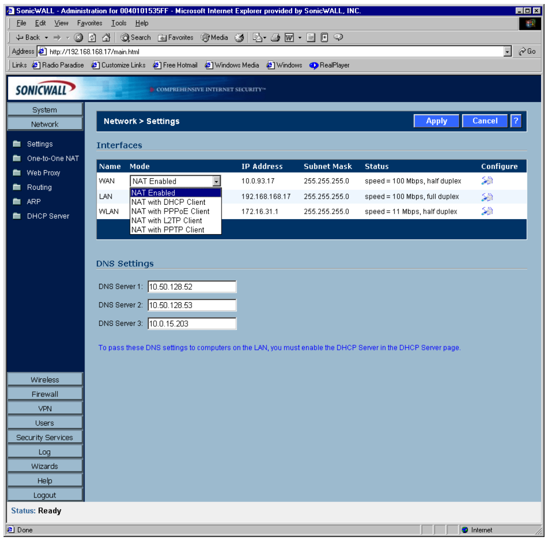
Network Addressing Modes

The **Mode** menu in the **Interfaces** table determines the network address scheme of your SonicWALL. It includes six options:

- **Transparent Mode** requires valid IP addresses for all computers on your network, but allows remote access to authenticated users. Your public WAN IP address is visible to the Internet.
- **NAT Enabled** mode translates the private IP addresses on the network to the single, valid IP address of the SonicWALL. Select **NAT Enabled** if your ISP assigned you only one or two valid IP addresses.
- **NAT with DHCP Client** mode configures the SonicWALL to request IP settings from a DHCP server on the Internet. **NAT with DHCP Client** is a typical network addressing mode for cable and DSL customers.
- **NAT with PPPoE** mode uses PPPoE to connect to the Internet. If desktop software and a user name and password is required by your ISP, select **NAT with PPPoE**.
- **NAT with L2TP Client** mode uses IPSec to connect a L2TP server and encrypts all data transmitted from the client to the server. However, it does not encrypt network traffic to other destinations.
- **NAT with PPTP Client** mode uses Point to Point Tunneling Protocol (PPTP) to connect to a remote server. It supports older Microsoft implementations requiring tunneling connectivity.


SonicWALL - Administration for 0040101535FF - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.17/main.html Go
Links Radio Paradise Customize Links Free Hotmail Windows Media Windows RealPlayer
SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Settings
One-to-One NAT
Web Proxy
Routing
ARP
DHCP Server
Wireless
Firewall
VPN
Users
Security Services
Log
Wizards
Help
Logout
Apply
Cancel
?
NAT Enabled
NAT with DHCP Client
NAT with PPPoE Client
NAT with L2TP Client
NAT with PPTP Client
Done
Internet

Network > Settings

Interfaces

Name	Mode	IP Address	Subnet Mask	Status	Configure
WAN	NAT Enabled	10.0.93.17	255.255.255.0	speed = 100 Mbps, half duplex	
LAN		192.168.168.17	255.255.255.0	speed = 100 Mbps, full duplex	
WLAN		172.16.31.1	255.255.255.0	speed = 11 Mbps, half duplex	

DNS Settings

DNS Server 1: 10.50.128.52

DNS Server 2: 10.50.128.53

DNS Server 3: 10.0.15.203

To pass these DNS settings to computers on the LAN, you must enable the DHCP Server in the DHCP Server page.

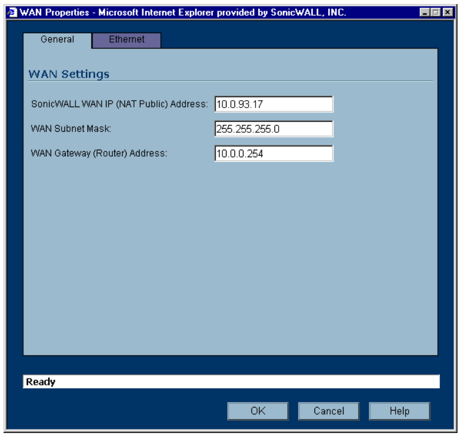
Status: Ready

Interfaces

The **Interfaces** table lists the **IP Addresses**, **Subnet Mask**, and **Status** information for the **WAN**, **LAN**, or **OPT**/**DMZ** links. To configure the **WAN**, **LAN**, or **OPT**/**DMZ** settings, click the **Notepad** icon in the **Configure** column.

Configuring WAN Settings

Click on the **Notepad** icon in the **Configure** column of the **WAN** information. The **WAN Properties** window is displayed.



WAN Properties - Microsoft Internet Explorer provided by SonicWALL, INC.

WAN Settings

SonicWALL WAN IP (NAT Public) Address: 10.0.93.17

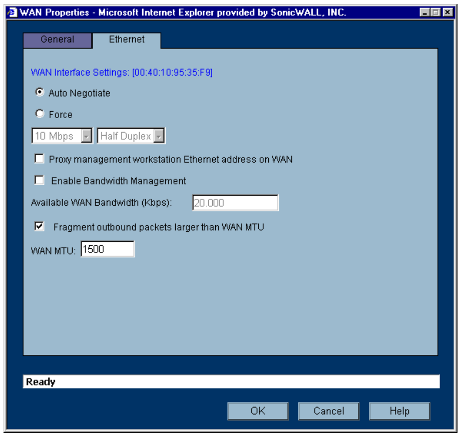
WAN Subnet Mask: 255.255.255.0

WAN Gateway (Router) Address: 10.0.0.254

Ready

WAN Properties>General

1. In the **WAN Settings** section, enter a valid public IP address in the **SonicWALL WAN IP (NAT Public) Address** field.
2. Enter the subnet mask in the **WAN Subnet Mask** field.
3. Enter the IP address of the router in the **WAN Gateway (Router) Address** field.
4. Click the **Ethernet** tab. The **Ethernet** tab allows you to manage the Ethernet settings of links connected to the SonicWALL.



WAN Properties - Microsoft Internet Explorer provided by SonicWALL, INC.

WAN Interface Settings: [00:40:10:95:35:F9]

● Auto Negotiate

○ Force

10 Mbps | Half Duplex

□ Proxy management workstation Ethernet address on WAN

□ Enable Bandwidth Management

Available WAN Bandwidth (Kbps): 20.000

☑ Fragment outbound packets larger than WAN MTU

WAN MTU: 1500

Ready

5. **Auto Negotiate** is selected by default because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you select **Force**, you must force the connection speed and duplex from the Ethernet card to the SonicWALL as well.
6. If you select **Force,** select the speed and duplex from the pulldown menus.
7. Select **Proxy management workstation Ethernet address on WAN** if you are managing the Ethernet connection from the LAN side of your network. The SonicWALL takes the Ethernet address of the computer managing the SonicWALL appliance and proxies that address onto the WAN port of the SonicWALL. For instance, if your ISP is using the MAC address of your network card for identification, you can proxy the MAC address of your network card onto the SonicWALL WAN port.

Alert! *If you enable this feature, it may take the SonicWALL a lengthy period of time to locate the management station.*

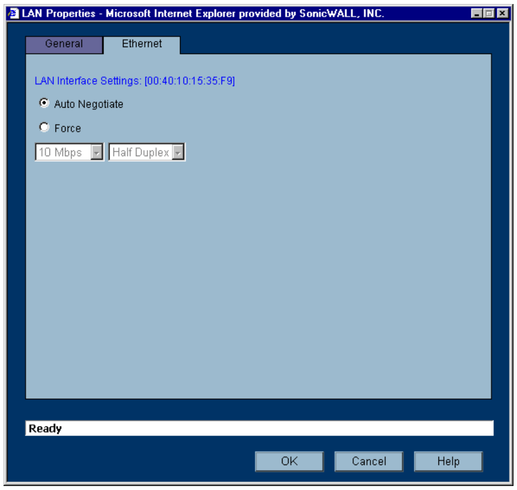
8. Select **Bandwidth Management** to allocate bandwidth resources to critical applications on the your network. 20.00 Kbps is the default available WAN bandwidth.

Alert! *Bandwidth management is only available on outbound network traffic.*

9. **Fragment outbound packets larger than WAN MTU** is selected by default with a default WAN MTU value of 1500 based on the Ethernet standard MTU. The minimum value is 68. Decreasing the packet size can improve network performance as large packets require more network transmissions when a router cannot handle the packet size.
10. Click **OK**. Then click **Apply** on the **Network>Settings** page. The SonicWALL is now updated.

Configuring LAN Settings

Click on the **Notepad** icon in the **Configure** column of the **LAN** information. The **LAN Properties** window is displayed.



LAN Properties - Microsoft Internet Explorer provided by SonicWALL, INC.

LAN Interface Settings: [00:40:10:15:35:F9]

● Auto Negotiate

○ Force

10 Mbps | Half Duplex

Ready

LAN Properties>General

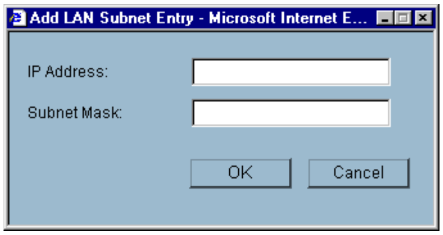
1. In the **LAN Settings** section, enter a valid private IP address in the **SonicWALL LAN IP (NAT Public) Address** field.

2. Enter the subnet mask in the **LAN Subnet Mask** field.

Multiple LAN Subnet Support

This features supports legacy networks incorporating the SonicWALL, and makes it easier to add more nodes if the original subnet is full. To configure this feature, you must have an additional IP address assigned to the SonicWALL. All users on the subnet must use this address as their default router/gateway address.

3. Click **Add**. The **Add LAN Subnet Entry** window is displayed.

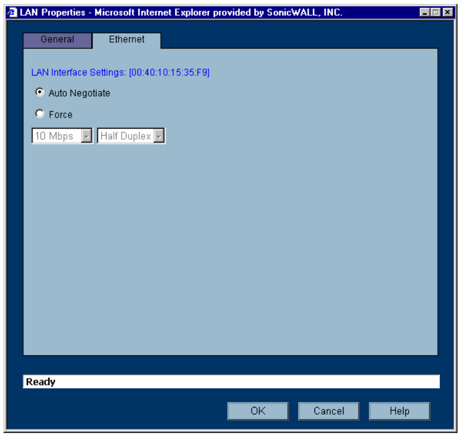


Add LAN Subnet Entry - Microsoft Internet E...

IP Address:

Subnet Mask:

4. Enter the additional LAN IP address in the **IP Address** field.
5. Enter the subnet in the **Subnet Mask** field.
6. Select an entry and click **Edit** to change the information.
7. Select an entry and click **Delete** to remove the entry from the table.
8. Click **Delete All** to remove all the entries in the table.
9. Click the **Ethernet** tab.



LAN Properties - Microsoft Internet Explorer provided by SonicWALL, INC.

LAN Interface Settings: [00:40:10:15:35:F9]

● Auto Negotiate

○ Force

10 Mbps Half Duplex

Ready

The **Ethernet** tab allows you to manage the Ethernet settings of links connected to the SonicWALL.

10. **Auto Negotiate** is selected by default because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you select **Force**, you must force the connection speed and duplex from the Ethernet card to the SonicWALL as well.
11. If you select **Force,** select the speed and duplex from the pulldown menus.
12. Select **Proxy management workstation Ethernet address on WAN** if you are managing the Ethernet connection from the LAN side of your network. The SonicWALL takes the Ethernet address of the computer managing the SonicWALL appliance and proxies that address onto the WAN port of the SonicWALL.

Tip! *If you are not managing the Ethernet connection from the LAN, the SonicWALL looks for a random computer on the network creating a lengthy search process.*

13. Select **Bandwidth Management** to allocate bandwidth resources to critical applications on the your network. 20.00 Kbps is the default available WAN bandwidth.

Alert! *Bandwidth management is only available on outbound network traffic.*

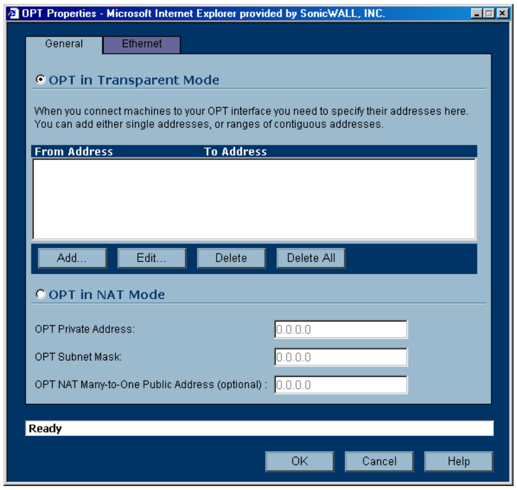
14. **Fragment outbound packets larger than WAN MTU** is selected by default with a default WAN MTU value of 1500 based on the Ethernet standard MTU. The minimum value is 68. Decreasing the packet size can improve network performance as large packets require more network transmissions when a router cannot handle the packet size.
15. Click **OK**. Then click **Apply** on the **Network>Settings** page. The SonicWALL is now updated.

Configuring OPT/DMZ Settings

The **OPT Properties** or **DMZ Properties** window includes the same settings as the **LAN Properties** window. Refer to the **LAN Properties** window instructions for configuring your **OPT** or **DMZ** interface properties.

Configuring the OPT/DMZ Port in Transparent Mode

If your ISP provided you with enough IP addresses for all the computers and network devices on your OPT/DMZ, enable **Transparent Mode**.


OPT Properties - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Ethernet
Add...
Edit...
Delete
Delete All
OK
Cancel
Help

● OPT in Transparent Mode

When you connect machines to your OPT interface you need to specify their addresses here. You can add either single addresses, or ranges of contiguous addresses.

From Address	To Address

○ OPT in NAT Mode

OPT Private Address: 0.0.0.0

OPT Subnet Mask: 0.0.0.0

OPT NAT Many-to-One Public Address (optional) : 0.0.0.0

Ready

To configure **Transparent** addressing mode, complete the following instructions:

1. Select **OPT/DMZ in Transparent Mode**.
2. Click **Add**.
3. Enter a range of valid IP address from your network address range in the **SonicWALL IP Address** field.
4. Click **OK**.
5. Click **OK**. Once the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the browser window.

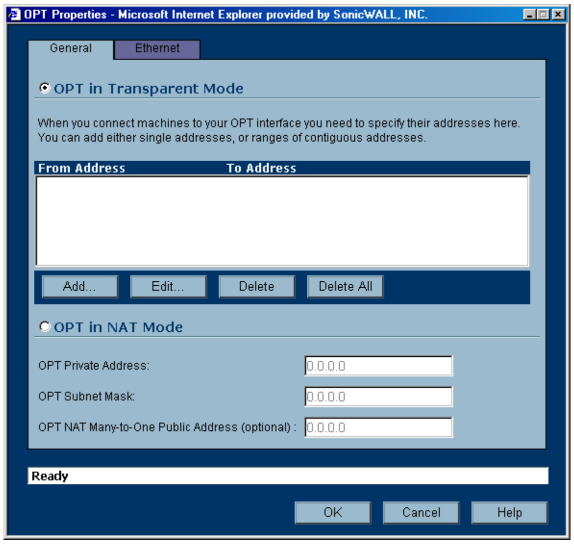
Configuring the OPT/DMZ Port in NAT Mode

If your ISP has not given you enough IP addresses for all of the computers and network devices on your OPT/DMZ, you can configure the SonicWALL to use NAT Enabled mode. Using a single IP address, you can connect your network to the Internet securely and invisibly using Network Address Translation (NAT). NAT provides additional security and anonymity to your network. Because you do not have enough IP addresses for your network, enable NAT and assign private IP addresses to the computers and devices on your LAN. You can use IP addresses from one of the following IP address ranges:

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

Alert! *Do not assign the same IP address range to the LAN and the OPT/DMZ.*

Click the **Notepad** icon in the **Configure** column of the **Interfaces** table. The **OPT/DMZ Properties** window is displayed.


OPT Properties - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Ethernet
Add...
Edit...
Delete
Delete All
OK
Cancel
Help

● OPT in Transparent Mode

When you connect machines to your OPT interface you need to specify their addresses here. You can add either single addresses, or ranges of contiguous addresses.

From Address	To Address

○ OPT in NAT Mode

OPT Private Address: 0.0.0.0

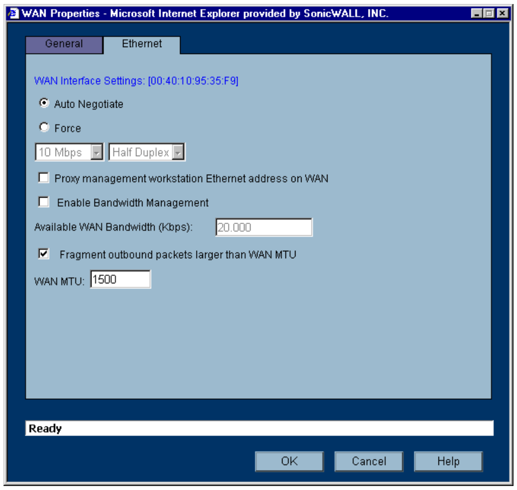
OPT Subnet Mask: 0.0.0.0

OPT NAT Many-to-One Public Address (optional) : 0.0.0.0

Ready

1. In the **OPT/DMZ Private Address** field, enter a valid private IP address.
2. Enter the subnet mask in the **OPT/DMZ Subnet Mask** field.
3. Click **OK**.

4. Click the **Ethernet** tab. The **Ethernet** tab allows you to manage the Ethernet settings of links connected to the SonicWALL.



WAN Properties - Microsoft Internet Explorer provided by SonicWALL, INC.

WAN Interface Settings: [00:40:10:95:35:F9]

● Auto Negotiate

○ Force

10 Mbps | Half Duplex

□ Proxy management workstation Ethernet address on WAN

□ Enable Bandwidth Management

Available WAN Bandwidth (Kbps): 20.000

☑ Fragment outbound packets larger than WAN MTU

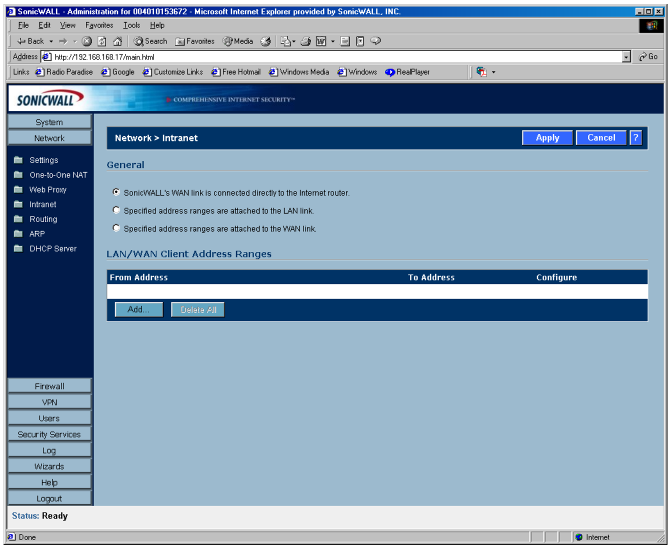
WAN MTU: 1500

Ready

5. **Auto Negotiate** is selected by default because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you select **Force**, you must force the connection speed and duplex from the Ethernet card to the SonicWALL as well.
6. If you select **Force**, select the speed and duplex from the pulldown menus.
7. Click **OK**. Then click **Apply** on the **Network>Settings** page. The SonicWALL is now updated.

Configuring the SonicWALL in Transparent Mode

Transparent Mode requires valid IP addresses for all computers on your network, and allows remote access to authenticated users. Your public WAN IP address is visible to the Internet. To enable Transparent Mode, select **Transparent Mode** from the **Mode** menu. The WAN and LAN IP addresses are now identical. To complete the configuration, click **Intranet** in the **Network** menu list.



SonicWALL - Administration for 004010153672 - Microsoft Internet Explorer provided by SonicWALL, INC.

