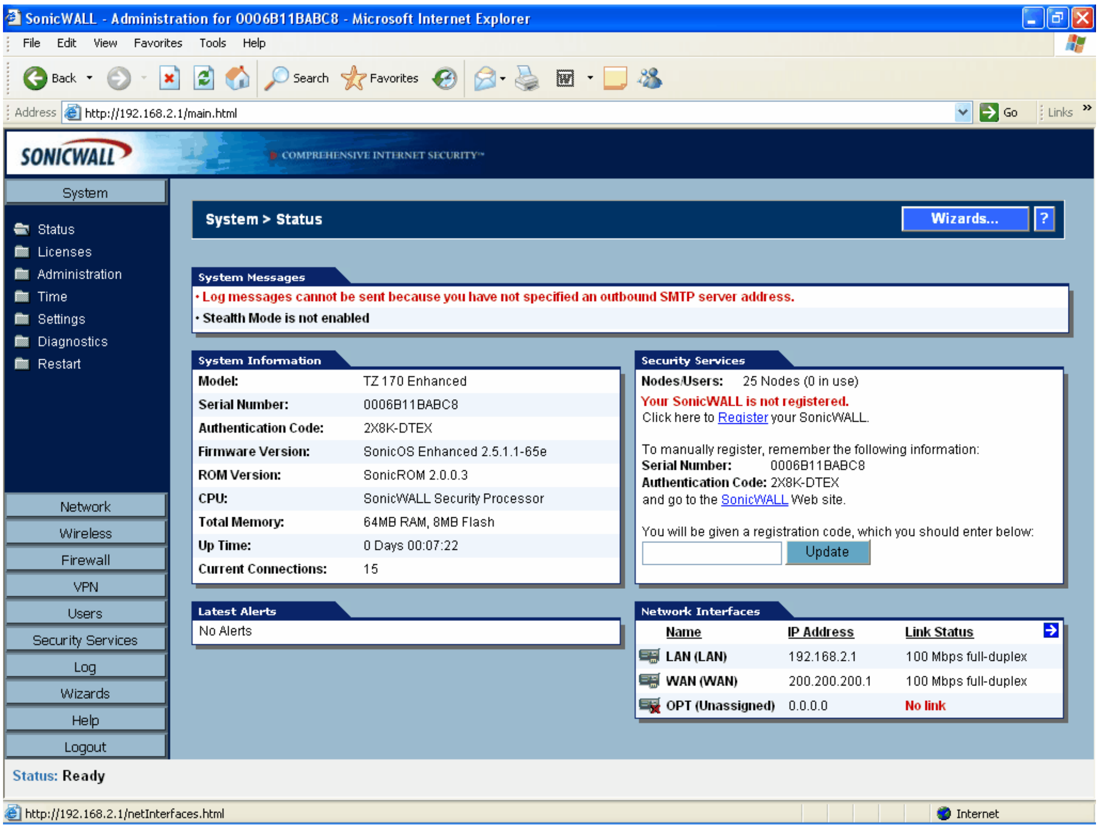
When all the settings are correct, click the Apply button. The wizard displays a message of congratulations.

Click the Close button.

8. Log in again

If you changed the router's LAN IP address, you need to change the PC's address. If you turned on the router's DHCP server, set the PC to obtain its address automatically. Otherwise, give the PC an address in the new subnet. You may need to restart the SonicWALL router to force it to assign an IP address to the PC.

Browse to the router's new address and log in. The GUI displays the System > Status page.


SonicWALL - Administration for 0006B11BABC8 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.2.1/main.html
Go Links
SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Status
Licenses
Administration
Time
Settings
Diagnostics
Restart
Network
Wireless
Firewall
VPN
Users
Security Services
Log
Wizards
Help
Logout
Wizards...
?
http://192.168.2.1/netInterfaces.html
Internet

System > Status

System Messages

- Log messages cannot be sent because you have not specified an outbound SMTP server address.
- Stealth Mode is not enabled

System Information

Model:	TZ 170 Enhanced
Serial Number:	0006B11BABC8
Authentication Code:	2X8K-DTEX
Firmware Version:	SonicOS Enhanced 2.5.1.1-65e
ROM Version:	SonicROM 2.0.0.3
CPU:	SonicWALL Security Processor
Total Memory:	64MB RAM, 8MB Flash
Up Time:	0 Days 00:07:22
Current Connections:	15

Security Services

Nodes/Users: 25 Nodes (0 in use)

Your SonicWALL is not registered.
Click here to Register your SonicWALL.

To manually register, remember the following information:
Serial Number: 0006B11BABC8
Authentication Code: 2X8K-DTEX
and go to the SonicWALL Web site.

You will be given a registration code, which you should enter below:

Update

Latest Alerts

No Alerts

Network Interfaces

Name	IP Address	Link Status
LAN (LAN)	192.168.2.1	100 Mbps full-duplex
WAN (WAN)	200.200.200.1	100 Mbps full-duplex
OPT (Unassigned)	0.0.0.0	No link