Address: http://192.168.168.17/main.html

Network > Intranet

General

● SonicWALL's WAN link is connected directly to the Internet router.

○ Specified address ranges are attached to the LAN link.

○ Specified address ranges are attached to the WAN link.

LAN/WAN Client Address Ranges

From Address	To Address	Configure

Status: Ready

1. Select **Specified address ranges are attached to the LAN link**.
2. Click **Add** in the **From Address** table.
3. Enter the range of network IP addresses on the LAN.
4. Click **OK** and then click **Apply**.

5. Click **Restart** in the Status bar of the management interface. The SonicWALL restarts and updates the configuration.

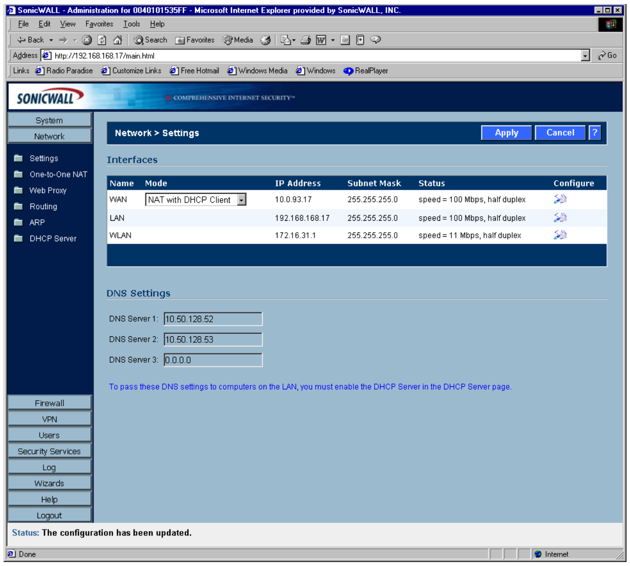
Configuration Example

Your ISP has given you a public IP address of 66.217.71.191 and a range of public IP address from 66.217.71.192 to 66.217.71.200. To configure the SonicWALL in Transparent Mode, select **Transparent Mode** from the **Mode** menu. Then follow these steps:

1. Click the icon in the **Configure** column to display the **WAN Settings** window.
2. Enter your IP address, 66.217.71.191, in the **WAN IP Address** field. Complete the rest of the fields in the **WAN Settings** window using information provided by the ISP.
3. Click **OK**.
4. Click **Intranet** in the **Network** menu list.
5. Select **Specified address ranges are attached to the LAN link**.
6. Click **Add** in the **LAN/WAN Client Address Ranges** table.
7. Enter your IP address, 66.217.71.192, in the **IP Address From** field.
8. Enter the IP address, 66.217.71.200, in the **IP Address To** field and click **OK**.
9. Click **Apply**, and then **Restart** in the **Status** bar. The SonicWALL restarts and updates the configuration.

Configuring NAT with DHCP Client

If your ISP did not provide you with a public IP address, the SonicWALL can obtain an IP address from a DHCP server at the ISP. NAT with DHCP Client is typically used with cable and DSL connections. To configure NAT with DHCP Client, log into the SonicWALL and click **Network**.


SonicWALL - Administration for 0040101535FF - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.17/main.html
Go
Links Radio Paradise Customize Links Free Hotmail Windows Media Windows RealPlayer
SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Settings
One-to-One NAT
Web Proxy
Routing
ARP
DHCP Server
Firewall
VPN
Users
Security Services
Log
Wizards
Help
Logout
Apply
Cancel
?
Done
Internet

Network > Settings

Interfaces

Name	Mode	IP Address	Subnet Mask	Status	Configure
WAN	NAT with DHCP Client	10.0.93.17	255.255.255.0	speed = 100 Mbps, half duplex	
LAN		192.168.168.17	255.255.255.0	speed = 100 Mbps, half duplex	
WLAN		172.16.31.1	255.255.255.0	speed = 11 Mbps, half duplex	

DNS Settings

DNS Server 1: 10.50.128.52

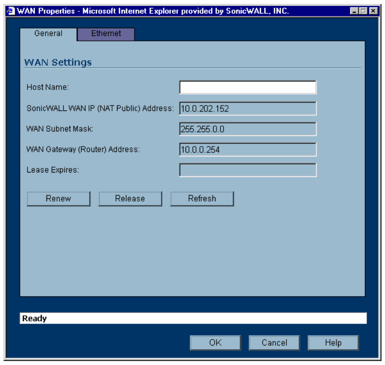
DNS Server 2: 10.50.128.53

DNS Server 3: 0.0.0.0

To pass these DNS settings to computers on the LAN, you must enable the DHCP Server in the DHCP Server page.

Status: The configuration has been updated.

1. Select **NAT with DHCP Client** from the **Network Addressing Mode** menu.
2. Click the Notepad icon in the **WAN** entry of the **Interfaces** table. The **WAN Properties** window is displayed.



WAN Properties - Microsoft Internet Explorer provided by SonicWALL, INC.

General | Ethernet

WAN Settings

Host Name:

SonicWALL WAN IP (NAT Public) Address: 10.0.202.152

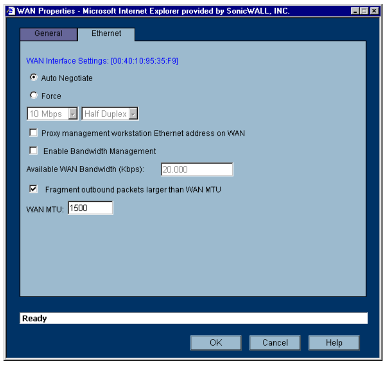
WAN Subnet Mask: 255.255.0.0

WAN Gateway (Router) Address: 10.0.0.254

Lease Expires:

Ready

3. Enter the host name assigned to you by your ISP in the **Host Name** field. (Optional)
4. Click **Renew** to obtain new IP address settings for the SonicWALL.
5. Click **Release** to remove the IP address settings from the SonicWALL. Click **Refresh** to reload the current settings into the SonicWALL.
6. Click the **Ethernet** tab. The **Ethernet** tab allows you to manage the Ethernet settings of links connected to the SonicWALL.



WAN Properties - Microsoft Internet Explorer provided by SonicWALL, INC.

General | Ethernet

WAN Interface Settings: [00:40:10:95:35:F9]

● Auto Negotiate

○ Force

10 Mbps | Half Duplex

☐ Proxy management workstation Ethernet address on WAN

☐ Enable Bandwidth Management

Available WAN Bandwidth (Kbps): 20.000

☑ Fragment outbound packets larger than WAN MTU

WAN MTU: 1500

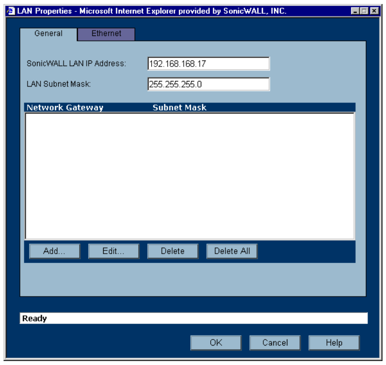
Ready

7. **Auto Negotiate** is selected by default because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you select **Force**, you must force the connection speed and duplex from the Ethernet card to the SonicWALL as well.
8. If you select **Force**, select the speed and duplex from the pulldown menus.
9. **Fragment outbound packets larger than WAN MTU** is selected by default. If the MTU size is too large, it requires more transmissions if the packet encounters a router unable to handle a larger packet. The default value is 1500 octets based on the Ethernet standard MTU. The minimum packet size is 68 octets. Decreasing the packet size may improve network performance.
10. Click **OK**.

Note: *DNS Settings are obtained automatically when the SonicWALL receives its IP address information from the DHCP Server.*

Configuring LAN Settings

Click on the **Notepad** icon in the **Configure** column of the **LAN** information. The **LAN Properties** window is displayed.



SonicWALL LAN IP Address: 192.168.168.17

LAN Subnet Mask: 255.255.255.0

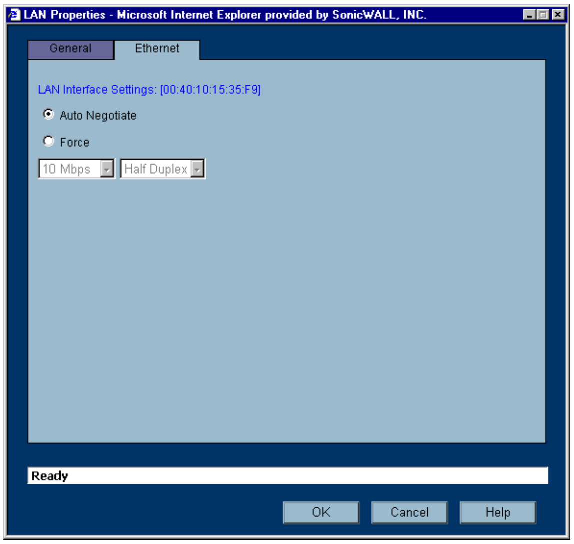
LAN Properties>General

1. In the **LAN Settings** section, enter a valid private IP address in the **SonicWALL LAN IP (NAT Public) Address** field.
2. Enter the subnet mask in the **LAN Subnet Mask** field.

Multiple LAN Subnet Mask Support

This features supports legacy networks incorporating the SonicWALL, and makes it easier to add more nodes if the original subnet is full. To configure this feature, you must have an additional IP address assigned to the SonicWALL. All users on the subnet must use this address as their default router/gateway address.

3. Click **Add**. The **Add LAN Subnet Entry** window is displayed.
4. Enter the additional LAN IP address in the **IP Address** field.
5. Enter the subnet in the **Subnet Mask** field.
6. Select an entry and click **Edit** to change the information.
7. Select an entry and click **Delete** to remove the entry from the table.
8. Click **Delete All** to remove all the entries in the table.
9. Click the **Ethernet** tab. The **Ethernet** tab allows you to manage the Ethernet settings of links connected to the SonicWALL.



LAN Properties - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Ethernet
Ready
OK
Cancel
Help

LAN Interface Settings: [00:40:10:15:35:F9]

● Auto Negotiate

○ Force

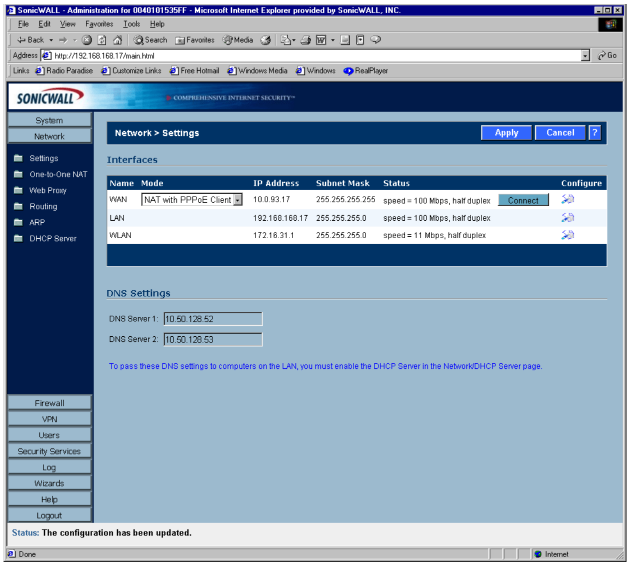
10 Mbps | Half Duplex

10. **Auto Negotiate** is selected by default because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you select **Force**, you must force the connection speed and duplex from the Ethernet card to the SonicWALL as well.
11. If you select **Force**, select the speed and duplex from the pulldown menus.
12. Click **OK**. Then click **Apply** on the **Network>Settings** page.

Configuring NAT with PPPoE Client

The SonicWALL can use Point-to-Point Protocol over Ethernet to connect to the Internet. If your ISP requires the installation of desktop software as well as a user name and password to access the Internet, enable NAT with PPPoE Client.

1. Log into the SonicWALL and click **Network**.



SonicWALL - Administration for 0040101535FF - Microsoft Internet Explorer provided by SonicWALL, INC.

Address: http://192.168.168.17/main.html

Network > Settings

Interfaces

Name	Mode	IP Address	Subnet Mask	Status	Configure
WAN	NAT with PPPoE Client	10.0.93.17	255.255.255.255	speed = 100 Mbps, half duplex Connect	
LAN		192.168.168.17	255.255.255.0	speed = 100 Mbps, half duplex	
WLAN		172.16.31.1	255.255.255.0	speed = 11 Mbps, half duplex	

DNS Settings

DNS Server 1: 10.50.128.52

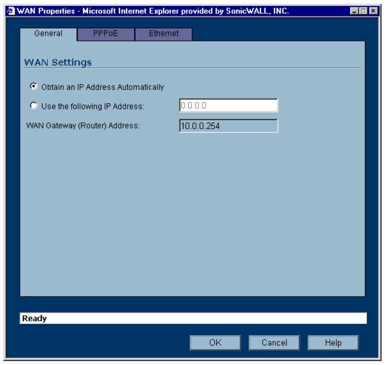
DNS Server 2: 10.50.128.53

To pass these DNS settings to computers on the LAN, you must enable the DHCP Server in the Network/DHCP Server page.

Status: The configuration has been updated.

File Edit View Favorites Tools Help
Back Search Favorites Media
Links Radio Paradise Customize Links Free Hotmail Windows Media Windows RealPlayer
Go
SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Settings
One-to-One NAT
Web Proxy
Routing
ARP
DHCP Server
Firewall
VPN
Users
Security Services
Log
Wizards
Help
Logout
Apply
Cancel
?
Done
Internet

2. Select **NAT with PPPoE Client** from the **Network Addressing Mode** menu.
3. Click the Notepad icon in the WAN entry of the **Interfaces** table. The **WAN Properties** window is displayed.



WAN Properties - Microsoft Internet Explorer provided by SonicWALL, INC.

WAN Settings

● Obtain an IP Address Automatically

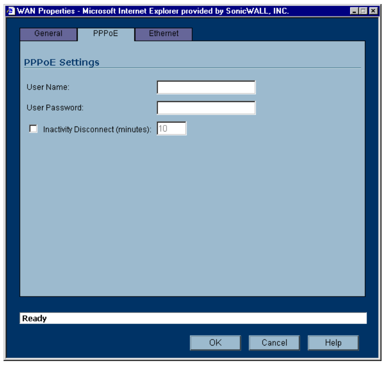
○ Use the following IP Address: 0.0.0.0

WAN Gateway (Router) Address: 10.0.0.254

Ready

4. Select **Obtain an IP Address Automatically** if you do not have a public IP address from your ISP. If you have an IP address from your ISP, select **Use the following Address**, and enter the IP address in the IP address field.

5. Click the **PPPoE** tab.



WAN Properties - Microsoft Internet Explorer provided by SonicWALL, INC.

PPPoE Settings

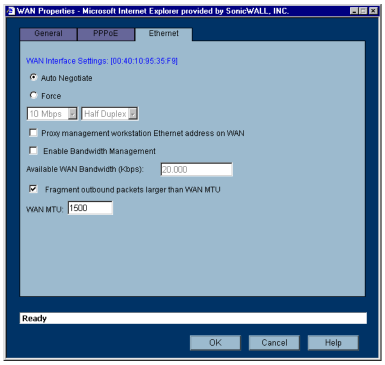
User Name:

User Password:

☐ Inactivity Disconnect (minutes): 10

Ready

6. Enter your user name and password provided by your ISP in the **User Name** and **User Password** fields.
7. Select **Inactivity Disconnect (minutes)** to end the connection after a specified time of inactivity. 10 minutes is the default value.
8. Click the **Ethernet** tab. The **Ethernet** tab allows you to manage the Ethernet settings of links connected to the SonicWALL



WAN Properties - Microsoft Internet Explorer provided by SonicWALL, INC.

WAN Interface Settings: [00:40:10:95:35:F9]

● Auto Negotiate

○ Force

10 Mbps ▾ Half Duplex ▾

☐ Proxy management workstation Ethernet address on WAN

☐ Enable Bandwidth Management

Available WAN Bandwidth (Kbps): 20.000

☑ Fragment outbound packets larger than WAN MTU

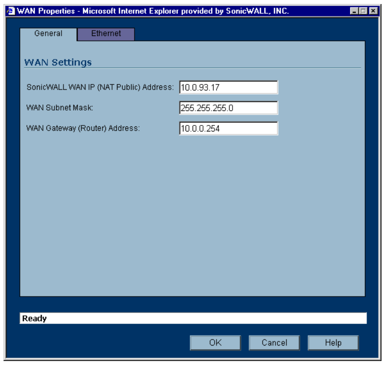
WAN MTU: 1500

Ready

9. **Auto Negotiate** is selected by default because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you select **Force**,
10. Select the speed and duplex from the pulldown menus. If you select **Force**, you must force the connection speed and duplex from the Ethernet card to the SonicWALL as well.
11. Click **OK**.

Configuring LAN Properties for NAT with PPPoE Client

Click the Notepad icon in the LAN entry of the **Interfaces** table. The **LAN Properties** window is displayed.


WAN Properties - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Ethernet
OK
Cancel
Help

WAN Settings

SonicWALL WAN IP (NAT Public) Address: 10.0.93.17

WAN Subnet Mask: 255.255.255.0

WAN Gateway (Router) Address: 10.0.0.254

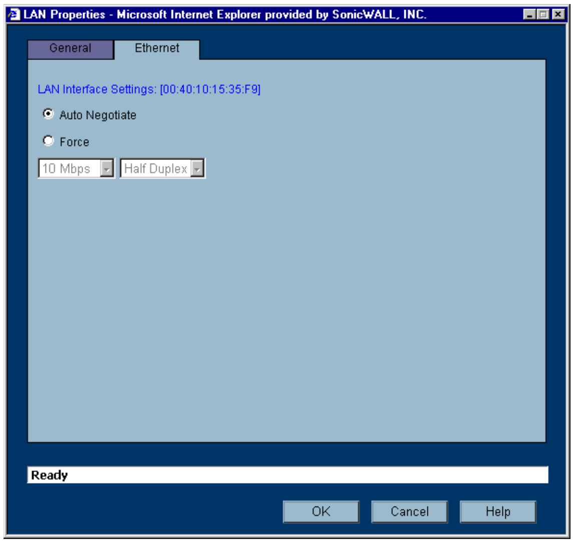
Ready

1. In the **LAN Settings** section, enter a valid private IP address in the **SonicWALL LAN IP (NAT Public) Address** field.
2. Enter the subnet mask in the **LAN Subnet Mask** field.

Multiple LAN Subnet Support

This features supports legacy networks incorporating the SonicWALL, and makes it easier to add more nodes if the original subnet is full. To configure this feature, you must have an additional IP address assigned to the SonicWALL. All users on the subnet must use this address as their default router/gateway address.

3. Click **Add**. The **Add LAN Subnet Entry** window is displayed.
4. Enter the additional LAN IP address in the **IP Address** field.
5. Enter the subnet in the **Subnet Mask** field.
6. Select an entry and click **Edit** to change the information.
7. Select an entry and click **Delete** to remove the entry from the table.
8. Click **Delete All** to remove all the entries in the table.
9. Click the **Ethernet** tab. The **Ethernet** tab allows you to manage the Ethernet settings of links connected to the SonicWALL.