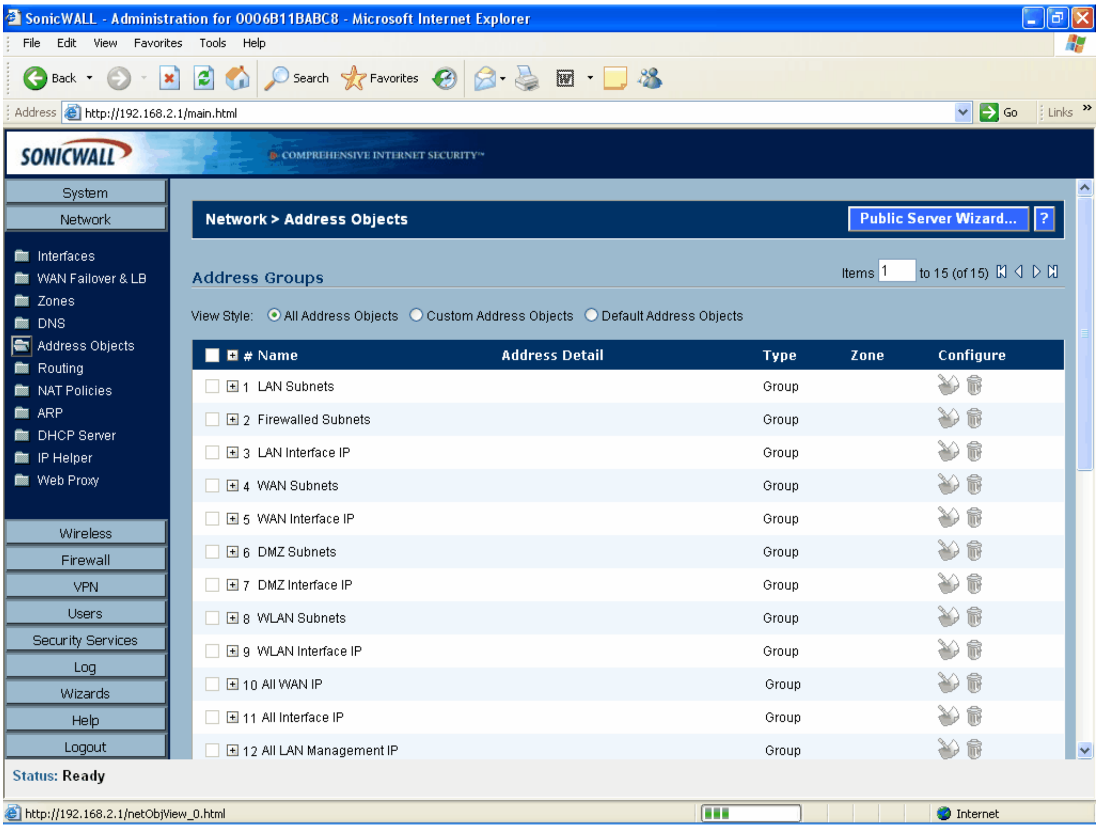
Status: Ready

Define the LAN subnet of the peer

Before you can configure the VPN, you need to create an address "object". The address object defines the LAN subnet of the VPN peer router—in this example, the Allied Telesis router. There is no wizard for creating the address object, so the following steps use the Network pages instead.

1. Open the Address Objects summary

In the left-hand menu of the System > Status page, select Network, then Address Objects. The GUI displays a list of all the existing address objects.



Network > Address Objects

Address Groups

Items 1 to 15 (of 15)

View Style: ● All Address Objects ○ Custom Address Objects ○ Default Address Objects

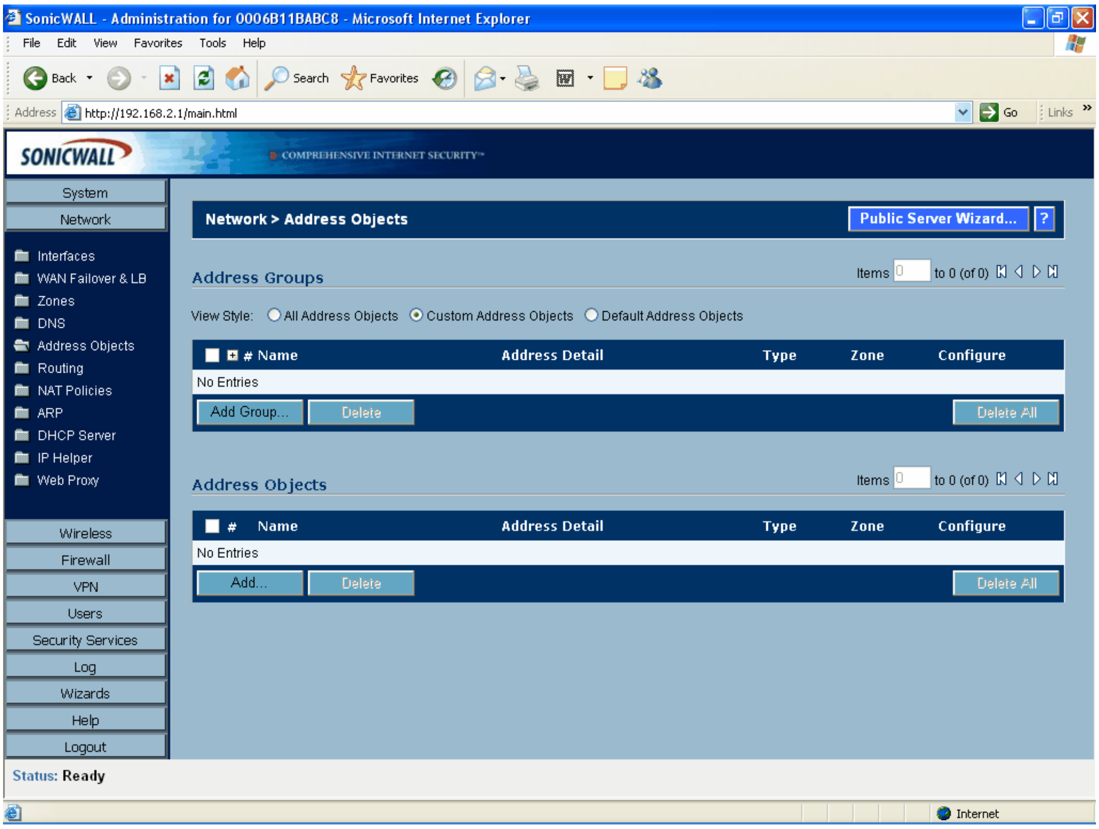
# Name	Address Detail	Type	Zone	Configure
1 LAN Subnets		Group		
2 Firewalled Subnets		Group		
3 LAN Interface IP		Group		
4 WAN Subnets		Group		
5 WAN Interface IP		Group		
6 DMZ Subnets		Group		
7 DMZ Interface IP		Group		
8 WLAN Subnets		Group		
9 WLAN Interface IP		Group		
10 All WAN IP		Group		
11 All Interface IP		Group		
12 All LAN Management IP		Group		

Status: Ready

http://192.168.2.1/netObjView_0.html

2. Open the Custom Address Objects summary

Select the “Custom Address Objects” view style, which displays lists of Address Groups and Address Objects.



Network > Address Objects

Address Groups Items 0 to 0 (of 0)

View Style: ○ All Address Objects ● Custom Address Objects ○ Default Address Objects

□ # Name	Address Detail	Type	Zone	Configure
No Entries				

Add Group... Delete Delete All

Address Objects Items 0 to 0 (of 0)

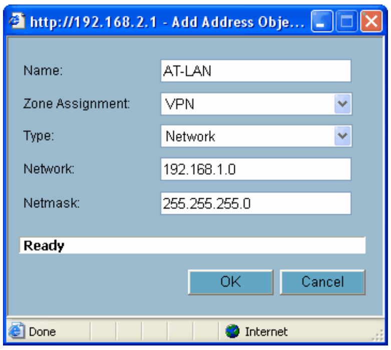
□ # Name	Address Detail	Type	Zone	Configure
No Entries				

Add... Delete Delete All

Status: Ready

There will be no custom address objects defined yet, so both the Address Groups and Address Objects lists are empty. In Address Objects (the bottom section of the window), click the Add button.