LAN Properties - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Ethernet
OK
Cancel
Help

LAN Interface Settings: [00:40:10:15:35:F9]

● Auto Negotiate

○ Force

10 Mbps | Half Duplex

Ready

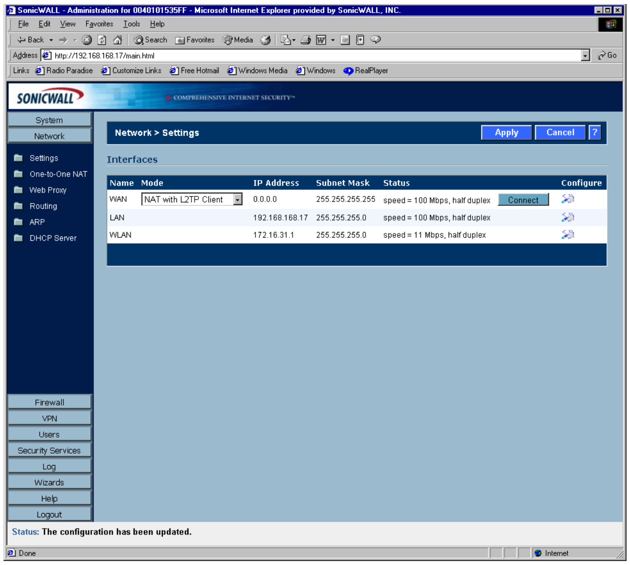
10. **Auto Negotiate** is selected by default because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you select **Force**, you must force the connection speed and duplex from the Ethernet card to the SonicWALL as well.

11. If you select **Force**, select the speed and duplex from the pulldown menus.
12. Click **OK**. Then click **Apply** on the **Network>Settings** page.

Configuring NAT with L2TP Client

If your Internet connection is provided through a L2TP server, you must configure the SonicWALL to use NAT with L2TP Client. L2TP (Layer 2 Tunneling Protocol) provides interoperability between VPN vendors that protocols such as Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Forwarding (L2F) do not have.

1. Log into the SonicWALL, and click **Network**.


SonicWALL - Administration for 0040101535FF - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.17/main.html Go
Links Radio Paradise Customize Links Free Hotmail Windows Media Windows RealPlayer
SONICWALL COMPREHENSIVE INTERNET SECURITY
System
Network
Settings
One-to-One NAT
Web Proxy
Routing
ARP
DHCP Server
Firewall
VPN
Users
Security Services
Log
Wizards
Help
Logout
Apply
Cancel
?
Done
Internet

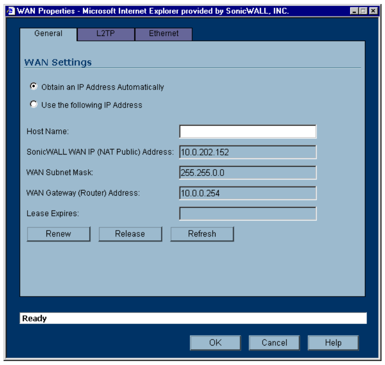
Network > Settings

Interfaces

Name	Mode	IP Address	Subnet Mask	Status		Configure
WAN	NAT with L2TP Client	0.0.0.0	255.255.255.255	speed = 100 Mbps, half duplex	Connect	
LAN		192.168.168.17	255.255.255.0	speed = 100 Mbps, half duplex		
WLAN		172.16.31.1	255.255.255.0	speed = 11 Mbps, half duplex		

Status: The configuration has been updated.

2. Select **NAT with L2TP Client** from the **Network Addressing Mode** menu.
3. Click the Notepad icon in the **WAN** entry of the **Interfaces** table. The **WAN Properties** window is displayed.


WAN Properties - Microsoft Internet Explorer provided by SonicWALL, INC.
General
L2TP
Ethernet
Renew
Release
Refresh
OK
Cancel
Help

WAN Settings

● Obtain an IP Address Automatically

○ Use the following IP Address

Host Name:

SonicWALL WAN IP (NAT Public) Address: 10.0.202.152

WAN Subnet Mask: 255.255.0.0

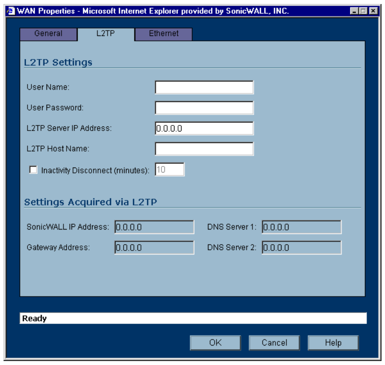
WAN Gateway (Router) Address: 10.0.0.254

Lease Expires:

Ready

4. **Obtain an IP Address Automatically** is selected by default. Enter your host name in the the **Host Name** field. Click **Renew** to obtain new IP addressing information. Click **Release** to discard IP addressing information. Click **Refresh** to reload the IP addressing information.
5. If you have IP addressing information, select **Use the following IP Address**.
6. Enter your public IP address in the **SonicWALL WAN IP (NAT Public) Address** field.
7. Enter the WAN Subnet information in the **WAN Subnet Mask** field.
8. Enter the WAN Gateway IP address in the **WAN Gateway (Router) Address** field.

9. Click on the **L2TP** tab.


WAN Properties - Microsoft Internet Explorer provided by SonicWALL, INC.
General
L2TP
Ethernet
OK
Cancel
Help

L2TP Settings

User Name:

User Password:

L2TP Server IP Address: 0.0.0.0

L2TP Host Name:

□ Inactivity Disconnect (minutes): 10

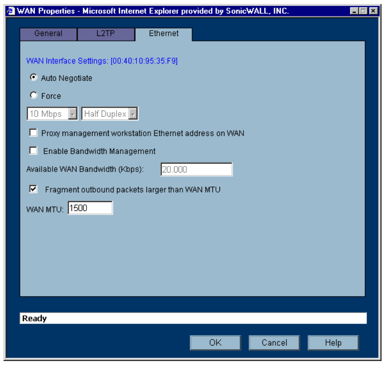
Settings Acquired via L2TP

SonicWALL IP Address: 0.0.0.0 DNS Server 1: 0.0.0.0

Gateway Address: 0.0.0.0 DNS Server 2: 0.0.0.0

Ready

10. Enter your user name in the **User Name** field.
11. Enter your password in the **User Password** field.
12. Enter the IP address of the L2TP Server in the **L2TP Server IP Address** field.
13. Enter the host name of the L2TP Server in the **L2TP Host Name** field.
14. Select **Inactivity Disconnect (minutes)** to end the connection after a specified time of inactivity.
15. Once a connection is established, the SonicWALL WAN IP address, the Gateway address and the DNS Server IP addresses are displayed in the **Settings Acquired via L2TP** section.
16. Click the **Ethernet** tab. The **Ethernet** tab allows you to manage the Ethernet settings of links connected to the SonicWALL.


WAN Properties - Microsoft Internet Explorer provided by SonicWALL, INC.
General
L2TP
Ethernet
OK
Cancel
Help

WAN Interface Settings: [00:40:10:95:35:F9]

● Auto Negotiate

○ Force

10 Mbps Half Duplex

□ Proxy management workstation Ethernet address on WAN

□ Enable Bandwidth Management

Available WAN Bandwidth (Kbps): 20.000

☑ Fragment outbound packets larger than WAN MTU

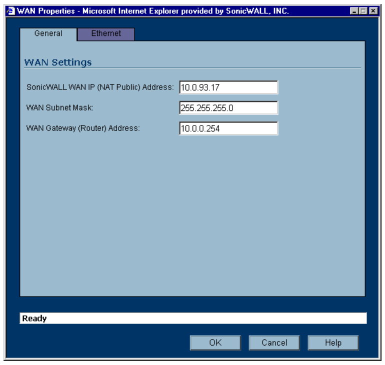
WAN MTU: 1500

Ready

17. **Auto Negotiate** is selected by default because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you select **Force**, you must force the connection speed and duplex from the Ethernet card to the SonicWALL as well.
18. If you select **Force**, select the speed and duplex from the pulldown menus.
19. **Fragment outbound packets larger than WAN MTU** is selected by default. If the MTU size is too large, it requires more transmissions if the packet encounters a router unable to handle a larger packet. The default value is 1500 octets based on the Ethernet standard MTU. The minimum packet size is 68 octets. Decreasing the packet size may improve network performance.
20. Click **OK**.

Configuring LAN Properties for NAT with L2TP Client

Click the Notepad icon in the LAN entry of the **Interfaces** table. The **LAN Properties** window is displayed.


WAN Properties - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Ethernet
OK
Cancel
Help

WAN Settings

SonicWALL WAN IP (NAT Public) Address: 10.0.93.17

WAN Subnet Mask: 255.255.255.0

WAN Gateway (Router) Address: 10.0.0.254

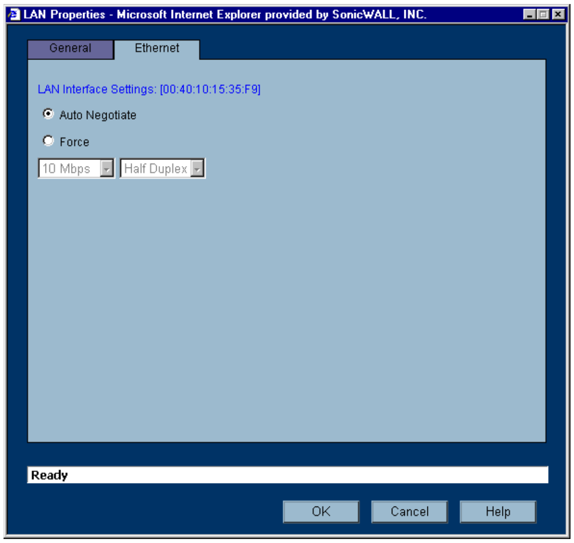
Ready

1. In the **LAN Settings** section, enter a valid private IP address in the **SonicWALL LAN IP (NAT Public) Address** field.
2. Enter the subnet mask in the **LAN Subnet Mask** field.

Multiple LAN Subnet Mask Support

This features supports legacy networks incorporating the SonicWALL, and makes it easier to add more nodes if the original subnet is full. To configure this feature, you must have an additional IP address assigned to the SonicWALL. All users on the subnet must use this address as their default router/gateway address.

3. Click **Add**. The **Add LAN Subnet Entry** window is displayed.
4. Enter the LAN IP address in the **IP Address** field.
5. Enter the subnet in the **Subnet Mask** field.
6. Select an entry and click **Edit** to change the information.
7. Select an entry and click **Delete** to remove the entry from the table.
8. Click **Delete All** to remove all the entries in the table.
9. Click the **Ethernet** tab. The **Ethernet** tab allows you to manage the Ethernet settings of links connected to the SonicWALL.


LAN Properties - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Ethernet
OK
Cancel
Help

LAN Interface Settings: [00:40:10:15:35:F9]

● Auto Negotiate

○ Force

10 Mbps | Half Duplex

Ready

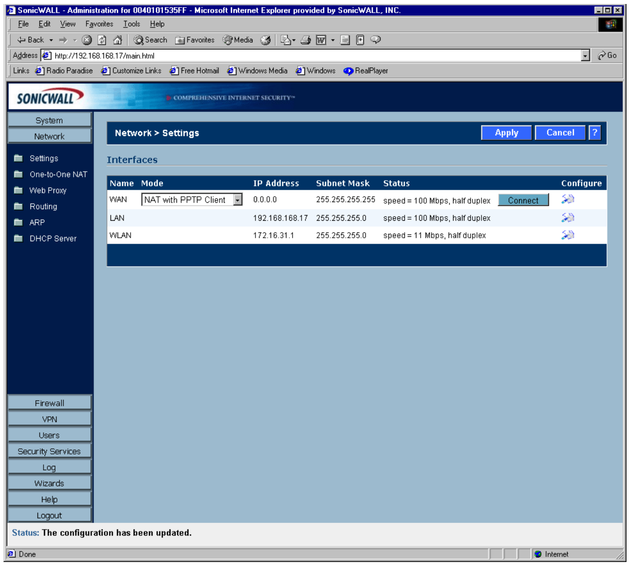
10. **Auto Negotiate** is selected by default because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you select **Force**, you must force the connection speed and duplex from the Ethernet card to the SonicWALL as well.

11. If you select **Force**, select the speed and duplex from the pulldown menus.
12. Click **OK**. Then click **Apply** on the **Network>Settings** page.

Configuring NAT with PPTP Client

If your Internet connection is provided through a PPTP server, you must configure the SonicWALL to use NAT with PPTP Client.

Log into the SonicWALL, and click **Network**.


SonicWALL - Administration for 0040101535FF - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.17/main.html Go
Links Radio Paradise Customize Links Free Hotmail Windows Media Windows RealPlayer
SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Settings
One-to-One NAT
Web Proxy
Routing
ARP
DHCP Server
Firewall
VPN
Users
Security Services
Log
Wizards
Help
Logout
Apply
Cancel
?
Connect
Done
Internet

Network > Settings

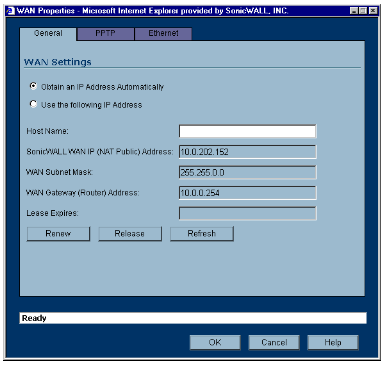
Interfaces

Name	Mode	IP Address	Subnet Mask	Status	Configure
WAN	NAT with PPTP Client	0.0.0.0	255.255.255.255	speed = 100 Mbps, half duplex	
LAN		192.168.168.17	255.255.255.0	speed = 100 Mbps, half duplex	
WLAN		172.16.31.1	255.255.255.0	speed = 11 Mbps, half duplex	

Status: The configuration has been updated.

1. Select **NAT with PPTP Client** from the **Network Addressing Mode** menu.

2. Click the Notepad icon in the **WAN** entry of the **Interfaces** table. The **WAN Properties** window is displayed.


WAN Properties - Microsoft Internet Explorer provided by SonicWALL, INC.
General
PPTP
Ethernet
Renew
Release
Refresh
OK
Cancel
Help

WAN Settings

● Obtain an IP Address Automatically

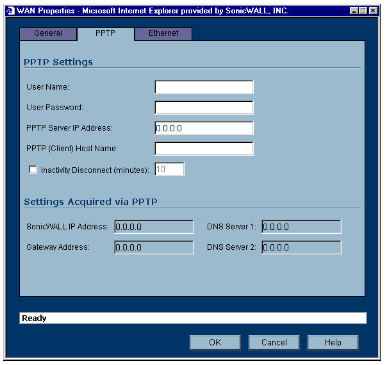
○ Use the following IP Address

Host Name:	
SonicWALL WAN IP (NAT Public) Address:	10.0.202.152
WAN Subnet Mask:	255.255.0.0
WAN Gateway (Router) Address:	10.0.0.254
Lease Expires:	

Ready

3. **Obtain an IP Address Automatically** is selected by default. Enter your host name in the **Host Name** field. Click **Renew** to obtain new IP addressing information. Click **Release** to discard IP addressing information. Click **Refresh** to reload the IP addressing information.
4. If you have IP addressing information, select **Use the following IP Address**.
5. Enter the WAN IP address in the **SonicWALL WAN IP (NAT Public) Address** field.
6. Enter the WAN Subnet information in the **WAN Subnet Mask** field.
7. Enter the WAN Gateway IP address in the **WAN Gateway (Router) Address** field.

8. Click on the **PPTP** tab.



WAN Properties - Microsoft Internet Explorer provided by SonicWALL, INC.

PPTP Settings

User Name:

User Password:

PPTP Server IP Address: 0.0.0.0

PPTP (Client) Host Name:

☐ Inactivity Disconnect (minutes): 10

Settings Acquired via PPTP

SonicWALL IP Address: 0.0.0.0

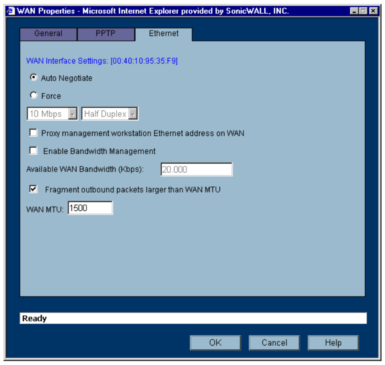
DNS Server 1: 0.0.0.0

Gateway Address: 0.0.0.0

DNS Server 2: 0.0.0.0

Ready

9. Enter your user name in the **User Name** field.
10. Enter your password in the **User Password** field.
11. Enter the IP address of the PPTP Server in the **PPTP Server IP Address** field.
12. Enter the host name of the PPTP Client in the **PPTP (Client) Host Name** field.
13. Select **Inactivity Disconnect (minutes)** to end the connection after a specified time of inactivity.
14. Once a connection is established, the SonicWALL WAN IP address, the Gateway address and the DNS Server IP addresses are displayed in the **Settings Acquired via PPTP** section.
15. Click the **Ethernet** tab. The **Ethernet** tab allows you to manage the Ethernet settings of links connected to the SonicWALL.



WAN Properties - Microsoft Internet Explorer provided by SonicWALL, INC.

WAN Interface Settings: [00:40:10:95:35:F9]

● Auto Negotiate

○ Force

10 Mbps   Half Duplex

☐ Proxy management workstation Ethernet address on WAN

☐ Enable Bandwidth Management

Available WAN Bandwidth (Kbps): 20.000

☑ Fragment outbound packets larger than WAN MTU

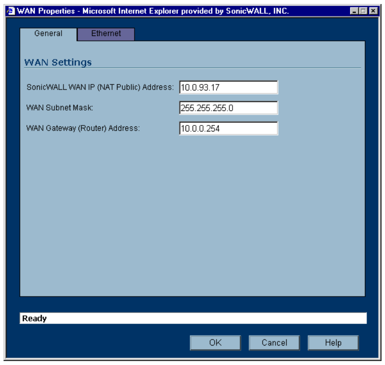
WAN MTU: 1500

Ready

16. **Auto Negotiate** is selected by default because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you select **Force**, you must force the connection speed and duplex from the Ethernet card to the SonicWALL as well.
17. If you select **Force**, select the speed and duplex from the pulldown menus.
18. **Fragment outbound packets larger than WAN MTU** is selected by default. If the MTU size is too large, it requires more transmissions if the packet encounters a router unable to handle a larger packet. The default value is 1500 octets based on the Ethernet standard MTU. The minimum packet size is 68 octets. Decreasing the packet size may improve network performance.
19. Click **OK**.

Configuring LAN Properties for NAT with PPTP Client

1. Click the Notepad icon in the LAN entry of the Interfaces table. The **LAN Properties** window is displayed.



WAN Properties - Microsoft Internet Explorer provided by SonicWALL, INC.

WAN Settings

SonicWALL WAN IP (NAT Public) Address: 10.0.93.17

WAN Subnet Mask: 255.255.255.0

WAN Gateway (Router) Address: 10.0.0.254

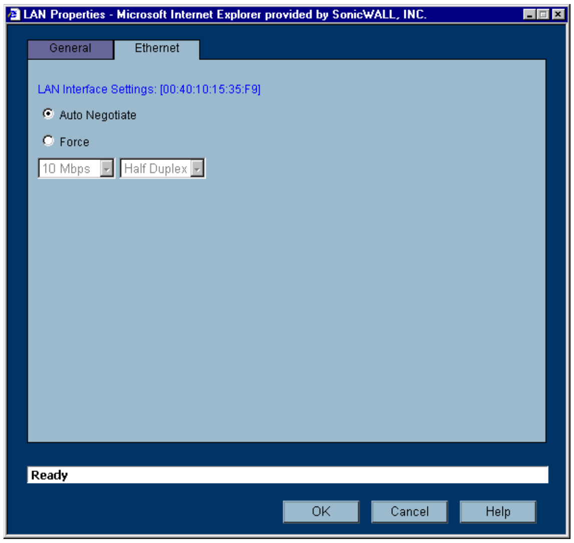
1. In the **LAN Settings** section, enter a valid private IP address in the **SonicWALL LAN IP (NAT Public) Address** field.

2. Enter the subnet mask in the **LAN Subnet Mask** field.

Multiple LAN Subnet Mask Support

This features supports legacy networks incorporating the SonicWALL, and makes it easier to add more nodes if the original subnet is full. To configure this feature, you must have an additional IP address assigned to the SonicWALL. All users on the subnet must use this address as their default router/gateway address.

3. Click **Add**. The **Add LAN Subnet Entry** window is displayed.
4. Enter the LAN IP address in the **IP Address** field.
5. Enter the subnet in the **Subnet Mask** field.
6. Select an entry and click **Edit** to change the information.
7. Select an entry and click **Delete** to remove the entry from the table.
8. Click **Delete All** to remove all the entries in the table.
9. Click the **Ethernet** tab. The **Ethernet** tab allows you to manage the Ethernet settings of links connected to the SonicWALL.



LAN Properties - Microsoft Internet Explorer provided by SonicWALL, INC.

LAN Interface Settings: [00:40:10:15:35:F9]

● Auto Negotiate

○ Force

10 Mbps | Half Duplex

10. **Auto Negotiate** is selected by default because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you select **Force**, you must force the connection speed and duplex from the Ethernet card to the SonicWALL as well.

11. If you select **Force,** select the speed and duplex from the pulldown menus.
12. Click **OK**. Then click **Apply** on the **Network>Settings** page.
13. Restart the SonicWALL for the changes to take effect.

DNS Settings

DNS (Domain Name System) is a hierarchical system for identifying hosts on the Internet or on a private, corporate TCP/IP internetwork. It is a method for identifying hosts with friendly names instead of IP addresses as well as a method for locating hosts. Hosts are located by resolving their names into their associated IP addresses so network communication can be initiated with the host computer.

You can enter up to three IP addresses in the **DNS Settings** section. However, at least one IP address of a DNS Server is required to resolve host names to IP addresses or IP addresses to host names.

Note: *It is strongly recommended to have at least two DNS IP addresses configured on the SonicWALL. This provides redundancy in the event one DNS server is unavailable.*

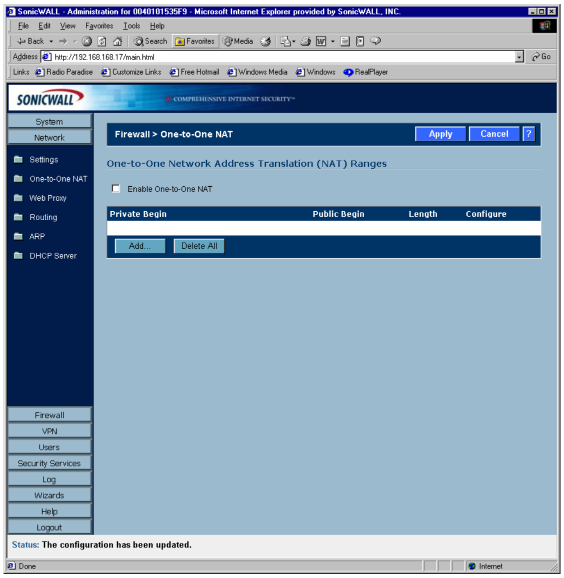
1. Enter the IP address in the **DNS Server 1** field.
2. Enter the second IP address in the **DNS Server 2** field.
3. Click **Apply** for the changes to take effect on the SonicWALL.

Network>One-to-One NAT

One-to-One NAT maps valid, external addresses to private addresses hidden by NAT. Computers on your private LAN are accessed on the Internet at the corresponding public IP addresses.

You can create a relationship between internal and external addresses by defining internal and external address ranges. Once the relationship is defined, the computer with the first IP address of the private address range is accessible at the first IP address of the external address range, the second computer at the second external IP address, etc.

To configure One-to-One NAT, select the **Network>One-to-One NAT** page.


SonicWALL - Administration for 0040101535F9 - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.17/main.html Go
Links Radio Paradise Customize Links Free Hotmail Windows Media Windows RealPlayer
SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Settings
One-to-One NAT
Web Proxy
Routing
ARP
DHCP Server
Firewall
VPN
Users
Security Services
Log
Wizards
Help
Logout
Apply
Cancel
?
Add...
Delete All
Done
Internet

Firewall > One-to-One NAT

One-to-One Network Address Translation (NAT) Ranges

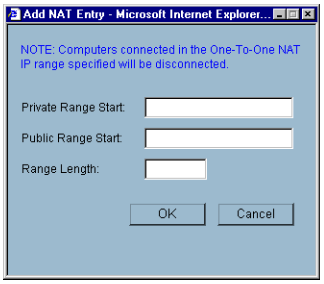
☐ Enable One-to-One NAT

Private Begin	Public Begin	Length	Configure

Status: The configuration has been updated.

To configure One-to-One NAT, complete the following instructions.

1. Select the **Enable One-to-One NAT** check box.
2. Click **Add**.



Add NAT Entry - Microsoft Internet Explorer...

NOTE: Computers connected in the One-To-One NAT IP range specified will be disconnected.

Private Range Start:

Public Range Start:

Range Length:

3. Enter the beginning IP address of the private address range being mapped in the **Private Range Start** field. This is the IP address of the first machine that is accessible from the Internet.
4. Enter the beginning IP address of the valid address range being mapped in the **Public Range Begin** field. This address should be assigned by your ISP and be in the same logical subnet as the NAT public IP address.

Alert! *Do not include the SonicWALL WAN IP (NAT Public) Address or the WAN Gateway (Router) Address in this range.*

5. Enter the number of public IP addresses that should be mapped to private addresses in the Range Length field. The range length can not exceed the number of valid IP addresses. Up to 64 ranges can be added. To map a single address, enter a Range Length of 1.
6. Click **OK**.
7. Click **Apply**. Once the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the browser window.

Alert! *One-to-One NAT maps valid, public IP addresses to private LAN IP addresses. It does not allow traffic from the Internet to the private LAN.*

Tip! *After One-to-One NAT is configured, create an Allow rule to permit traffic from the Internet to the private IP address(es) on the LAN.*

To edit an existing entry in the One-to-One Network Address Translation (NAT) Ranges, click the Notepad icon. To delete an entry, click the Trashcan icon. To delete all entries, click **Delete All**.

One-to-One NAT Configuration Example

This example assumes that you have a SonicWALL running in the NAT-enabled mode, with IP addresses on the LAN in the range 192.168.1.1 - 192.168.1.254, and a WAN IP address of 208.1.2.2. Also, you own the IP addresses in the range 208.1.2.1 - 208.1.2.6.

Alert! *If you have only one IP address from your ISP, you cannot use One-to-One NAT.*

You have three web servers on the LAN with the IP addresses of 192.168.1.10, 192.168.1.11, and 192.168.1.12. Each of the servers must have a default gateway pointing to 192.168.1.1, the SonicWALL LAN IP address.

You also have three additional IP addresses from your ISP, 208.1.2.4, 208.1.2.5, and 208.1.2.6, that you want to use for three additional web servers. Use the following steps to configure One-to-One NAT:

1. Select **Enable One-to-One NAT**.
2. Click **Add**.
3. Enter in the IP address, 192.168.1.10, in the **Private Range Begin** field.
4. Enter in the IP address, 208.1.2.4, in the **Public Range Begin** field.
5. Enter in 3 in the **Range Length** field.

Tip! *You can configure the IP addresses individually, but it is easier to configure them in a range. However, the IP addresses on both the private and public sides must be consecutive to configure a range of addresses.*

6. Click **OK**.
7. Click **Apply**.
8. Click **Firewall**, then **Access Rules**.
9. Click **Add**.
10. Configure the following settings:

- **Allow**
- **Service** - HTTP
- **Source** - WAN
- **Destination** - LAN 192.168.1.10 - 192.168.1.12

In the **Options** tab, select **always** from the **Apply this Rule** menu.

Click **OK**.

Requests for <http://208.1.2.4> are answered by the server at 192.168.1.10. Requests for <http://208.1.2.5> are answered by the server at 192.168.1.11, and requests for <http://208.1.2.6> are answered by the server at 192.168.1.12. From the LAN, the servers can only be accessed using the private IP addresses (192.168.1.x), not the public IP addresses or domain names. For example, from the LAN, you must use URLs like <http://192.168.1.10> to reach the web servers. An IP address, such as 192.168.1.10, on the LAN cannot be used in both public LAN server configurations and in public LAN server One-to-One NAT configurations.

Network>Web Proxy

A Web proxy server intercepts HTTP requests and determines if it has stored copies of the requested Web pages. If it does not, the proxy completes the request to the server on the Internet, returning the requested information to the user and also saving it locally for future requests.

Setting up a Web proxy server on a network can be cumbersome, because each computer on the network must be configured to direct Web requests to the server.

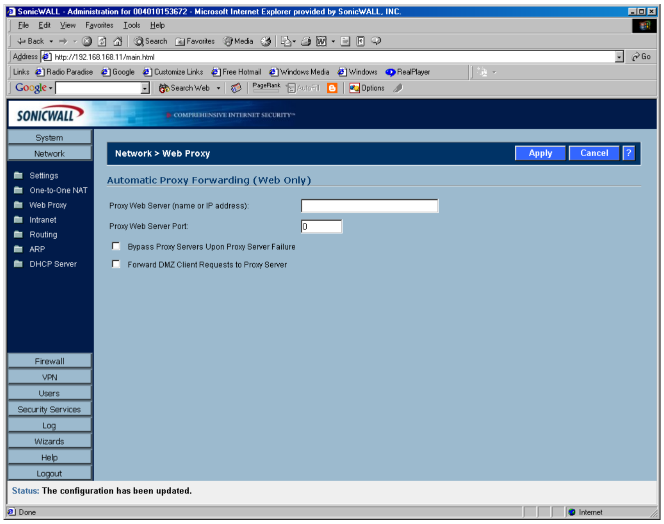
If you have a proxy server on your network, instead of configuring each computer's Web browser to point to the proxy server, you can move the server to the WAN and enable Web Proxy Forwarding. The SonicWALL automatically forwards all Web proxy requests to the proxy server without requiring all the computers on the network to be configured.

Configuring Automatic Proxy Forwarding (Web Only)

⚠

Alert! *The proxy server must be located on the WAN; it can not be located on the LAN.*

To configure a Proxy Web sever, select the **Network>Web Proxy** page.



SonicWALL - Administration for 004010153672 - Microsoft Internet Explorer provided by SonicWALL, INC.

Address: http://192.168.168.11/main.html

Network > Web Proxy

Automatic Proxy Forwarding (Web Only)

Proxy Web Server (name or IP address):

Proxy Web Server Port: 0

☐ Bypass Proxy Servers Upon Proxy Server Failure

☐ Forward DMZ Client Requests to Proxy Server

Status: **The configuration has been updated.**

1. Connect your Web proxy server to a hub, and connect the hub to the SonicWALL WAN port.
2. Enter the name or IP address of the proxy server in the **Proxy Web Server (name or IP address)** field.
3. Enter the proxy IP port in the **Proxy Web Server Port** field.
4. To bypass the Proxy Servers if a failure occurs, select the **Bypass Proxy Servers Upon Proxy Server Failure** check box.
5. Select **Forward OPT/DMZ Client Requests to Proxy Server** if you have clients configured on the SonicWALL OPT/DMZ port.
6. Click **Apply**. Once the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the browser window.

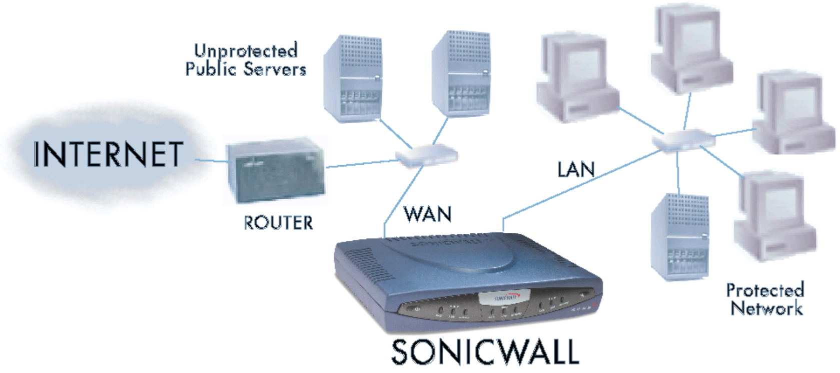
Bypass Proxy Servers Upon Proxy Failure

If a Web proxy server is specified on the **Network>Web Proxy** page, selecting the **Bypass Proxy Servers Upon Proxy Server Failure** check box allows clients behind the SonicWALL to bypass the Web proxy server in the event it becomes unavailable. Instead, the client’s browser accesses the Internet directly as if a Web proxy server is not specified.

Network>Intranet

The SonicWALL can be configured as an Intranet firewall to prevent network users from accessing sensitive servers. By default, users on your LAN can access the Internet router, but not devices connected to the WAN port of the SonicWALL. To enable access to the area between the SonicWALL WAN port and the Internet, you must configure the Intranet settings on the SonicWALL on the **Network>Intranet** page.

Intranet firewalling is achieved by connecting the SonicWALL between an unprotected and a protected segment, as shown below.



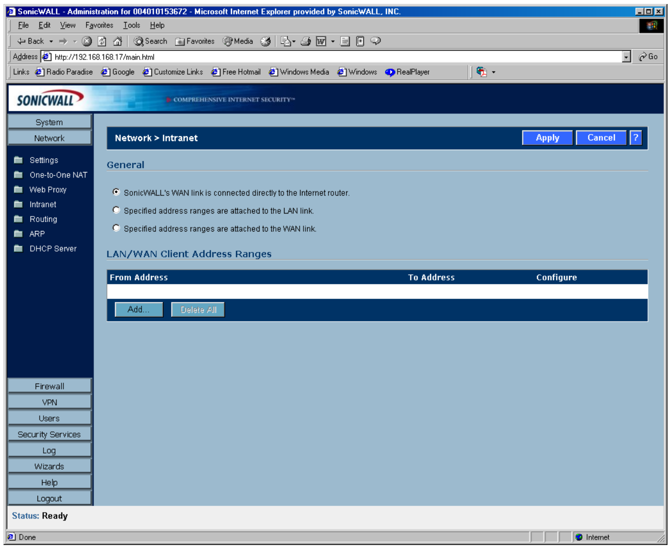
Installation

1. Connect the LAN Ethernet port on the back of the SonicWALL to the network segment to be protected against unauthorized access.

Alert! *Devices connected to the WAN port do not have firewall protection. It is recommended that you use another SonicWALL Internet security appliance to protect computers on the WAN.*

2. Connect the SonicWALL to a power outlet and make sure the SonicWALL is powered on.

To enable an Intranet firewall, you must specify which machines are located on the LAN, or you must specify which machines are located on the WAN.


SonicWALL - Administration for 004010153672 - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.17/main.html
Go
Links Radio Paradise Google Customize Links Free Hotmail Windows Media Windows RealPlayer
SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Settings
One-to-One NAT
Web Proxy
Intranet
Routing
ARP
DHCP Server
Firewall
VPN
Users
Security Services
Log
Wizards
Help
Logout
Apply
Cancel
?
Add...
Delete All
Done
Internet

Network > Intranet

General

● SonicWALL's WAN link is connected directly to the Internet router.

○ Specified address ranges are attached to the LAN link.

○ Specified address ranges are attached to the WAN link.

LAN/WAN Client Address Ranges

From Address	To Address	Configure

Status: Ready

It is best to select the network area with the least number of machines. For example, if only one or two machines are connected to the WAN, select **Specified address ranges are attached to the WAN link**. That way, you only have to enter one or two IP addresses in the **Add Range** section. Specify the IP addresses individually or as a range.

Intranet Settings

Select one of the following four options:

- **SonicWALL WAN link is connected directly to the Internet router**
- Select this option if the SonicWALL is protecting your entire network. This is the default setting.
- **Specified address ranges are attached to the LAN link**
- Select this option if it is easier to specify the devices on your LAN. Then enter your LAN IP address range(s). If you do not include all computers on your LAN, the computers not included will be unable to send or receive data through the SonicWALL.
- **Specified address ranges are attached to the WAN link**
- Select this option if it is easier to specify the devices on your WAN. Then enter your WAN IP address range(s). Computers connected to the WAN port that are not included are inaccessible to users on your LAN.
- **Add Range**
- To add a range of addresses, such as “199.2.23.50” to “199.2.23.54”, enter the starting address in the **From Address** field and the ending address in the **To Address** field. An individual IP address should be entered in the **From Address** field only.

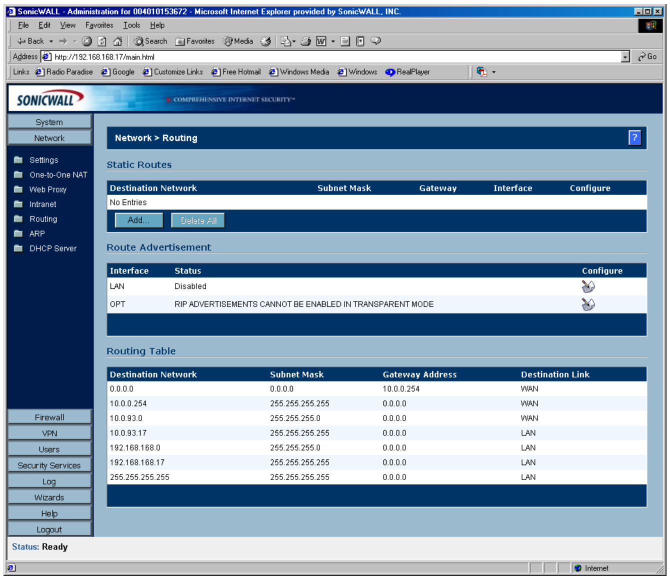
Tip! *Up to 64 address ranges can be entered.*

3. Click **Update**. Once the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the browser window.

Network>Routing

If you have routers on your LAN, OPT/DMZ, or WAN, you can configure static routes on the SonicWALL using the settings on the **Network>Routing** page. Static routing means configuring the SonicWALL to route network traffic to a specific, predefined destination.

Static routes must be defined if the LAN, OPT/DMZ, or WAN are segmented into subnets, either for size or practical considerations. For example, a subnet can be created to isolate a section of a company, such as finance, from network traffic on the rest of the LAN, OPT/DMZ, or WAN.


SonicWALL - Administration for 004010153672 - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.17/main.html Go
Links Radio Paradise Google Customize Links Free Hotmail Windows Media Windows RealPlayer
SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Settings
One-to-One NAT
Web Proxy
Intranet
Routing
ARP
DHCP Server
Firewall
VPN
Users
Security Services
Log
Wizards
Help
Logout
Internet

Network > Routing

Static Routes

Destination Network	Subnet Mask	Gateway	Interface	Configure
No Entries				

Add... Delete All

Route Advertisement

Interface	Status	Configure
LAN	Disabled	
OPT	RIP ADVERTISEMENTS CANNOT BE ENABLED IN TRANSPARENT MODE	

Routing Table

Destination Network	Subnet Mask	Gateway Address	Destination Link
0.0.0.0	0.0.0.0	10.0.0.254	WAN
10.0.0.254	255.255.255.255	0.0.0.0	WAN
10.0.93.0	255.255.255.0	0.0.0.0	WAN
10.0.93.17	255.255.255.255	0.0.0.0	LAN
192.168.168.0	255.255.255.0	0.0.0.0	LAN
192.168.168.17	255.255.255.255	0.0.0.0	LAN
255.255.255.255	255.255.255.255	0.0.0.0	LAN

Status: Ready

Static Routes

Static Routes are configured when network traffic is directed to subnets located behind routers on your network. For instance, you have a router on your network with the IP address of 192.168.168.254, and there is another subnet on your network with IP address range of 10.0.5.0 - 10.0.5.254 with a subnet mask of 255.255.255.0. To configure a static route to the 10.0.5.0 subnet, follow these instructions:

1. Click **Network**, then **Routing**.
2. Click **Add** in the **Static Routes** section.
3. Enter 10.0.5.0 in the **Destination Network** field.
4. Enter 255.255.255.0 in the **Subnet Mask** field.
5. Enter 192.168.168.254 in the **Default Gateway** field. This is the IP address of the router.
6. Select **LAN** from the **Interface** menu.
7. Click **OK.**

Tip! *You can configure up to 256 routes on the SonicWALL.*

Static Route Configuration Example

Static Route configurations allow for multiple subnets separated by an internal (LAN) router to be supported behind the sonicwall LAN. This option is only be used when the secondary subnet is accessed through an internal (LAN) router that is between it and the Sonicwall LAN port. Once static routes are configured, network traffic can be directed to these subnets.