3. Define the address object



Name:	AT-LAN
Zone Assignment:	VPN
Type:	Network
Network:	192.168.1.0
Netmask:	255.255.255.0

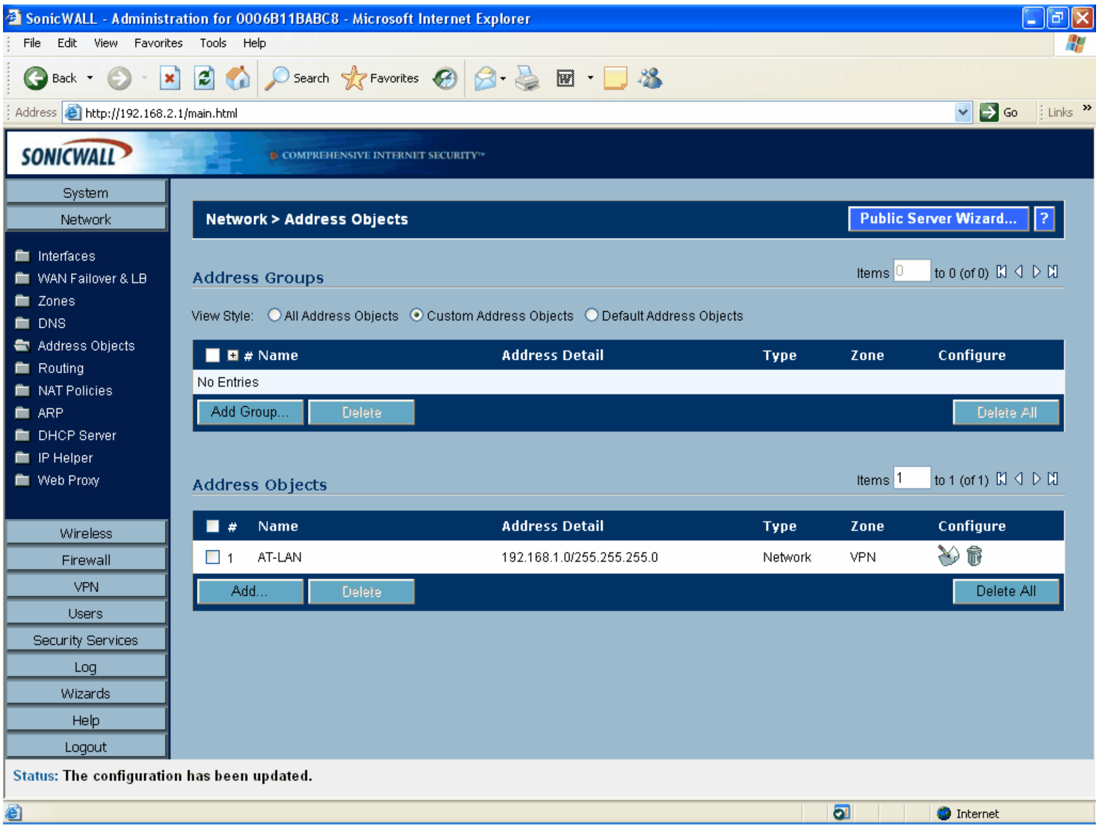
Ready

Enter the address object settings: the appropriate network (see "The network" on page 3), and other settings as shown in the following screenshot. The address object describes the LAN that is connected to the Allied Telesis router.

Click the OK button to display the Custom Address Objects summary page again.

4. Check the settings

Check that the object is correct. If you need to change the object, click on the icon of a note and pencil at the right of the object's entry.



Network > Address Objects

Address Groups — Items 0 to 0 (of 0)

View Style: ○ All Address Objects ● Custom Address Objects ○ Default Address Objects

# Name	Address Detail	Type	Zone	Configure
No Entries				

Add Group... Delete Delete All

Address Objects — Items 1 to 1 (of 1)

	#	Name	Address Detail	Type	Zone	Configure
□	1	AT-LAN	192.168.1.0/255.255.255.0	Network	VPN	

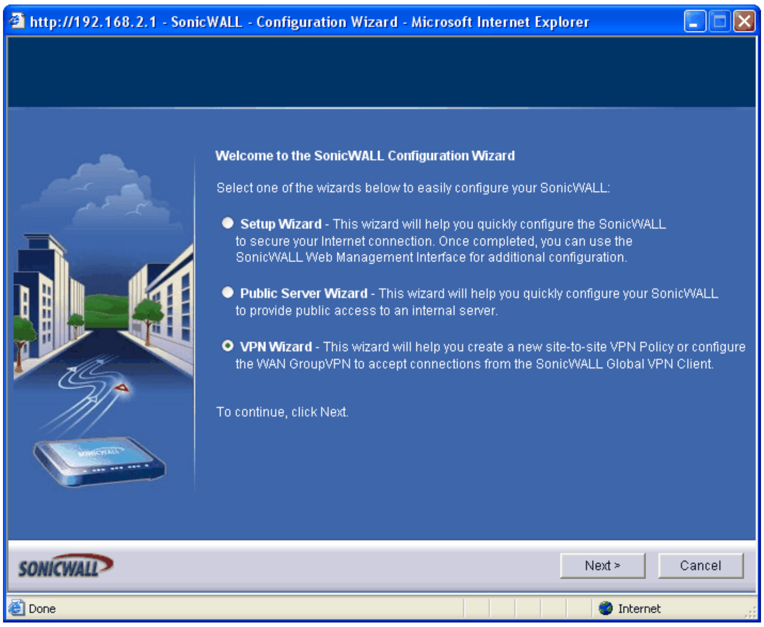
Add... Delete Delete All

Status: The configuration has been updated.

Create the VPN

The following steps use the VPN wizard to create the SonicWALL end of the VPN.

1. Return to the Configuration Wizards page



http://192.168.2.1 - SonicWALL - Configuration Wizard - Microsoft Internet Explorer

Welcome to the SonicWALL Configuration Wizard

Select one of the wizards below to easily configure your SonicWALL:

○ **Setup Wizard** - This wizard will help you quickly configure the SonicWALL to secure your Internet connection. Once completed, you can use the SonicWALL Web Management Interface for additional configuration.

○ **Public Server Wizard** - This wizard will help you quickly configure your SonicWALL to provide public access to an internal server.