Key terms:

- **Destination Network**: the network IP address of the remote subnet. The address usually ends in 0, i.e 10.0.5.0.
- **Subnet Mask**: the subnet mask of the remote network (i.e. 255.255.255.0)
- **Gateway**: the IP address of the Internal (LAN) router that is local to the sonicwall.

For example:

SonicWALL LAN IP Address: 192.168.168.1
Subnet mask: 255.255.255.0
Router IP Address: 192.168.168.254
Secondary Subnet: 10.0.5.0
Subnet mask: 255.255.255.0

If you have an Internal (LAN) router on your network with the IP address of 192.168.168.254, and there is another subnet on your network with IP address range of 10.0.5.0 - 10.0.5.254 with a subnet mask of 255.255.255.0. To configure a static route to the 10.0.5.0 subnet, follow these instructions:

Click **Network**, and then **Routing**.

1. Click **Add** in the **Static Routes** section.
2. Enter 10.0.5.0 in the **Destination Network** field.
3. Enter 255.255.255.0 in the **Subnet Mask** field.
4. Enter 192.168.168.254 in the **Default Gateway** field. This is the IP address of the internal (LAN) router that is local to the SonicWall.
5. Select **LAN** from the **Interface** menu.
6. Click **OK**.

Tip! *Be sure the Internal (LAN) router is configured as follows: If the SonicWall is in NAT Enabled mode, the internal (LAN) router needs to have a route of last resort (i.e. gateway address) that is the SonicWall LAN IP address.*

Route Advertisement

The SonicWALL uses RIPv1 or RIPv2 to advertise its static and dynamic routes to other routers on the network. Changes in the status of VPN tunnels between the SonicWALL and remote VPN gateways are also reflected in the RIPv2 advertisements. Choose between RIPv1 or RIPv2 based on your router's capabilities or configuration. RIPv1 is an earlier version of the protocol that has fewer features, and it also sends packets via broadcast instead of multicast. RIPv2 packets are backwards-compatible and can be accepted by some RIPv1 implementations that provide an option of listening for multicast packets. The RIPv2 Enabled (broadcast) selection broadcasts packets instead of multicasting packets is for heterogeneous networks with a mixture of RIPv1 and RIPv2 routers.

To enable Route Advertisement, click the Notepad icon in the **Configure** column for each interface.

1. Select one of the following types of RIP Advertisements:

   •**RIPv1 Enabled** - RIPv1 is the first version of Routing Information Protocol.

- **RIPv2 Enabled (multicast)** - to send route advertisements using multicasting (a single data packet to specific notes on the network).
- **RIPv2 Enabled (broadcast)** - to send route advertisements using broadcasting (a single data packet to all nodes on the network).

2. Select **Never**, or **When WAN is up**, or **Always** from the **Advertise Default Route** menu.
3. **Advertise Static Routes** - If you have static routes configured on the SonicWALL, enable this feature to exclude them from Route Advertisement.
4. **Advertise VPN destination networks** - select to advertise VPN networks.
   - **Route Change Damp Time (seconds**) - is the delay between the time a VPN tunnel changes state (up or down) and the time the change is advertised with RIP. The delay, in seconds, prevents ambiguous route advertisements sent as a result of a temporary change in a VPN tunnel status. Enter a value in seconds between advertisements broadcasted over the network in the Route **Change Damp Time (seconds)** field. The default value is 30 seconds. A lower value corresponds with a higher volume of broadcast traffic over the network.
5. **Deleted Route Advertisements** - enter the number of advertisements that a deleted route broadcasts until it stops in the **Deleted Route Advertisements** field. The default value is 5.
6. **Route Metric (1-15)** - Enter a value from 1 to 15 in the **Route Metric** field. This is the number of times a packet touches a router from the source IP address to the destination IP address.
7. **RIPv2 Route Tag (4 Hex Digits**) - If RIPv2 is selected from the **Route Advertisements** menu, you can enter a value for the Route Tag. This value is implementation-dependent and provides a mechanism for routers to classify the originators of RIPv2 advertisements. This field is optional.
8. **RIPv2 Authentication** You can enable RIPv2 Authentication by selecting the type of authentication from the menu:
   - **User defined** - Enter 4 hex digits in the **Authentication Type (4 hex digits)** field. Enter 32 hex digits in the **Authentication Data (32 Hex Digits)** field.
   - **Cleartext Password** - Enter a password in the **Authentication Password (Max 16 Chars)** field. A maximum of 16 characters can be used to define a password.
9. **MD5 Digest** - Enter a numerical value from 0-255 in the Authentication Key-Id (0-255) field. Enter a 32 hex digit value for the **Authentication Key (32 hex digits)** field, or use the generated key.

Route Table

The **Route Table** is a list of destinations that the IP software maintains on each host and router.

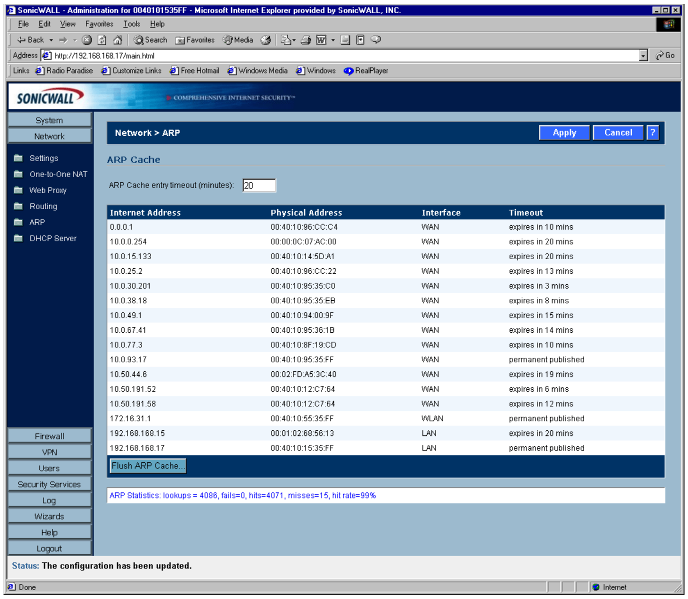
Click **Route Table** to display routing information on the SonicWALL.

The network IP address, subnet mask, gateway address, and the corresponding link are displayed.

Most of the entries are the result of configuring LAN and WAN network settings. The SonicWALL LAN, or OPT/DMZ, and WAN IP addresses are displayed as permanently published at all times.

Network>ARP

The ARP (Address Resolution Protocol) Cache stores IP or logical addresses received from ARP replies in order to minimize the number of ARP broadcasts on a network. ARP broadcasts can degrade network performance if too many broadcast requests are sent over the network. Once the ARP request is stored, the host does not have to send out ARP requests for the same IP datagram.


SonicWALL - Administration for 0040101535FF - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.17/main.html
Go
Links Radio Paradise Customize Links Free Hotmail Windows Media Windows RealPlayer
SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Settings
One-to-One NAT
Web Proxy
Routing
ARP
DHCP Server
Firewall
VPN
Users
Security Services
Log
Wizards
Help
Logout
Network > ARP
Apply
Cancel
?
ARP Cache
Flush ARP Cache...
Done
Internet

ARP Cache entry timeout (minutes): 20

Internet Address	Physical Address	Interface	Timeout
0.0.0.1	00:40:10:96:CC:C4	WAN	expires in 10 mins
10.0.0.254	00:00:0C:07:AC:00	WAN	expires in 20 mins
10.0.15.133	00:40:10:14:5D:A1	WAN	expires in 20 mins
10.0.25.2	00:40:10:96:CC:22	WAN	expires in 13 mins
10.0.30.201	00:40:10:95:35:C0	WAN	expires in 3 mins
10.0.38.18	00:40:10:95:35:EB	WAN	expires in 8 mins
10.0.49.1	00:40:10:94:00:9F	WAN	expires in 15 mins
10.0.67.41	00:40:10:95:36:1B	WAN	expires in 14 mins
10.0.77.3	00:40:10:8F:19:CD	WAN	expires in 10 mins
10.0.93.17	00:40:10:95:35:FF	WAN	permanent published
10.50.44.6	00:02:FD:A5:3C:40	WAN	expires in 19 mins
10.50.191.52	00:40:10:12:C7:64	WAN	expires in 6 mins
10.50.191.58	00:40:10:12:C7:64	WAN	expires in 12 mins
172.16.31.1	00:40:10:55:35:FF	WLAN	permanent published
192.168.168.15	00:01:02:68:56:13	LAN	expires in 20 mins
192.168.168.17	00:40:10:15:35:FF	LAN	permanent published

ARP Statistics: lookups = 4086, fails=0, hits=4071, misses=15, hit rate=99%

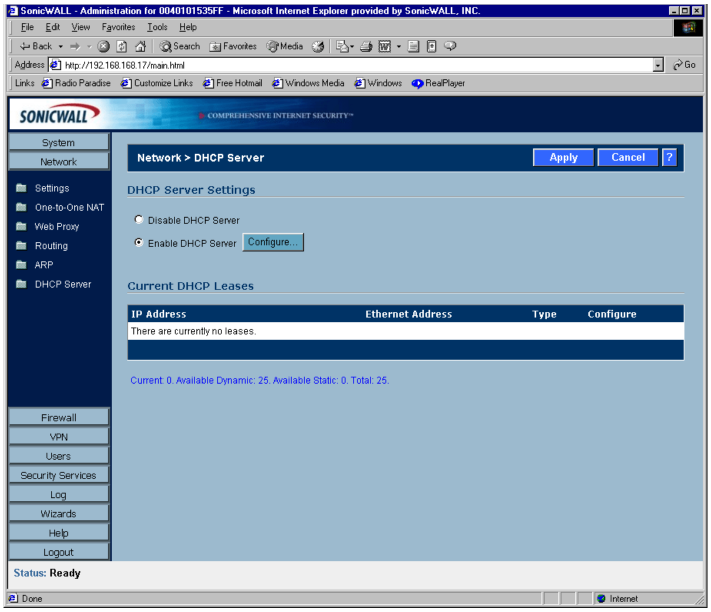
Status: The configuration has been updated.

It is sometimes necessary to flush the ARP cache if the IP address has changed for a device on the network. Since the IP address is linked to a physical address, the IP address can change but still be associated with the physical address in the ARP Cache. Flushing the ARP Cache allows new information to be gathered and stored in the ARP Cache. Click **Flush ARP Cache** to clear the information.

To configure a specific length of time for the entry to time out, enter a value in minutes in the **ARP Cache entry time out (minutes)** field.

Network>DHCP Server

The SonicWALL DHCP Server distributes IP addresses, subnet masks, gateway addresses, and DNS server addresses to the computers on your network.


SonicWALL - Administration for 0040101535FF - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.17/main.html
Go
Links Radio Paradise Customize Links Free Hotmail Windows Media Windows RealPlayer
SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Settings
One-to-One NAT
Web Proxy
Routing
ARP
DHCP Server
Firewall
VPN
Users
Security Services
Log
Wizards
Help
Logout
Network > DHCP Server
Apply
Cancel
?
Configure...
Done
Internet

DHCP Server Settings

○ Disable DHCP Server

● Enable DHCP Server

Current DHCP Leases

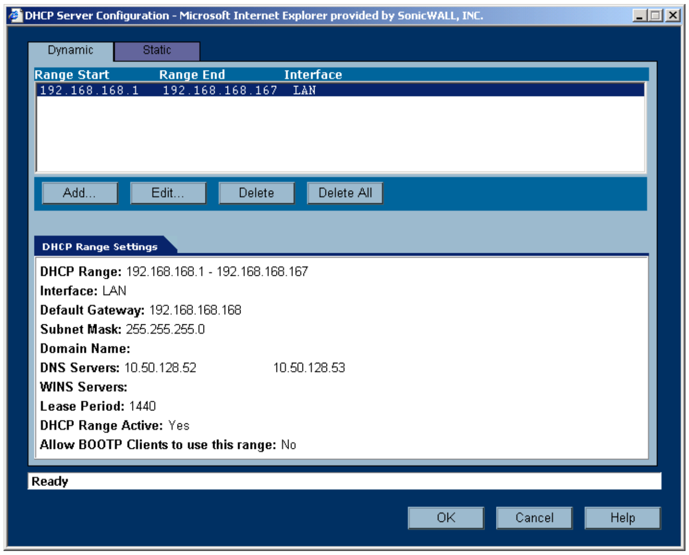
IP Address	Ethernet Address	Type	Configure
There are currently no leases.			

Current: 0. Available Dynamic: 25. Available Static: 0. Total: 25.

Status: Ready

DHCP Settings

To enable the DHCP Server feature on the SonicWALL, select **Enable DHCP Server**, and click **Configure**. The **DHCP Server Configuration** window is displayed.


DHCP Server Configuration - Microsoft Internet Explorer provided by SonicWALL, INC.
Dynamic
Static
Add...
Edit...
Delete
Delete All
DHCP Range Settings
OK
Cancel
Help

Range Start	Range End	Interface
192.168.168.1	192.168.168.167	LAN

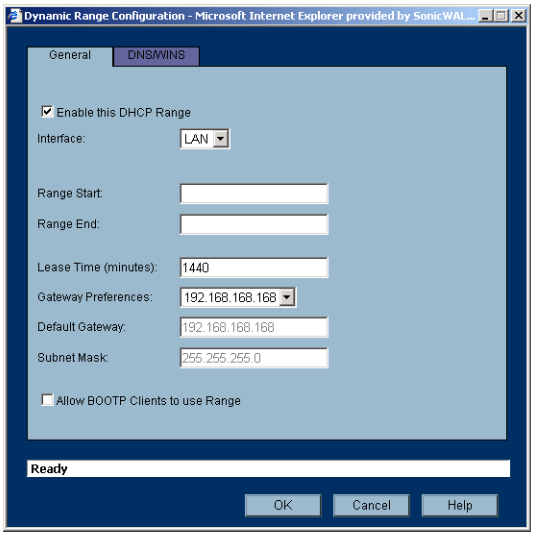
DHCP Range: 192.168.168.1 - 192.168.168.167
Interface: LAN
Default Gateway: 192.168.168.168
Subnet Mask: 255.255.255.0
Domain Name:
DNS Servers: 10.50.128.52 10.50.128.53
WINS Servers:
Lease Period: 1440
DHCP Range Active: Yes
Allow BOOTP Clients to use this range: No

Ready

Configuring DHCP Server for Dynamic Ranges

In the **Dynamic Ranges** table, the **Range Start**, **Range End**, and **Interface** information is displayed. To add ranges to the table, click **Add.**

The **Dynamic Ranges Configuration** window is displayed.



Dynamic Range Configuration - Microsoft Internet Explorer provided by SonicWAL...

☑ Enable this DHCP Range

Interface: LAN

Range Start:

Range End:

Lease Time (minutes): 1440

Gateway Preferences: 192.168.168.168

Default Gateway: 192.168.168.168

Subnet Mask: 255.255.255.0

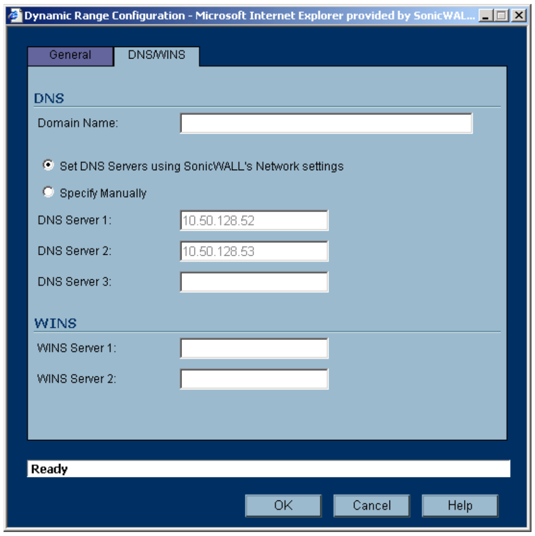
☐ Allow BOOTP Clients to use Range

Ready

The General Tab

1. Select **LAN** or **OPT/DMZ** from the **Interface** menu. If **LAN** is selected, the IP addresses are in the same private subnet as the SonicWALL LAN. If **OPT/DMZ** is selected, the IP addresses are in the same private subnet as the SonicWALL OPT/DMZ.
2. Enter the beginning IP address in the **Range Start** field. The default IP address is appropriate for most networks.
3. Enter the last IP address in the **Range End** field. If there are more than 25 computers on your network, enter the appropriate ending IP address in the **Range End** field.
4. Enter the number of minutes an IP address is used before it is issued another IP address in the **Lease Time (minutes)** field. 60 minutes is the default value.
5. Select the gateway from the **Gateway Preferences** menu. The LAN IP address is the default value, but you can select **Other** and enter a different IP address for the gateway.
6. If you select the SonicWALL LAN IP address from the **Gateway Preferences** menu, the **Default Gateway** and **Subnet Mask** fields are unavailable. If you select **Other**, the fields are available for you to enter the Default Gateway and Subnet Mask information into the fields.
7. Select **Allow BOOTP Clients to use Range** if you have BOOTP Clients on your network.
8. Click the **DNS/WINS** tab to continue configuring the DHCP Server feature.

The DNS/WINS Tab



Dynamic Range Configuration - Microsoft Internet Explorer provided by SonicWAL...

General | DNS/WINS

DNS

Domain Name:

● Set DNS Servers using SonicWALL's Network settings

○ Specify Manually

DNS Server 1: 10.50.128.52

DNS Server 2: 10.50.128.53

DNS Server 3:

WINS

WINS Server 1:

WINS Server 2:

Ready

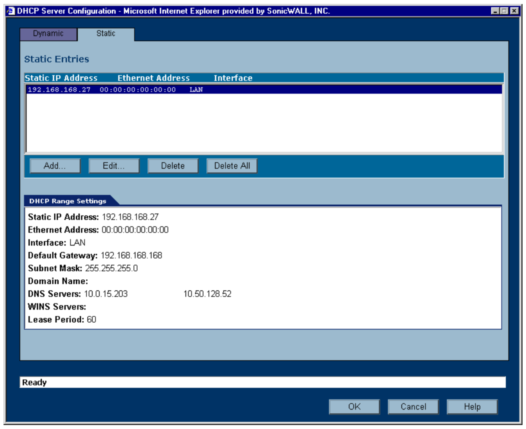
9. If you have a domain name for the DNS Server, enter it in the **Domain Name** field.
10. **Set DNS Servers using SonicWALL's Network Settings** is selected by default. When selected, the DNS Server IP fields are unavailable.
11. If you do not want to use the SonicWALL network settings, select **Specify Manually**, and enter the IP address of your DNS Server in the **DNS Server 1** field.

Note: *You must specify at least one DNS server. It is also helpful to have a second DNS IP address in the event the first DNS server is unavailable.*

12. If you have WINS running on your network, enter the WINS server IP address(es) in the **WINS Server 1** field.
13. Click **OK** to add the settings to the SonicWALL.
14. Then click **Apply** for the settings to take effect on the SonicWALL.

Configuring Static DHCP Entries

Click the **Static** tab to add static DHCP entries to the SonicWALL. Static entries are IP addresses assigned to servers requiring permanent IP settings.



DHCP Server Configuration - Microsoft Internet Explorer provided by SonicWALL, INC.