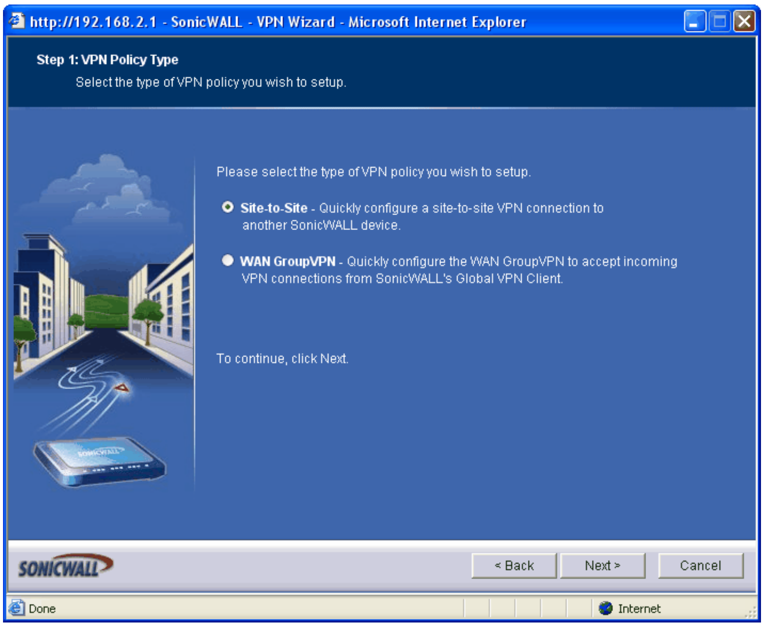
● **VPN Wizard** - This wizard will help you create a new site-to-site VPN Policy or configure the WAN GroupVPN to accept connections from the SonicWALL Global VPN Client.

To continue, click Next.

Click on the Wizards button in the left-hand menu to open the Configuration Wizard page, then select the VPN wizard.

Click the Next button.

2. Start the Site-to-Site VPN wizard



http://192.168.2.1 - SonicWALL - VPN Wizard - Microsoft Internet Explorer

Step 1: VPN Policy Type

Select the type of VPN policy you wish to setup.

Please select the type of VPN policy you wish to setup.

● **Site-to-Site** - Quickly configure a site-to-site VPN connection to another SonicWALL device.

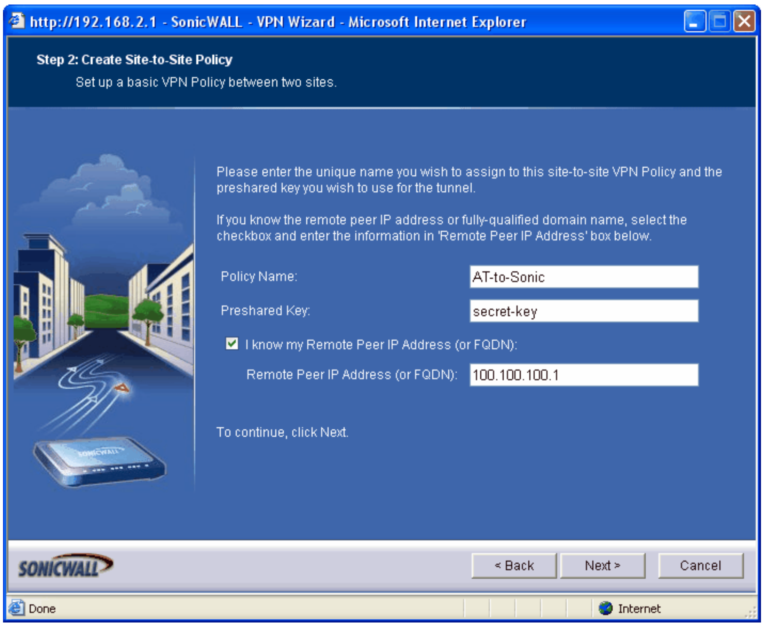
○ **WAN GroupVPN** - Quickly configure the WAN GroupVPN to accept incoming VPN connections from SonicWALL's Global VPN Client.

To continue, click Next.

Select the Site-to-Site option.

Click the Next button.

3. Create the Site-to-Site policy


http://192.168.2.1 - SonicWALL - VPN Wizard - Microsoft Internet Explorer

Step 2: Create Site-to-Site Policy

Set up a basic VPN Policy between two sites.

Please enter the unique name you wish to assign to this site-to-site VPN Policy and the preshared key you wish to use for the tunnel.

If you know the remote peer IP address or fully-qualified domain name, select the checkbox and enter the information in 'Remote Peer IP Address' box below.

Policy Name: AT-to-Sonic

Preshared Key: secret-key

☑ I know my Remote Peer IP Address (or FQDN):

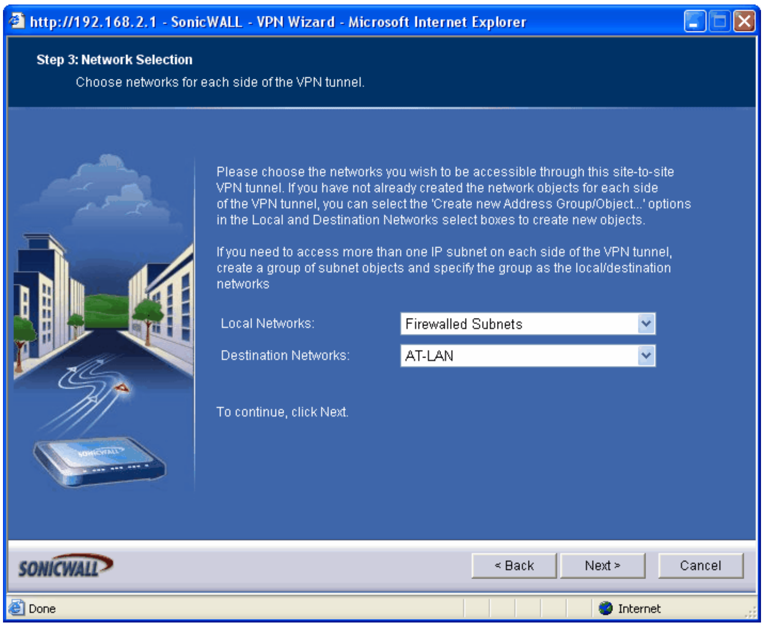
Remote Peer IP Address (or FQDN): 100.100.100.1

To continue, click Next.

Name the policy. Enter the pre-shared key, which must be the same as the Allied Telesis router's secret key. Enter the remote peer address, which is the SonicWALL-facing side of the NAT device in this example (see "The network" on page 3).

Click the Next button.

4. Select the networks for each end of the LAN


http://192.168.2.1 - SonicWALL - VPN Wizard - Microsoft Internet Explorer

Step 3: Network Selection

Choose networks for each side of the VPN tunnel.

Please choose the networks you wish to be accessible through this site-to-site VPN tunnel. If you have not already created the network objects for each side of the VPN tunnel, you can select the 'Create new Address Group/Object...' options in the Local and Destination Networks select boxes to create new objects.

If you need to access more than one IP subnet on each side of the VPN tunnel, create a group of subnet objects and specify the group as the local/destination networks

Local Networks: Firewalled Subnets

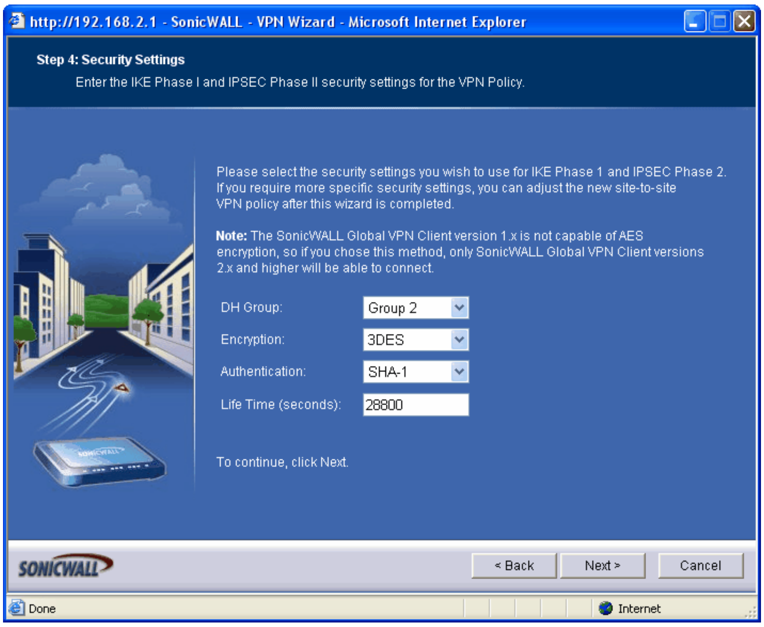
Destination Networks: AT-LAN

To continue, click Next.

For the local (SonicWALL) end, select Firewalled Subnets. For the destination (Allied Telesis) end, select the address object that you created in "Define the LAN subnet of the peer" on page 20.

Click the Next button.

5. Specify security settings


http://192.168.2.1 - SonicWALL - VPN Wizard - Microsoft Internet Explorer
< Back
Next >
Cancel
SONICWALL
Done
Internet

Step 4: Security Settings

Enter the IKE Phase I and IPSEC Phase II security settings for the VPN Policy.

Please select the security settings you wish to use for IKE Phase 1 and IPSEC Phase 2. If you require more specific security settings, you can adjust the new site-to-site VPN policy after this wizard is completed.

Note: The SonicWALL Global VPN Client version 1.x is not capable of AES encryption, so if you chose this method, only SonicWALL Global VPN Client versions 2.x and higher will be able to connect.

DH Group: Group 2

Encryption: 3DES

Authentication: SHA-1

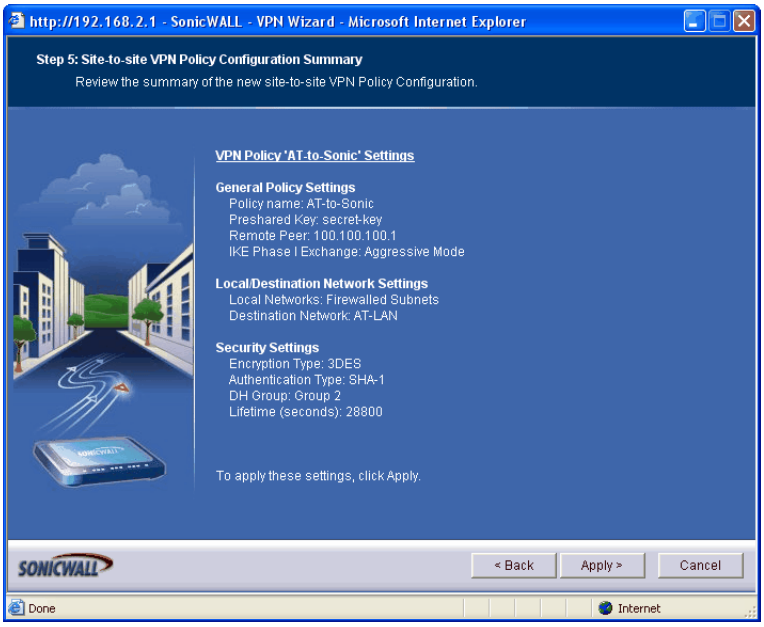
Life Time (seconds): 28800

To continue, click Next.

You do not need to modify the default security settings.

Click the Next button.

6. Check the settings


http://192.168.2.1 - SonicWALL - VPN Wizard - Microsoft Internet Explorer
< Back
Apply >
Cancel
SONICWALL
Done
Internet

Step 5: Site-to-site VPN Policy Configuration Summary

Review the summary of the new site-to-site VPN Policy Configuration.

VPN Policy 'AT-to-Sonic' Settings

General Policy Settings
Policy name: AT-to-Sonic
Preshared Key: secret-key
Remote Peer: 100.100.100.1
IKE Phase I Exchange: Aggressive Mode

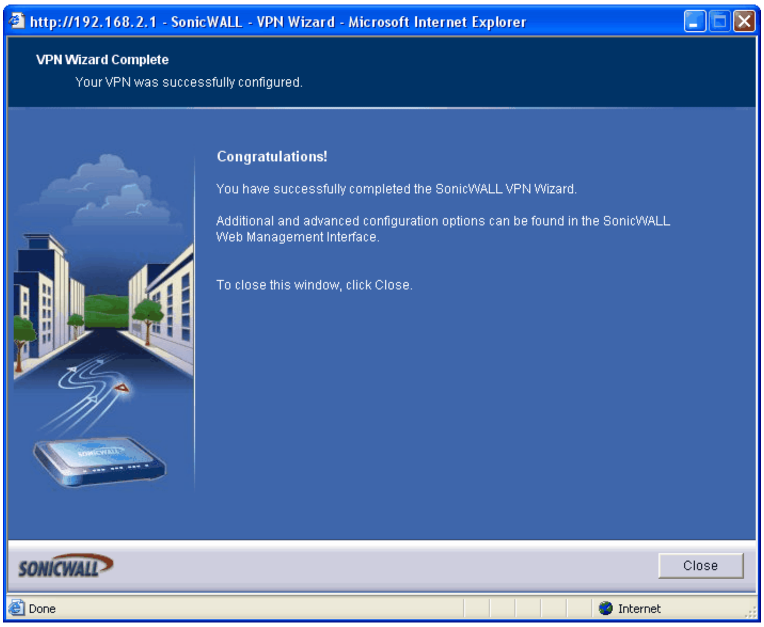
Local/Destination Network Settings
Local Networks: Firewalled Subnets
Destination Network: AT-LAN

Security Settings
Encryption Type: 3DES
Authentication Type: SHA-1
DH Group: Group 2
Lifetime (seconds): 28800

To apply these settings, click Apply.