Dynamic | Static

Static Entries

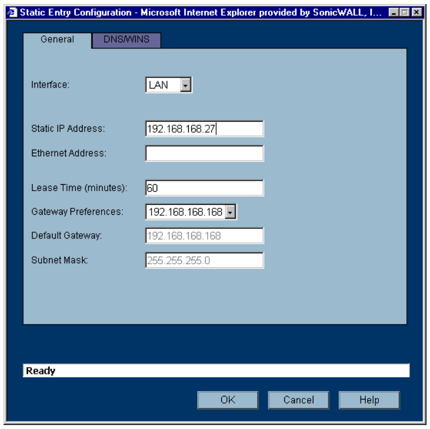
Static IP Address	Ethernet Address	Interface
192.168.168.27	00:00:00:00:00:00	LAN

DHCP Range Settings

Static IP Address: 192.168.168.27
Ethernet Address: 00:00:00:00:00:00
Interface: LAN
Default Gateway: 192.168.168.168
Subnet Mask: 255.255.255.0
Domain Name:
DNS Servers: 10.0.15.203 10.50.128.52
WINS Servers:
Lease Period: 60

Ready

To configure static entries, click **Add**.


Static Entry Configuration - Microsoft Internet Explorer provided by SonicWALL, I...
General
DNS/WINS
OK
Cancel
Help

Interface: LAN

Static IP Address: 192.168.168.27

Ethernet Address:

Lease Time (minutes): 60

Gateway Preferences: 192.168.168.168

Default Gateway: 192.168.168.168

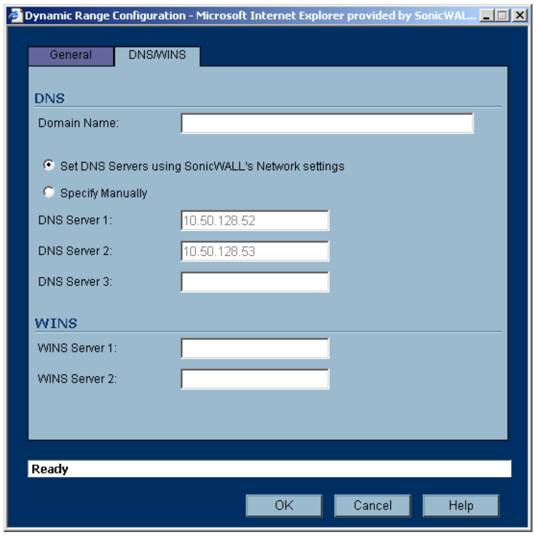
Subnet Mask: 255.255.255.0

Ready

The General Tab

1. Select **LAN** or **OPT/DMZ** from the **Interface** menu. If **LAN** is selected, the IP addresses are in the same private subnet as the SonicWALL LAN. If **OPT/DMZ** is selected, the IP addresses are in the same private subnet as the SonicWALL OPT/DMZ.
2. Enter the device IP address in the **Static IP Address** field.
3. Enter the device Ethernet (MAC) address in the **Ethernet Address** field.
4. Enter the number of minutes an IP address is used before it is issued another IP address in the **Lease Time (minutes)** field. 60 minutes is the default value.
5. Select the gateway from the **Gateway Preferences** menu. The LAN IP address is the default value, but you can select **Other** and enter a different IP address for the gateway.
6. If you select the SonicWALL LAN IP address from the **Gateway Preferences** menu, the **Default Gateway** and **Subnet Mask** fields are unavailable. If you select **Other**, the fields are available for you to enter the Default Gateway and Subnet Mask information into the fields.
7. Select **Allow BOOTP Clients to use Range** if you have BOOTP Clients on your network.
8. Click the **DNS/WINS** tab to continue configuring the DHCP Server feature.

The DNS/WINS Tab


Dynamic Range Configuration - Microsoft Internet Explorer provided by SonicWAL...
General
DNS/WINS
DNS
WINS
OK
Cancel
Help

Domain Name:

● Set DNS Servers using SonicWALL's Network settings

○ Specify Manually

DNS Server 1: 10.50.128.52

DNS Server 2: 10.50.128.53

DNS Server 3:

WINS Server 1:

WINS Server 2:

Ready

9. If you have a domain name for the DNS Server, enter it in the **Domain Name** field.

10. **Set DNS Servers using SonicWALL's Network Settings** is selected by default. When selected, the DNS Server IP fields are unavailable.
11. If you do not want to use the SonicWALL network settings, select **Specify Manually**, and enter the IP address of your DNS Server in the **DNS Server 1** field. You must specify at least one DNS server.
12. If you have WINS running on your network, enter the WINS server IP address(es) in the **WINS Server 1** field.
13. Click **OK** to add the settings to the SonicWALL.

Then click **Apply** for the settings to take effect on the SonicWALL.

Tip! *The SonicWALL DHCP server can assign a total of 254 dynamic and static IP addresses.*

Current DHCP Leases

The current DHCP lease information is displayed in the **Current DHCP Leases** table. Each binding displays the IP address and the Ethernet address along with the type of binding, Dynamic, Dynamic BOOTP, or Static BOOTP. To delete a binding, which frees the IP address on the DHCP server, click the Trashcan icon next to the entry. To edit an entry, click the Notepad icon next to the entry.

5 Configuring the TZ 170 Wireless

The TZ 170 Wireless supports two wireless protocols called IEEE 802.11b and 802.11g, commonly known as Wi-Fi, and sends data via radio transmissions. Wi-Fi transmission speed is usually faster than broadband connection speed, but it is slower than Ethernet.

The SonicWALL TZ 170 Wireless combines three networking components to offer a fully secure wireless firewall: an Access Point, a secure wireless gateway, and a stateful firewall with flexible NAT and VPN termination and initiation capabilities. With this combination, the TZ 170 Wireless offers the flexibility of wireless without compromising network security.

Typically, the TZ 170 Wireless is the access point for your wireless LAN and serves as the central access point for computers on your LAN. In addition, it shares a single broadband connection with the computers on your network. Since the TZ 170 Wireless also provides firewall protection, intruders from the Internet cannot access the computers or files on your network. This is especially important for an “always-on” connection such as a cable modem or T1 line that is shared by computers on a network.

However, wireless LANs are vulnerable to “eavesdropping” by other wireless networks which means you should establish a wireless security policy for your wireless LAN. Wired Equivalent Privacy, WEP, should not be used as your only security policy.

On the TZ 170 Wireless, wireless clients connect to the Access Point layer of the firewall. Instead of bridging the connection directly to the wired network, wireless traffic is first passed to the Secure Wireless Gateway layer where the client is required to be authenticated via User Level Authentication. Access to Wireless Guest Services (WGS) and MAC Filter Lists are managed by the TZ 170 Wireless. It is also at this layer that the TZ 170 Wireless has the capability of enforcing WiFiSec, an IPSec-based VPN overlay for wireless networking. As wireless network traffic successfully passes through these layers, it is then passed to the VPN-NAT-Stateful firewall layer where WiFiSec termination, address translation, and access rules are applied. If all of the security criteria is met, then wireless network traffic can then pass via one of the following Distribution Systems (DS):

- LAN
- WAN
- Wireless Client on the WLAN
- VPN tunnel

Considerations for Using Wireless Connections

- **Mobility** - if the majority of your network is laptop computers, wireless is more portable than wired connections.
- **Convenience** - wireless networks do not require cabling of individual computers or opening computer cases to install network cards.
- **Speed** - if network speed is important to you, you may want to consider using Ethernet connections rather than wireless connections.
- **Range and Coverage** - if your network environment contains numerous physical barriers or interference factors, wireless networking may not be suitable for your network.
- **Security** - wireless networks have inherent security issues due to the unrestricted nature of the wireless transmissions. However, the TZ 170 Wireless is a firewall and has NAT capabilities which provides security, and you can use WiFiSec to secure data transmissions.

Recommendations for Optimal Wireless Performance

- Place the TZ 170 Wireless near the center of your intended network. This can also reduce the possibility of eavesdropping by neighboring wireless networks.
- Minimize the number of walls or ceilings between the TZ 170 Wireless and the receiving points such as PCs or laptops.
- Try to place the TZ 170 Wireless in a direct line with other wireless components. Best performance is achieved when wireless components are in direct line of sight with each other.
- Building construction can make a difference on wireless performance. Avoid placing the TZ 170 Wireless near walls, fireplaces, or other large solid objects. Placing the TZ 170 Wireless near metal objects such as computer cases, monitors, and appliances can affect performance of the unit.
- Metal framing, UV window film, concrete or masonry walls, and metallic paint can reduce signal strength if the TZ 170 Wireless is installed near these types of materials.
- Installing the TZ 170 Wireless in a high place can help avoid obstacles and improve performance for upper stories of a building.
- Neighboring wireless networks and devices can affect signal strength, speed, and range of the TZ 170 Wireless. Also, devices such as cordless phones, radios, microwave ovens, and televisions may cause interference on the TZ 170 Wireless.

Adjusting the TZ 170 Wireless Antennas

The antennas on the TZ 170 Wireless can be adjusted for the best radio reception. Begin with the antennas pointing straight up, and then adjust as necessary. Note that certain areas, such as the area directly below the TZ 170 Wireless, get relatively poor reception. Pointing the antenna directly at another wireless device does not improve reception. Do not place the antennas next to metal doors or walls as this can cause interference.

Wireless Guest Services (WGS)

With your TZ 170 Wireless, you can provide wireless guest services to wireless-equipped users who are not part of your corporate network, for example, a consultant or a sales person. You can offer authenticated wireless users access to the Internet through your TZ 170 Wireless while preventing access to your corporate LAN, or allowing them access to specific resources on the LAN and unencrypted access to the Internet.

When WGS is active, wireless clients can authenticate and associate with the Access Layer of the SonicWALL. When a Web browser is launched, the wireless user is prompted to provide a user name and password to gain access to WGS. The browser is redirected to the HTTP (unencrypted) management address of the TZ 170 Wireless, but the user name and password is not transmitted. Instead, a secure hash is transmitted rendering the information useless to anyone “eavesdropping” on the network. After authentication, users are tracked and controlled by the client MAC address as well as Account and Session lifetimes.

In order to take advantage of Wireless Guest Services, you must provide a guest with a user name and password which they use to authenticate themselves using HTTP and a Web browser, creating a secure HTTP session.

Wireless Node Count Enforcement

Users on the WLAN are not counted towards the node enforcement on the SonicWALL. Only users on the LAN are counted towards the node limit.

MAC Filter List

The SonicWALL TZ 170 wireless networking protocol provides native MAC address filtering capabilities. When MAC address filtering occurs at the 802.11 layer, wireless clients are prevented from authenticating and associating with the wireless access point. Since data communications cannot occur without authentication and association, access to the network cannot be granted until the client has given the network administrator the MAC address of their wireless network card.

The TZ 170 Wireless uses WGS to overcome this limitation by moving MAC address filtering to the Secure Wireless Gateway layer. This allows wireless users to authenticate and associate with the Access Point layer of the SonicWALL, and be redirected to the WGS by the Secure Wireless Gateway where the user authenticates and obtains WLAN to WAN access.

Easy WGS MAC Filtering is an extension of WGS that simplifies the administrative burden of manually adding MAC addresses to the MAC Filter List. Users can add themselves to the MAC Filter List by providing a user name and password assigned to them by the SonicWALL administrator. WGS must be enabled on the TZ 170 Wireless before Easy MAC Filter List can be implemented.

WiFiSec Enforcement

Enabling **WiFiSec Enforcement** on the SonicWALL enforces the use of IPSec-based VPN for access from the WLAN to the WAN or LAN, and provides access from the WLAN to the WAN independent of WGS. Access from one wireless client to another is configured on the **Wireless>Advanced** page where you can disable or enable access between wireless clients.

WiFiSec uses the easy provisioning capabilities of the SonicWALL Global VPN client making it easy for experienced and inexperienced administrators to implement on the network. The level of interaction between the Global VPN Client and the user depends on the WiFiSec options selected by the administrator. WiFiSec IPSec terminates on the WLAN/LAN port, and is configured using the Group VPN Security Policy including noneditable parameters specifically for wireless access.

- **Apply NAT & Firewall Rules** - On
- **Forward Packets to Remote VPNs** - On
- **Default LAN Gateway** - <management IP Address> if left unspecified
- **VPN Terminated at the LAN/WLAN** - to differentiate between VPN Security Associations terminated at the WAN port.

SonicOS Standard Wireless Features and Enhancements

SonicOS Standard introduces a number of new features designed to enhance the functionality, performance, and versatility of the TZ 170 Wireless.

- **Wireless Status Page Updates**
- **Secure Wireless Bridging**
- **802.11b and 802.11g Protocol Support**
- **Enhanced Wireless Guest Services**
- **Dynamic Address Translation**
- **Flexible Default Route**

Wireless Status Page Updates

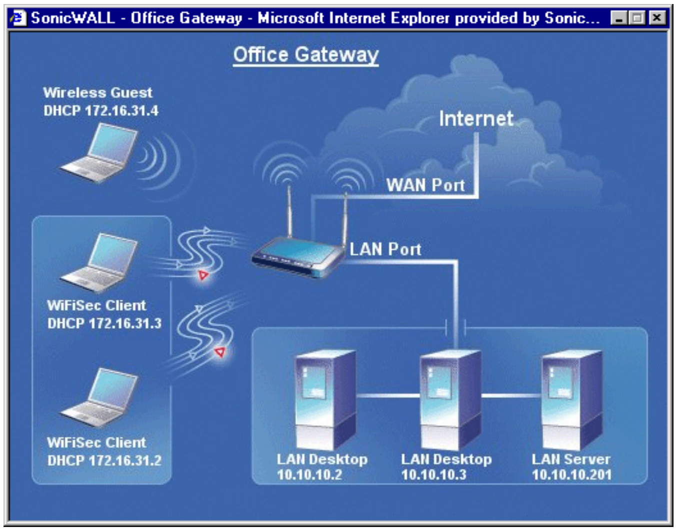
In addition to providing different status views for **Access Point** and **Wireless Bridge** modes, two new functions have been added to the **Wireless > Status** page:

- **Hyperlinked WLAN Settings** - All configurable WLAN settings are now hyperlinked to their respective pages for configuration. (Present in both Access Point and Wireless Bridge modes). Enabled features are displayed in green, and disabled features are displayed in red.

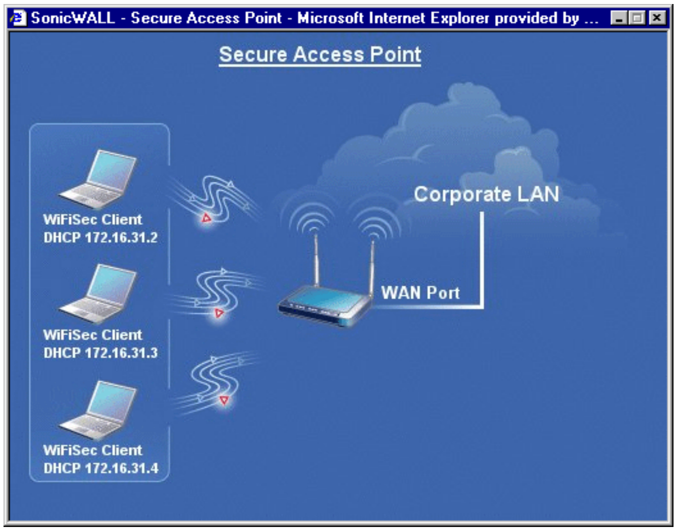
- **Automated Station Blocking** - Previously, the **Station Status** view allowed for stations to be added to the MAC allow list, or disassociated from the TZ 170 Wireless. The disassociated station, however, could easily re-associate unless other prohibitive actions were taken. This functionality has been enhanced by adding the **Block** icon. Clicking this icon disassociates the station and adds the station to the MAC block list.

TZ 170 Wireless Deployment Scenarios

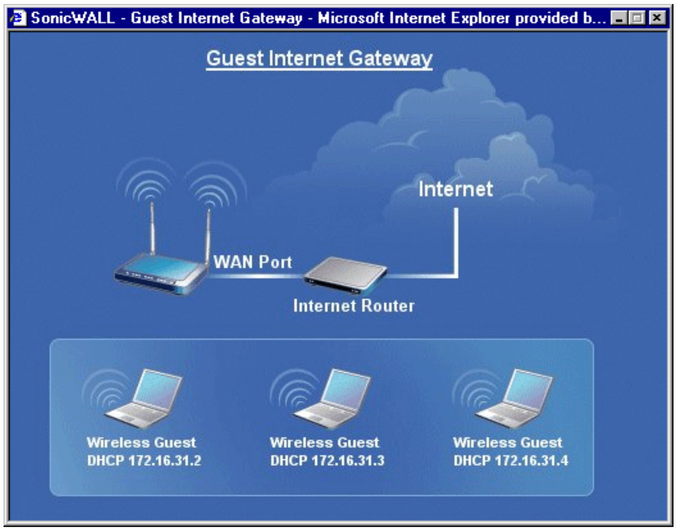
Office Gateway - Provides secure access for wired and wireless users on your network.



Secure Access Point - Add secure wireless access to an existing wireless network.



Guest Internet Gateway - Provide guests controlled wireless access to the Internet only.

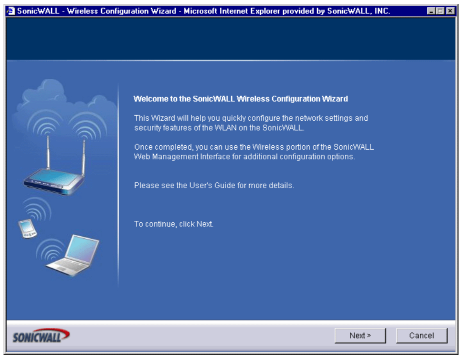


Custom Deployment - View all available options and optimize the configuration for your individual needs.

Configuring the TZ 170 Wireless as an Office Gateway

Log into the TZ 170 Wireless using your administrator's name and password. Click **Wizards**.

Welcome to the SonicWALL Setup Wizard


SonicWALL - Wireless Configuration Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Welcome to the SonicWALL Wireless Configuration Wizard

This Wizard will help you quickly configure the network settings and security features of the WLAN on the SonicWALL.

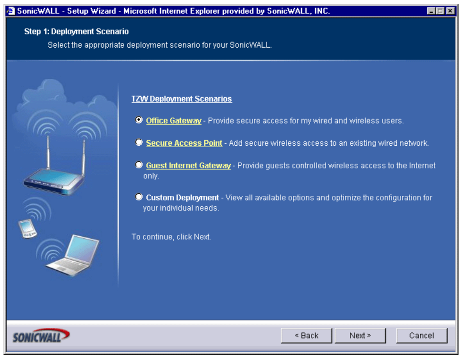
Once completed, you can use the Wireless portion of the SonicWALL Web Management Interface for additional configuration options.

Please see the User's Guide for more details.

To continue, click Next.

1. To begin configuration, click **Next**. Click **Cancel** to close the wizard.

Selecting the Deployment Scenario


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 1: Deployment Scenario

Select the appropriate deployment scenario for your SonicWALL.

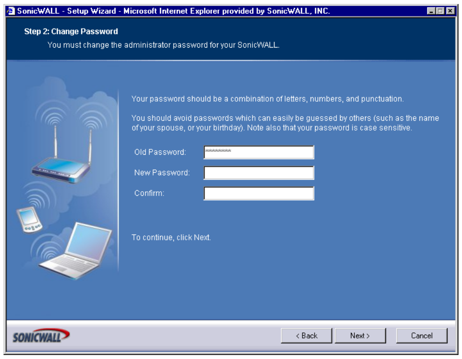
TZW Deployment Scenarios

- ● Office Gateway - Provide secure access for my wired and wireless users.
- ○ Secure Access Point - Add secure wireless access to an existing wired network.
- ○ Guest Internet Gateway - Provide guests controlled wireless access to the Internet only.
- ○ **Custom Deployment** - View all available options and optimize the configuration for your individual needs.

To continue, click Next.

2. Select **Office Gateway** as the deployment scenario. Click **Next**.

Changing the Password


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 2: Change Password

You must change the administrator password for your SonicWALL.

Your password should be a combination of letters, numbers, and punctuation.