Check the summary. If necessary, use the Back button to return and correct any settings you want to change.

When all the settings are correct, click the Apply button.


http://192.168.2.1 - SonicWALL - VPN Wizard - Microsoft Internet Explorer
SONICWALL
Close
Done
Internet

VPN Wizard Complete

Your VPN was successfully configured.

Congratulations!

You have successfully completed the SonicWALL VPN Wizard.

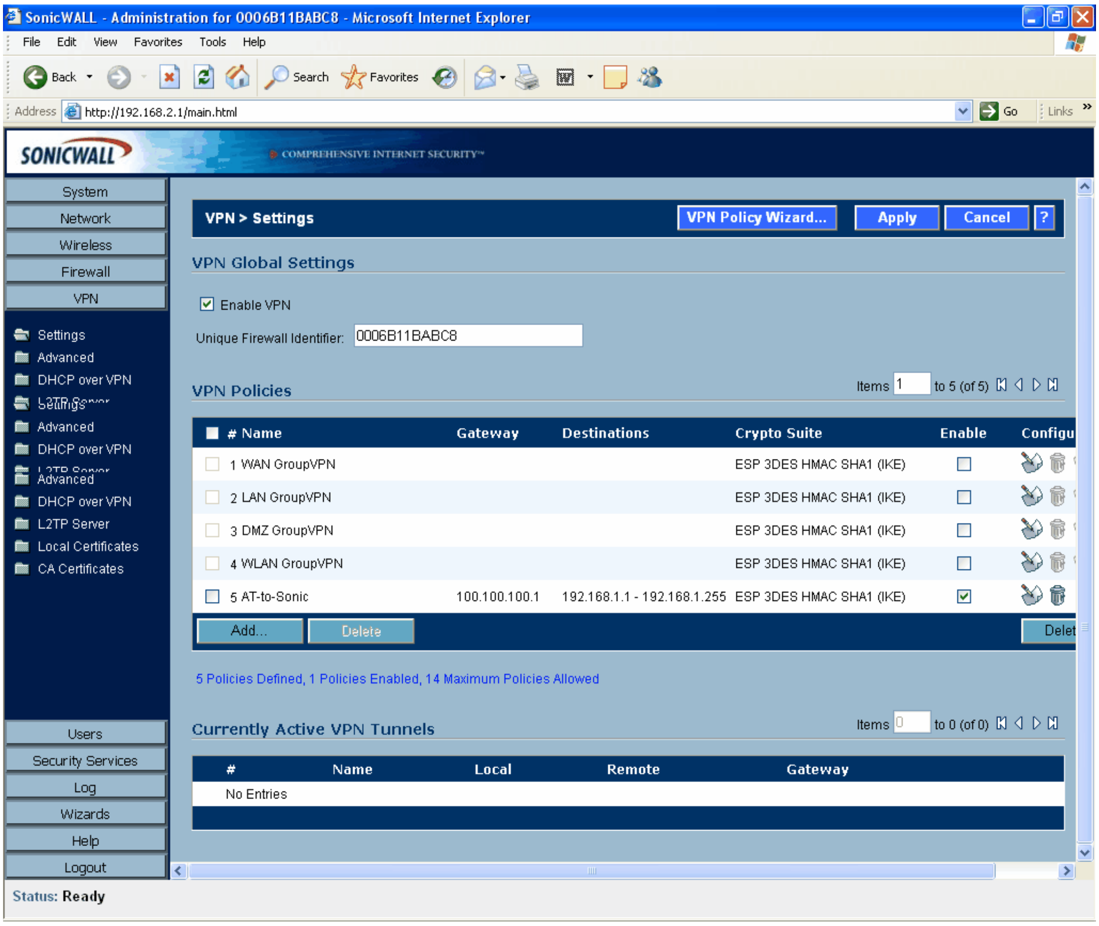
Additional and advanced configuration options can be found in the SonicWALL Web Management Interface.

To close this window, click Close.

The wizard displays a message of congratulations.

Click the Close button.

The GUI displays the VPN > Settings page.



VPN > Settings

VPN Global Settings

☑ Enable VPN

Unique Firewall Identifier: 0006B11BABC8

VPN Policies

Items 1 to 5 (of 5)

#	Name	Gateway	Destinations	Crypto Suite	Enable	Configu
1	WAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)	□	
2	LAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)	□	
3	DMZ GroupVPN			ESP 3DES HMAC SHA1 (IKE)	□	
4	WLAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)	□	
5	AT-to-Sonic	100.100.100.1	192.168.1.1 - 192.168.1.255	ESP 3DES HMAC SHA1 (IKE)	☑	

5 Policies Defined, 1 Policies Enabled, 14 Maximum Policies Allowed

Currently Active VPN Tunnels

Items 0 to 0 (of 0)

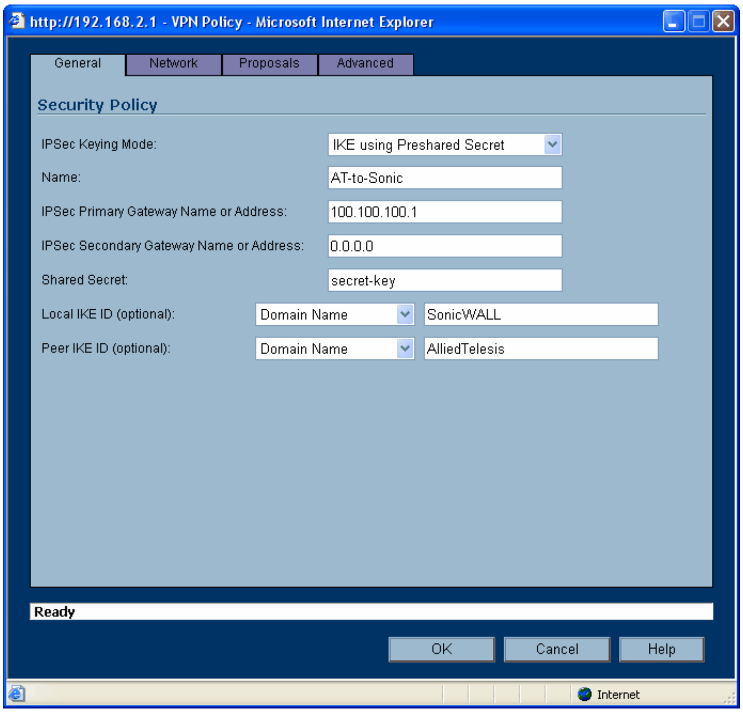
#	Name	Local	Remote	Gateway
No Entries				

Set the VPN IKE IDs and use Main Mode

Solutions with a NAT device in the tunnel path need to have IKE IDs specified. For all solutions, we recommend using Main mode instead of the default Aggressive mode. This section describes how to set both of these.

1. Specify the Local and Peer IKE IDs

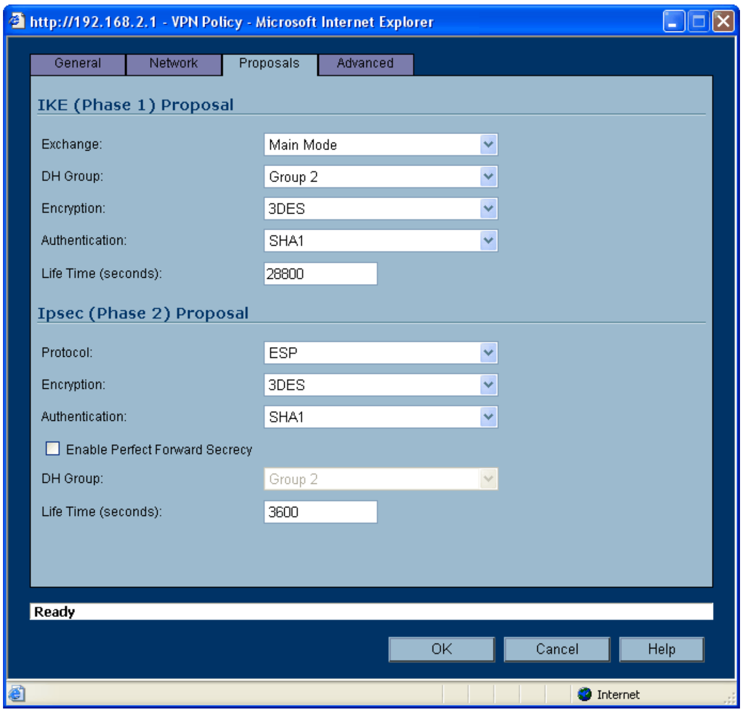
On the VPN > Settings page, click on the icon of a note and pencil at the right of the AlliedTelesis policy's entry. The VPN policy dialog box opens.



IPSec Keying Mode:	IKE using Preshared Secret	
Name:	AT-to-Sonic	
IPSec Primary Gateway Name or Address:	100.100.100.1	
IPSec Secondary Gateway Name or Address:	0.0.0.0	
Shared Secret:	secret-key	
Local IKE ID (optional):	Domain Name	SonicWALL
Peer IKE ID (optional):	Domain Name	AlliedTelesis

On the General tab, enter the Local and Peer IKE IDs. Select "type" of Domain Name. The values do not have to be real domain names, but must match the values on your Allied Telesis router (remember that "local" on the SonicWALL is "remote" on the Allied Telesis, and so on).

2. Specify IKE Main Mode


http://192.168.2.1 - VPN Policy - Microsoft Internet Explorer
General
Network
Proposals
Advanced
OK
Cancel
Help
Internet

IKE (Phase 1) Proposal

Exchange: Main Mode

DH Group: Group 2

Encryption: 3DES

Authentication: SHA1

Life Time (seconds): 28800

Ipsec (Phase 2) Proposal

Protocol: ESP

Encryption: 3DES

Authentication: SHA1

☐ Enable Perfect Forward Secrecy

DH Group: Group 2

Life Time (seconds): 3600

Ready

Click on the Proposals tab. Set Exchange to Main Mode. This is the preferred mode because it is more secure.

We also recommend that you change the lifetime for the IPsec (Phase2) Proposal to 3600 seconds, to match the Allied Telesis router.

Click OK.

3. If necessary, restart the router

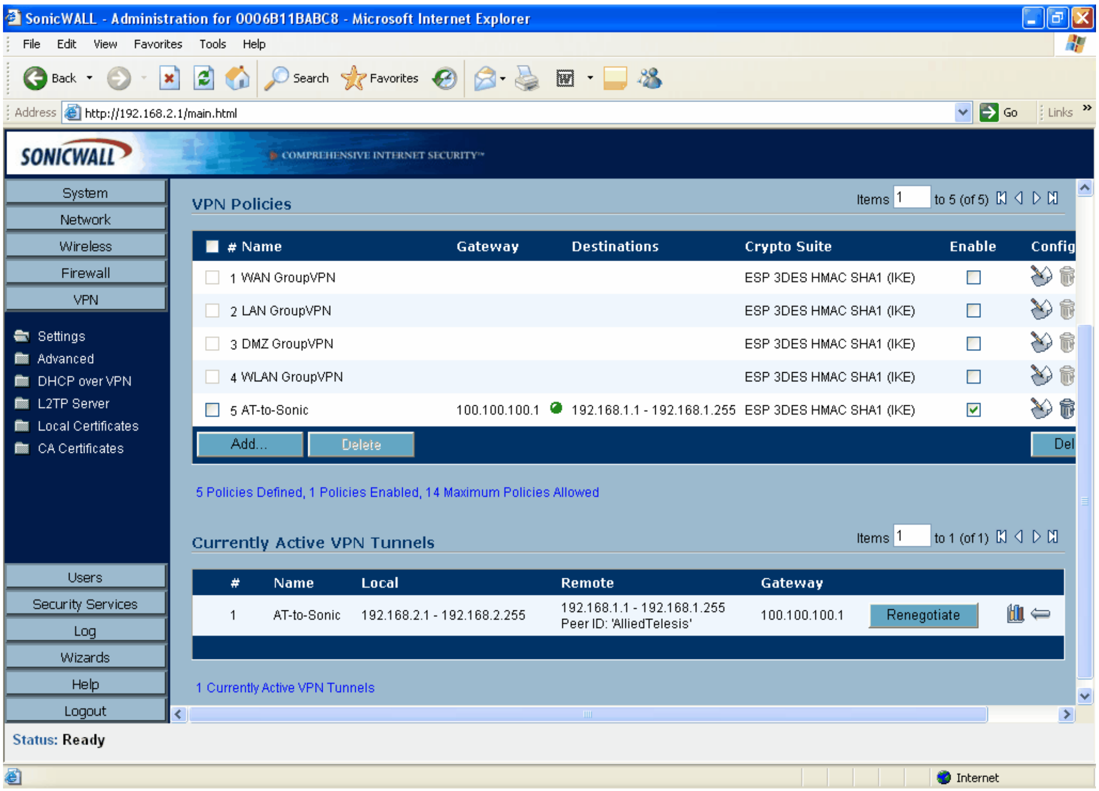
You may find that you need to restart the router to allow all changes to take effect. To do this, select System > Restart from the left-hand menu.