You should avoid passwords which can easily be guessed by others (such as the name of your spouse, or your birthday). Note also that your password is case sensitive.

Old Password: **********

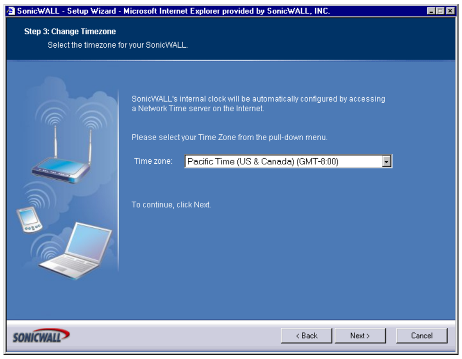
New Password:

Confirm:

To continue, click Next.

3. Type a new password in the **New Password** field. The password should be a unique combination of letters, or number, or symbols, or a combination of all three for the most secure password. Avoid names, birthdays, or any obvious words. Retype the password in the **Confirm** field. Click **Next**.

Selecting Your Time Zone


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 3: Change Timezone

Select the timezone for your SonicWALL.

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

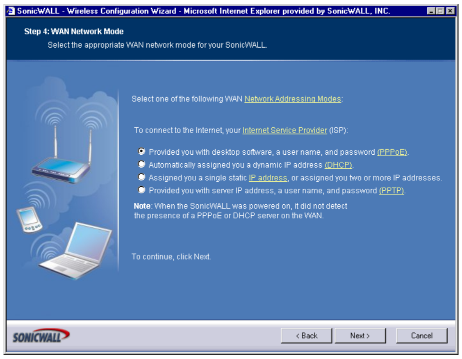
Please select your Time Zone from the pull-down menu.

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

To continue, click Next.

4. Select your Time Zone from the **Time Zone** menu. The SonicWALL uses an internal clock to timestamp logs and other functions requiring time. Click **Next**.

Configuring the WAN Network Mode


SonicWALL - Wireless Configuration Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 4: WAN Network Mode

Select the appropriate WAN network mode for your SonicWALL.

Select one of the following WAN Network Addressing Modes:

To connect to the Internet, your Internet Service Provider (ISP):

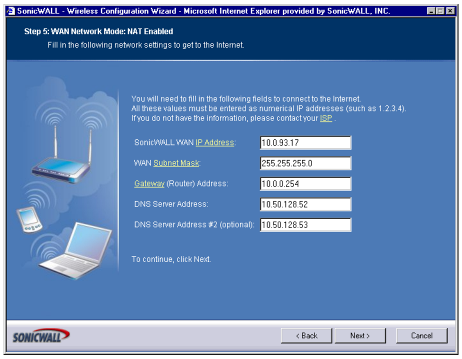
● Provided you with desktop software, a user name, and password (PPPoE).
○ Automatically assigned you a dynamic IP address (DHCP).
○ Assigned you a single static IP address, or assigned you two or more IP addresses.
○ Provided you with server IP address, a user name, and password (PPTP).

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

To continue, click Next.

5. If a DCHP server is detected on the WAN, the SonicWALL defaults to **NAT with DHCP Client** network mode. All WAN network settings are automatically detected and used for the network mode. If a PPPoE server is detected on the WAN, type the user name and password provided to you by your ISP in the **User Name** and **Password** fields. If your ISP has provided you with a single public IP address and other network information, use it to configure the SonicWALL WAN settings. Click **Next**.

Configuring WAN Settings



SonicWALL - Wireless Configuration Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 5: 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 1.2.3.4).
If you do not have the information, please contact your ISP .

SonicWALL WAN IP Address: 10.0.93.17

WAN Subnet Mask: 255.255.255.0

Gateway (Router) Address: 10.0.0.254

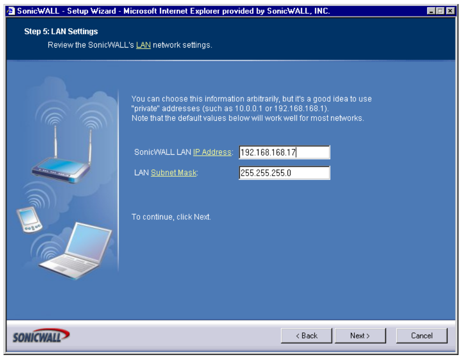
DNS Server Address: 10.50.128.52

DNS Server Address #2 (optional): 10.50.128.53

To continue, click Next.

6. If you selected **Assigned you a single, static IP address, or assigned you two more IP addresses**, you must have your IP address information from your ISP to fill in the above fields.

Configuring LAN Settings



SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 5: LAN Settings

Review the SonicWALL's LAN network settings.

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).
Note that the default values below will work well for most networks.

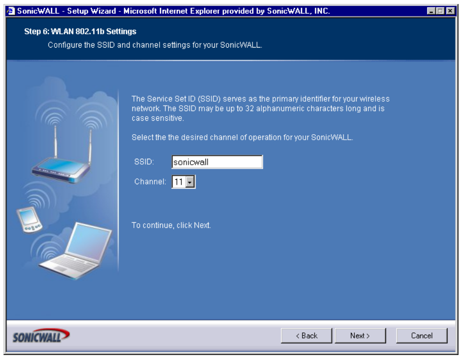
SonicWALL LAN IP Address: 192.168.168.17

LAN Subnet Mask: 255.255.255.0

To continue, click Next.

7. Type a private IP address in the **SonicWALL LAN IP Address** field. The default private IP address is acceptable for most configurations. Type the subnet in the **Subnet Mask** field. Click **Next**.

Configuring WLAN 802.11b Settings



SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 6: WLAN 802.11b Settings

Configure the SSID and channel settings for your SonicWALL.

The Service Set ID (SSID) serves as the primary identifier for your wireless
network. The SSID may be up to 32 alphanumeric characters long and is
case sensitive.

Select the the desired channel of operation for your SonicWALL.

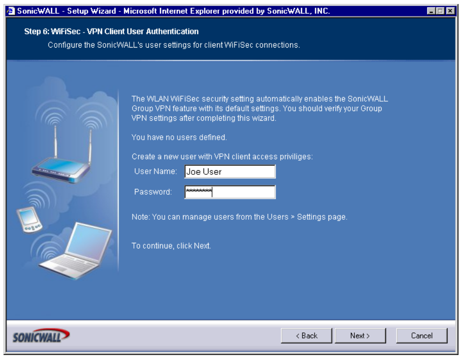
SSID: sonicwall

Channel: 11

To continue, click Next.

8. The Service Set ID (**SSID**) identifies your wireless network. It can be up to 32 alphanumeric characters long and is case-sensitive. Select the desired channel for your wireless port. Channel 11 is selected by default and is the most commonly used channel. Click **Next**.

Configuring WiFiSec - VPN Client User Authentication



SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 6: WiFiSec - VPN Client User Authentication

Configure the SonicWALL's user settings for client WiFiSec connections.

The WLAN WiFiSec security setting automatically enables the SonicWALL Group VPN feature with its default settings. You should verify your Group VPN settings after completing this wizard.

You have no users defined.

Create a new user with VPN client access priviliges:

User Name: Joe User

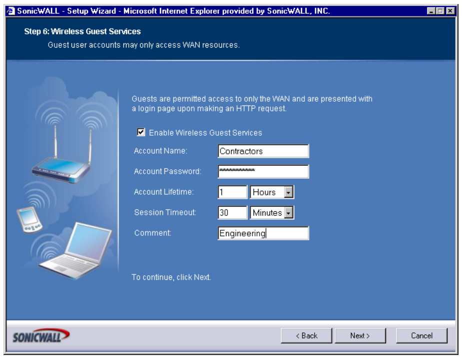
Password: ********

Note: You can manage users from the Users > Settings page.

To continue, click Next.

9. WiFiSec and Group VPN are automatically enabled on the SonicWALL using the default settings associated with each feature. To add a user with VPN Client privileges, type a user name and password in the **User Name** and **Password** fields. When users access the SonicWALL using the VPN client, they are prompted for a user name and password. Click **Next**.

Configuring Wireless Guest Services



SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 6: Wireless Guest Services

Guest user accounts may only access WAN resources.

Guests are permitted access to only the WAN and are presented with a login page upon making an HTTP request.

☑ Enable Wireless Guest Services

Account Name: Contractors

Account Password: ************

Account Lifetime: 1 Hours

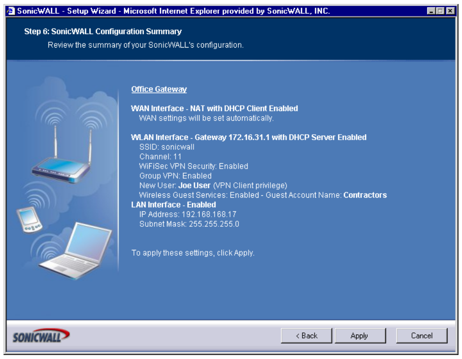
Session Timeout: 30 Minutes

Comment: Engineering

To continue, click Next.

10. When Wireless Guest Services is selected, guests on your WLAN are permitted access only to the WAN and are required to log in when accessing the Internet. Up to 10 users by default can use the same guest account. Type in the account name and password in the **Account Name** and **Password** fields. Configure the **Account Lifetime** and the **Session Timeout** times.

SonicWALL Configuration Summary



SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 6: SonicWALL Configuration Summary

Review the summary of your SonicWALL's configuration.

Office Gateway

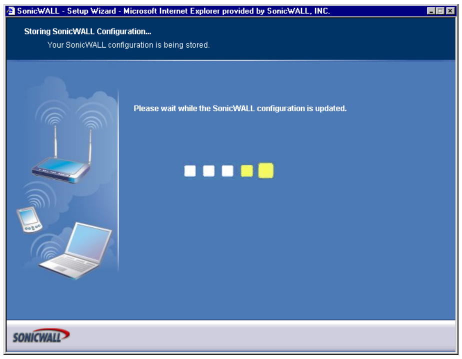
WAN Interface - NAT with DHCP Client Enabled
WAN settings will be set automatically.

WLAN Interface - Gateway 172.16.31.1 with DHCP Server Enabled
SSID: sonicwall
Channel: 11
WiFiSec VPN Security: Enabled
Group VPN: Enabled
New User: **Joe User** (VPN Client privilege)
Wireless Guest Services: Enabled - Guest Account Name: **Contractors**
LAN Interface - Enabled
IP Address: 192.168.168.17
Subnet Mask: 255.255.255.0

To apply these settings, click Apply.

11. The **Configuration Summary** page displays all of the settings configured using the **Deployment Scenario Wizard**. To change any of the settings, click **Back** until you see the settings you want to change. To use this configuration on the SonicWALL, click **Apply**.

Storing SonicWALL Configuration


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

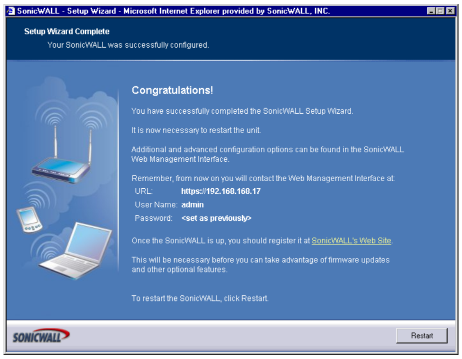
Storing SonicWALL Configuration...

Your SonicWALL configuration is being stored.

Please wait while the SonicWALL configuration is updated.

12. Wait for the settings to take effect on the SonicWALL.

Congratulations!


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
Restart

Setup Wizard Complete

Your SonicWALL was successfully configured.

Congratulations!

You have successfully completed the SonicWALL Setup Wizard.

It is now necessary to restart the unit.

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

Remember, from now on you will contact the Web Management Interface at:

URL: **https://192.168.168.17**
User Name: **admin**
Password: **<set as previously>**

Once the SonicWALL is up, you should register it at SonicWALL's Web Site.

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

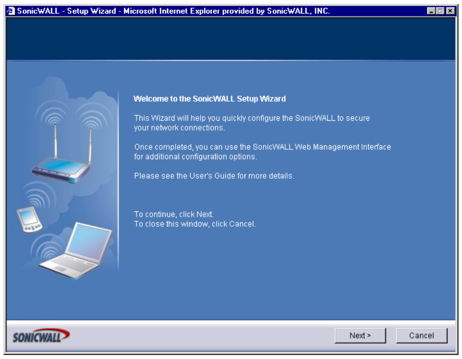
To restart the SonicWALL, click Restart.

13. When the settings are applied to the SonicWALL, the **Congratulations** page is displayed. Click **Restart** to complete the configuration.

Configuring the TZ 170 Wireless as a Secure Access Point

Log into the TZ 170 Wireless using your administrator’s name and password. Click **Wizards**.

Welcome to the SonicWALL Setup Wizard



SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Welcome to the SonicWALL Setup Wizard

This Wizard will help you quickly configure the SonicWALL to secure your network connections.

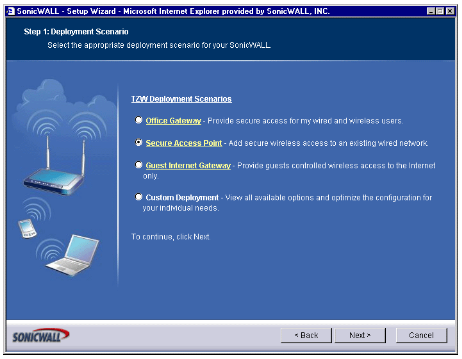
Once completed, you can use the SonicWALL Web Management Interface for additional configuration options.

Please see the User's Guide for more details.

To continue, click Next.
To close this window, click Cancel.

1. To begin configuration, click **Next**. Click **Cancel** to close the wizard.

Selecting the Deployment Scenario



SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 1: Deployment Scenario

Select the appropriate deployment scenario for your SonicWALL.

TZW Deployment Scenarios

○ Office Gateway - Provide secure access for my wired and wireless users.

● Secure Access Point - Add secure wireless access to an existing wired network.

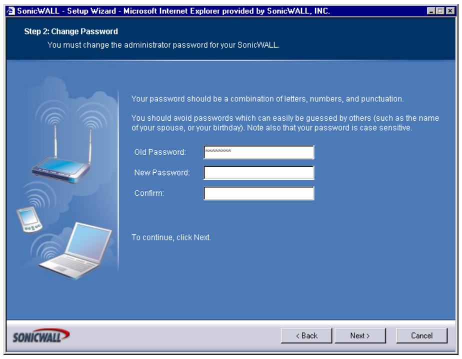
○ Guest Internet Gateway - Provide guests controlled wireless access to the Internet only.

○ **Custom Deployment** - View all available options and optimize the configuration for your individual needs.

To continue, click Next.

2. Select **Secure Access Point** as the deployment scenario. Click **Next**.

Changing the Password



SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 2: Change Password

You must change the administrator password for your SonicWALL.

Your password should be a combination of letters, numbers, and punctuation.

You should avoid passwords which can easily be guessed by others (such as the name of your spouse, or your birthday). Note also that your password is case sensitive.

Old Password: *********

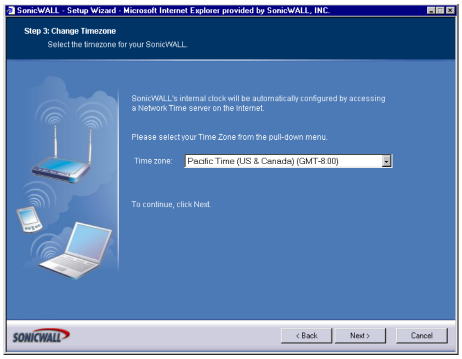
New Password:

Confirm:

To continue, click Next.

3. Type a new password in the **New Password** field. The password should be a unique combination of letters, or number, or symbols, or a combination of all three for the most secure password. Avoid names, birthdays, or any obvious words. Retype the password in the **Confirm** field. Click **Next**.

Selecting Your Time Zone



SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 3: Change Timezone

Select the timezone for your SonicWALL.

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

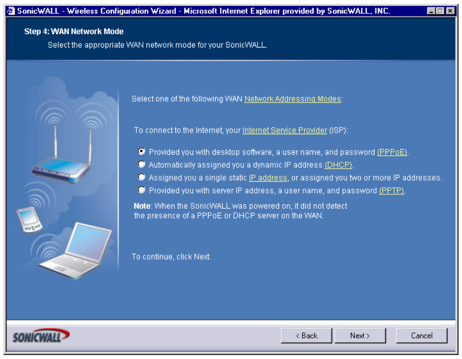
Please select your Time Zone from the pull-down menu.

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

To continue, click Next.

4. Select your Time Zone from the **Time Zone** menu. The SonicWALL uses an internal clock to timestamp logs and other functions requiring time. Click **Next**.

Configuring the WAN Network Mode



SonicWALL - Wireless Configuration Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 4: WAN Network Mode

Select the appropriate WAN network mode for your SonicWALL.

Select one of the following WAN Network Addressing Modes:

To connect to the Internet, your Internet Service Provider (ISP):

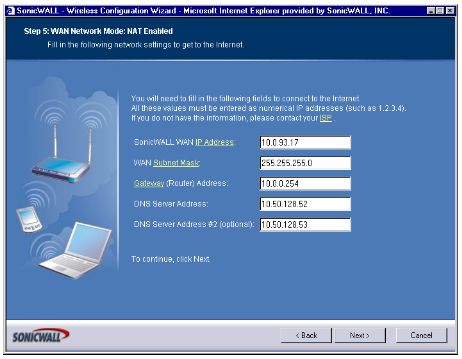
● Provided you with desktop software, a user name, and password (PPPoE).
○ Automatically assigned you a dynamic IP address (DHCP).
○ Assigned you a single static IP address, or assigned you two or more IP addresses.
○ Provided you with server IP address, a user name, and password (PPTP).

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

To continue, click Next.

5. If a DCHP server is detected on the WAN, the SonicWALL defaults to **NAT with DHCP Client** network mode. All WAN network settings are automatically detected and used for the network mode. If a PPPoE server is detected on the WAN, type the user name and password provided to you by your ISP in the **User Name** and **Password** fields. If your ISP has provided you with a single public IP address and other network information, use it to configure the SonicWALL WAN settings. Click **Next**.

Configuring WAN Settings


SonicWALL - Wireless Configuration Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 5: WAN Network Mode: NAT Enabled

Fill in the following network settings to get to the Internet.

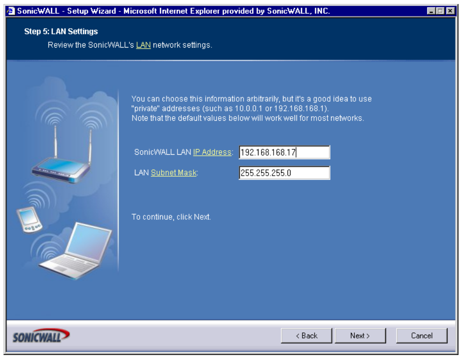
You will need to fill in the following fields to connect to the Internet.
All these values must be entered as numerical IP addresses (such as 1.2.3.4).
If you do not have the information, please contact your ISP .

SonicWALL WAN IP Address: 10.0.93.17
WAN Subnet Mask: 255.255.255.0
Gateway (Router) Address: 10.0.0.254
DNS Server Address: 10.50.128.52
DNS Server Address #2 (optional): 10.50.128.53

To continue, click Next.

If you selected **Assigned you a single, static IP address, or assigned you two more IP addresses**, you must have your IP address information from your ISP to fill in the above fields.

Configuring the LAN Settings


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 5: LAN Settings

Review the SonicWALL's LAN network settings.

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).
Note that the default values below will work well for most networks.

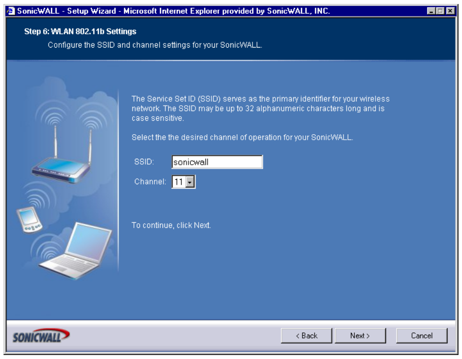
SonicWALL LAN IP Address: 192.168.168.17
LAN Subnet Mask: 255.255.255.0

To continue, click Next.