How to test the tunnel

There are several options for testing the tunnel. If these checks show that your tunnel is not working, see the How To Note *How To Troubleshoot A Virtual Private Network (VPN)*.

1. Check the tunnel status

On the SonicWALL router's VPN > Settings page, look for a green dot in the VPN policy entry, and for an entry in the "Currently Active VPN Tunnels" section.



VPN Policies

Items 1 to 5 (of 5)

# Name	Gateway	Destinations	Crypto Suite	Enable	Config
1 WAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)	☐	
2 LAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)	☐	
3 DMZ GroupVPN			ESP 3DES HMAC SHA1 (IKE)	☐	
4 WLAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)	☐	
5 AT-to-Sonic	100.100.100.1 ●	192.168.1.1 - 192.168.1.255	ESP 3DES HMAC SHA1 (IKE)	☑	

5 Policies Defined, 1 Policies Enabled, 14 Maximum Policies Allowed

Currently Active VPN Tunnels

Items 1 to 1 (of 1)

#	Name	Local	Remote	Gateway
1	AT-to-Sonic	192.168.2.1 - 192.168.2.255	192.168.1.1 - 192.168.1.255 Peer ID: 'AlliedTelesis'	100.100.100.1

1 Currently Active VPN Tunnels

Status: Ready

2. Ping the SonicWALL LAN

From the PC attached to the Allied Telesis router, ping the PC attached to the SonicWALL router, or the SonicWALL router's LAN address.

Note that when a NAT device is in the VPN path you can only initiate the tunnel from the router behind the NAT device, unless you create a suitable pinhole on the NAT device. In this example, that means you cannot ping from the SonicWALL end of the tunnel to the Allied Telesis end (unless you first ping in the other direction).

How to use the CLI instead of the GUI

This section gives an example of the Allied Telesis CLI commands that you need to enter for the IP, firewall, IPsec and ISAKMP aspects of this configuration.

```
# IP configuration
enable ip
add ip int=vlan1 ip=192.168.1.1
add ip int=eth0 ip=192.168.254.1 mask=255.255.255.252
add ip rou=0.0.0.0 mask=0.0.0.0 int=eth0 next=192.168.254.2

# Firewall configuration
enable firewall
create firewall policy=guilan
enable firewall policy=guilan icmp_f=ping
add firewall policy=guilan int=vlan1 type=private
add firewall policy=guilan int=eth0 type=public
add firewall poli=guilan nat=enhanced int=vlan1 gblint=eth0
add firewall poli=guilan rule=1 action=allow int=eth0 protocol=udp port=500
   ip=192.168.254.1 gblip=192.168.254.1 gblport=500
add firewall poli=guilan rule=2 action=allow int=eth0 protocol=udp port=4500
   ip=192.168.254.1 gblip=192.168.254.1 gblport=4500
add firewall poli=guilan rule=3 action=nonat int=eth0 protocol=ALL
   encap=ipsec
add firewall poli=guilan rule=4 action=nonat int=vlan1 protocol=ALL
   ip=192.168.1.1-192.168.1.254
set firewall poli=guilan rule=4 remote=192.168.2.1-192.168.2.254

# IPSEC configuration
create ipsec saspec=0 key=isakmp protocol=esp encalg=3desouter hashalg=sha
set ipsec saspec=0 antireplay=true
create ipsec bundle=0 key=isakmp string="0" expirysec=3600
create ipsec policy=eth0allowISAKMP int=eth0 action=permit
set ipsec policy=eth0allowISAKMP lport=500 transportprotocol=UDP
create ipsec policy=eth0allowISAKMPF int=eth0 action=permit
set ipsec policy=eth0allowISAKMPF lport=4500
create ipsec policy=wiz_AT-to-Sonic int=eth0 action=ipsec key=isakmp bundle=0
   peer=200.200.200.1 isakmp=wiz_AT-to-Sonic
set ipsec policy=wiz_AT-to-Sonic laddress=192.168.1.0 lmask=255.255.255.0
   raddress=192.168.2.0 rmask=255.255.255.0
set ipsec policy=wiz_AT-to-Sonic respondbadspi=TRUE
create ipsec policy=eth0allow int=eth0 action=permit
enable ipsec

# ISAKMP configuration
create isakmp policy=wiz_AT-to-Sonic peer=200.200.200.1 encalg=3desouter
   key=0 natt=true
set isakmp policy=wiz_AT-to-Sonic expirysec=28800 group=2
set isakmp policy=wiz_AT-to-Sonic sendd=true sendn=true
set isakmp policy=wiz_AT-to-Sonic localid="AlliedTelesis" remotei="SonicWALL"
enable isakmp
```

Appendix: Using this example if you don't have a NAT device in the same position

You can still use this example if you have no NAT device between the Allied Telesis router and the Internet, or if you have a NAT device between the SonicWALL router and the Internet. Simply change the peer addresses that you enter into the wizards, in the following ways:

If you have...	**in the Allied Telesis VPN wizard, for Remote Site Public IP Address, enter...**	**in the SonicWALL VPN wizard, for Remote Peer IP Address, enter...**
no NAT devices in the path of the VPN	the SonicWALL router's public-side address	the Allied Telesis router's public-side address
the SonicWALL router behind a NAT device instead of the Allied Telesis router	the NAT device's public-side address	the Allied Telesis router's public-side address
both routers behind a NAT device	the public-side address of the NAT device in front of the SonicWALL router	the public-side address of the NAT device in front of the Allied Telesis router

USA Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
European Headquarters | Via Motta 24 | 6830 Chiasso | Switzerland | T: +41 91 69769.00 | F: +41 91 69769.11
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
www.alliedtelesis.com