SONICWALL
< Back
Next >
Cancel

6. Type a private IP address in the **SonicWALL LAN IP Address** field. The default private IP address is acceptable for most configurations. Type the subnet in the **Subnet Mask** field. Click **Next.**

Configuring WLAN 802.11b Settings


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 6: WLAN 802.11b Settings

Configure the SSID and channel settings for your SonicWALL.

The Service Set ID (SSID) serves as the primary identifier for your wireless network. The SSID may be up to 32 alphanumeric characters long and is case sensitive.

Select the the desired channel of operation for your SonicWALL.

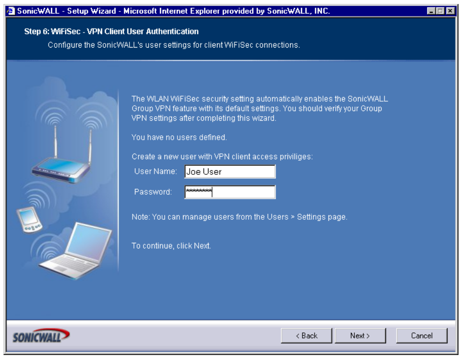
SSID: sonicwall
Channel: 11

To continue, click Next.

SONICWALL
< Back
Next >
Cancel

7. The Service Set ID (**SSID**) identifies your wireless network. It can be up to 32 alphanumeric characters long and is case-sensitive. Select the desired channel for your wireless port. Channel 11 is selected by default and is the most commonly used channel. Click **Next.**

Configuring WiFiSec - VPN Client User Authentication



SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 6: WiFiSec - VPN Client User Authentication

Configure the SonicWALL's user settings for client WiFiSec connections.

The WLAN WiFiSec security setting automatically enables the SonicWALL Group VPN feature with its default settings. You should verify your Group VPN settings after completing this wizard.

You have no users defined.

Create a new user with VPN client access priviliges:

User Name: Joe User

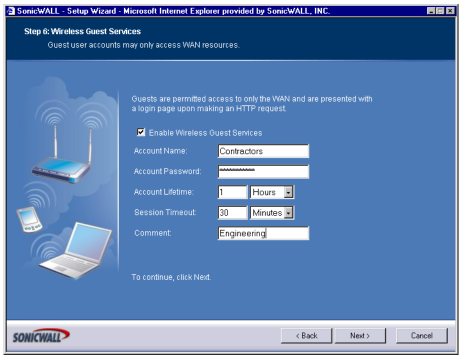
Password: ********

Note: You can manage users from the Users > Settings page.

To continue, click Next.

8. WiFiSec and Group VPN are automatically enabled on the SonicWALL using the default settings associated with each feature. To add a user with VPN Client privileges, type a user name and password in the **User Name** and **Password** fields. When users access the SonicWALL using the VPN client, they are prompted for a user name and password. Click **Next**.

Configuring Wireless Guest Services



SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 6: Wireless Guest Services

Guest user accounts may only access WAN resources.

Guests are permitted access to only the WAN and are presented with a login page upon making an HTTP request.

☑ Enable Wireless Guest Services

Account Name: Contractors

Account Password: ***********

Account Lifetime: 1 Hours

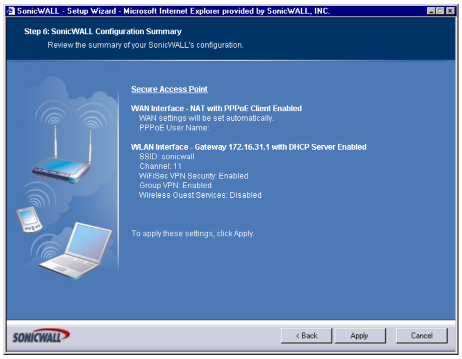
Session Timeout: 30 Minutes

Comment: Engineering

To continue, click Next.

9. When Wireless Guest Services is selected, guests on your WLAN are permitted access only to the WAN and are required to log in when accessing the Internet. Up to 10 users by default can use the same guest account. Type in the account name and password in the **Account Name** and **Password** fields. Configure the **Account Lifetime** and the **Session Timeout** times.

SonicWALL Configuration Summary



SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 6: SonicWALL Configuration Summary

Review the summary of your SonicWALL's configuration.

Secure Access Point

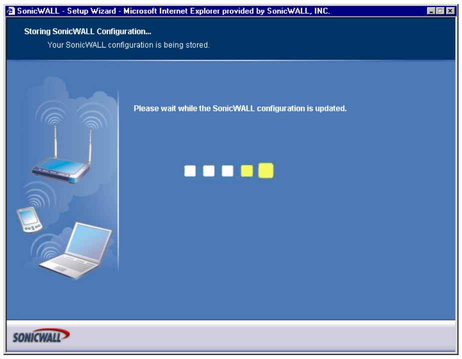
WAN Interface - NAT with PPPoE Client Enabled
WAN settings will be set automatically.
PPPoE User Name:

WLAN Interface - Gateway 172.16.31.1 with DHCP Server Enabled
SSID: sonicwall
Channel: 11
WiFiSec VPN Security: Enabled
Group VPN: Enabled
Wireless Guest Services: Disabled

To apply these settings, click Apply.

10. The **Configuration Summary** page displays all of the settings configured using the **Deployment Scenario Wizard**. To change any of the settings, click **Back** until you see the settings you want to change. To apply the current settings to the SonicWALL, click **Apply**.

Storing SonicWALL Configuration



SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

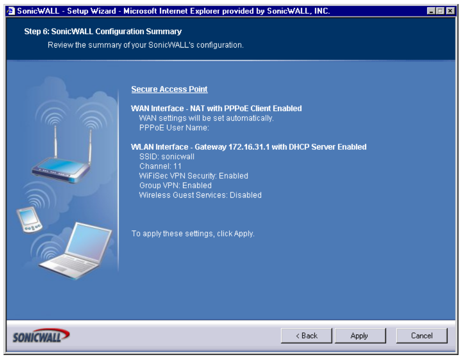
Storing SonicWALL Configuration...

Your SonicWALL configuration is being stored.

Please wait while the SonicWALL configuration is updated.

11. Wait for the settings to take effect on the SonicWALL.

Congratulations!



SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 6: SonicWALL Configuration Summary

Review the summary of your SonicWALL's configuration.

Secure Access Point

WAN Interface - NAT with PPPoE Client Enabled
WAN settings will be set automatically.
PPPoE User Name:

WLAN Interface - Gateway 172.16.31.1 with DHCP Server Enabled
SSID: sonicwall
Channel: 11
WiFiSec VPN Security: Enabled
Group VPN: Enabled
Wireless Guest Services: Disabled

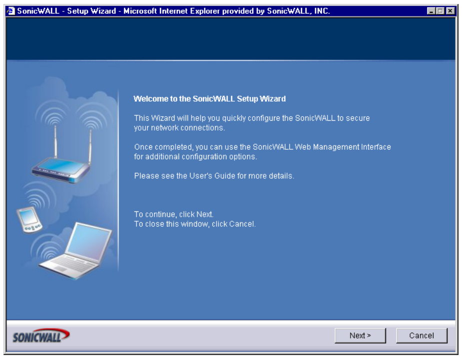
To apply these settings, click Apply.

When the settings are applied to the SonicWALL, the **Congratulations** page is displayed. Click **Restart** to complete the configuration.

Configuring the TZ 170 Wireless as a Guest Internet Gateway

Log into the TZ 170 Wireless using your administrator's name and password. Click **Wizards**.

Welcome to the SonicWALL Setup Wizard


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Welcome to the SonicWALL Setup Wizard

This Wizard will help you quickly configure the SonicWALL to secure your network connections.

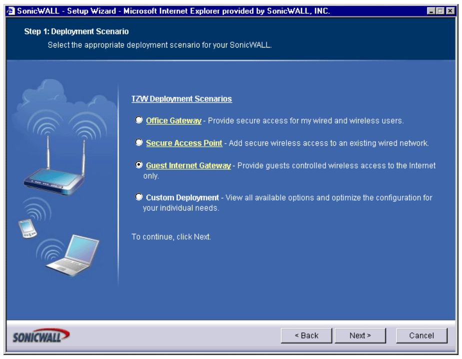
Once completed, you can use the SonicWALL Web Management Interface for additional configuration options.

Please see the User's Guide for more details.

To continue, click Next.
To close this window, click Cancel.

1. To begin configuration, click **Next**. Click **Cancel** to close the wizard.

Selecting the Deployment Scenario


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 1: Deployment Scenario

Select the appropriate deployment scenario for your SonicWALL.

TZW Deployment Scenarios

○ Office Gateway - Provide secure access for my wired and wireless users.

○ Secure Access Point - Add secure wireless access to an existing wired network.

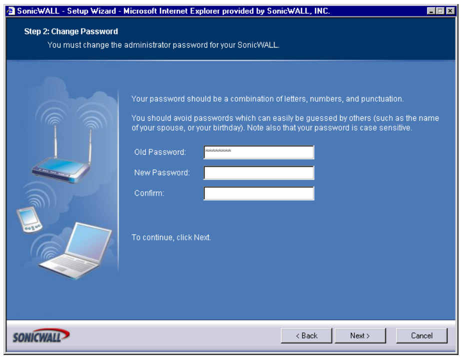
● Guest Internet Gateway - Provide guests controlled wireless access to the Internet only.

○ **Custom Deployment** - View all available options and optimize the configuration for your individual needs.

To continue, click Next.

2. Select **Guest Internet Gateway** as the deployment scenario. Click **Next**.

Changing the Password


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 2: Change Password

You must change the administrator password for your SonicWALL.

Your password should be a combination of letters, numbers, and punctuation.

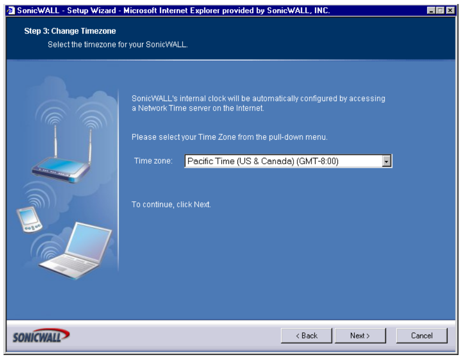
You should avoid passwords which can easily be guessed by others (such as the name of your spouse, or your birthday). Note also that your password is case sensitive.

Old Password: *********
New Password:
Confirm:

To continue, click Next.

3. Type a new password in the **New Password** field. The password should be a unique combination of letters, or number, or symbols, or a combination of all three for the most secure password. Avoid names, birthdays, or any obvious words. Retype the password in the **Confirm** field. Click **Next**.

Selecting Your Time Zone


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 3: Change Timezone

Select the timezone for your SonicWALL.

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

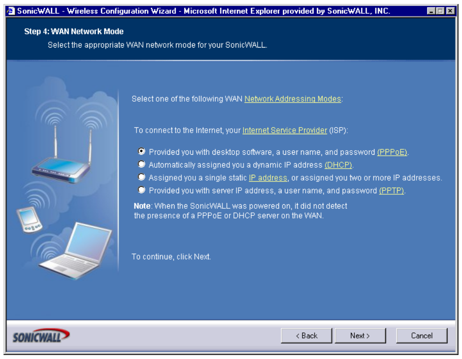
Please select your Time Zone from the pull-down menu.

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

To continue, click Next.

4. Select your Time Zone from the **Time Zone** menu. The SonicWALL uses an internal clock to timestamp logs and other functions requiring time. Click **Next**.

Configuring the WAN Network Mode


SonicWALL - Wireless Configuration Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 4: WAN Network Mode

Select the appropriate WAN network mode for your SonicWALL.

Select one of the following WAN Network Addressing Modes:

To connect to the Internet, your Internet Service Provider (ISP):

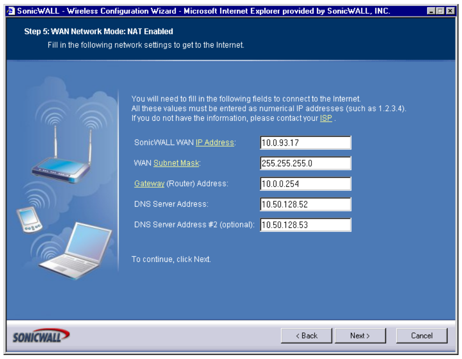
● Provided you with desktop software, a user name, and password (PPPoE).
○ Automatically assigned you a dynamic IP address (DHCP).
○ Assigned you a single static IP address, or assigned you two or more IP addresses.
○ Provided you with server IP address, a user name, and password (PPTP).

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

To continue, click Next.

5. If a DCHP server is detected on the WAN, the SonicWALL defaults to **NAT with DHCP Client** network mode. All WAN network settings are automatically detected and used for the network mode. If a PPPoE server is detected on the WAN, type the user name and password provided to you by your ISP in the **User Name** and **Password** fields. If your ISP has provided you with a single public IP address and other network information, use it to configure the SonicWALL WAN settings. Click **Next**.

Configuring WAN Settings


SonicWALL - Wireless Configuration Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 5: 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 1.2.3.4).
If you do not have the information, please contact your ISP .

SonicWALL WAN IP Address: 10.0.93.17

WAN Subnet Mask: 255.255.255.0

Gateway (Router) Address: 10.0.0.254

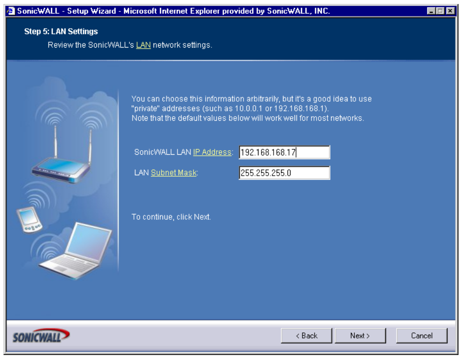
DNS Server Address: 10.50.128.52

DNS Server Address #2 (optional): 10.50.128.53

To continue, click Next.

6. If you selected **Assigned you a single, static IP address, or assigned you two more IP addresses**, you must have your IP address information from your ISP to fill in the above fields.

Configuring the LAN Settings



SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 5: LAN Settings

Review the SonicWALL's LAN network settings.

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).
Note that the default values below will work well for most networks.

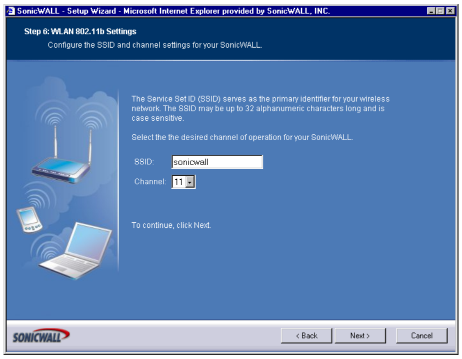
SonicWALL LAN IP Address: 192.168.168.17

LAN Subnet Mask: 255.255.255.0

To continue, click Next.

7. Type a private IP address in the **SonicWALL LAN IP Address** field. The default private IP address is acceptable for most configurations. Type the subnet in the **Subnet Mask** field. Click **Next**.

Configuring WLAN 802.11b Settings



SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 6: WLAN 802.11b Settings

Configure the SSID and channel settings for your SonicWALL.

The Service Set ID (SSID) serves as the primary identifier for your wireless network. The SSID may be up to 32 alphanumeric characters long and is case sensitive.

Select the the desired channel of operation for your SonicWALL.

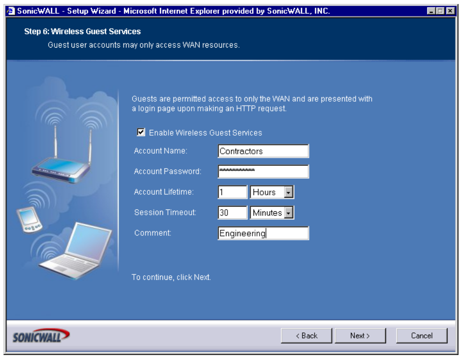
SSID: sonicwall

Channel: 11

To continue, click Next.

8. The Service Set ID (**SSID**) identifies your wireless network. It can be up to 32 alphanumeric characters long and is case-sensitive. Select the desired channel for your wireless port. Channel 11 is selected by default and is the most commonly used channel. Click **Next**.

Configuring Wireless Guest Services



SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 6: Wireless Guest Services

Guest user accounts may only access WAN resources.

Guests are permitted access to only the WAN and are presented with a login page upon making an HTTP request.

☑ Enable Wireless Guest Services

Account Name: Contractors

Account Password: ************

Account Lifetime: 1 Hours

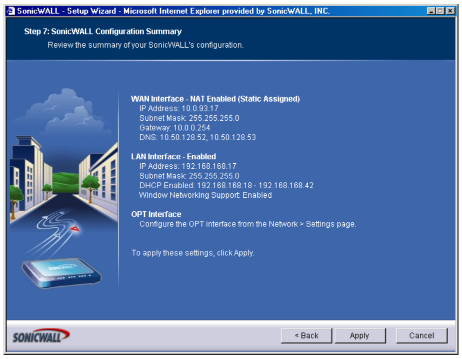
Session Timeout: 30 Minutes

Comment: Engineering

To continue, click Next.

9. When Wireless Guest Services is selected, guests on your WLAN are permitted access only to the WAN and are required to log in when accessing the Internet. Up to 10 users by default can use the same guest account. Type in the account name and password in the **Account Name** and **Password** fields. Configure the **Account Lifetime** and the **Session Timeout** times.

SonicWALL Configuration Summary



SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 7: SonicWALL Configuration Summary

Review the summary of your SonicWALL's configuration.

WAN Interface - NAT Enabled (Static Assigned)
IP Address: 10.0.93.17
Subnet Mask: 255.255.255.0
Gateway: 10.0.0.254
DNS: 10.50.128.52, 10.50.128.53

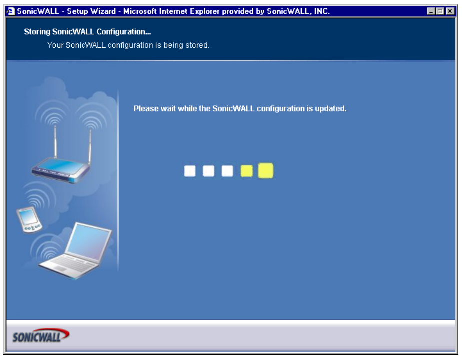
LAN Interface - Enabled
IP Address: 192.168.168.17
Subnet Mask: 255.255.255.0
DHCP Enabled: 192.168.168.18 - 192.168.168.42
Window Networking Support: Enabled

OPT Interface
Configure the OPT interface from the Network > Settings page.

To apply these settings, click Apply.

10. The **Configuration Summary** page displays all of the settings configured using the **Deployment Scenario Wizard**. To change any of the settings, click **Back** until you see the settings you want to change. To apply the current settings to the SonicWALL, click **Apply**.

Storing SonicWALL Configuration



SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

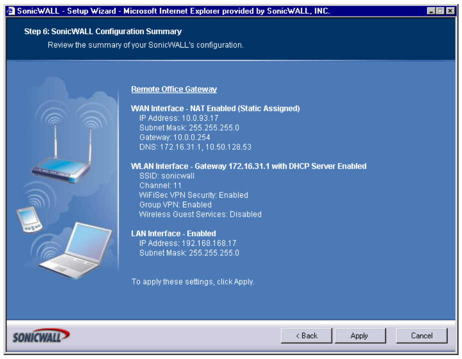
Storing SonicWALL Configuration...

Your SonicWALL configuration is being stored.

Please wait while the SonicWALL configuration is updated.

11. Wait for the settings to take effect on the SonicWALL.

Congratulations!



SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 6: SonicWALL Configuration Summary

Review the summary of your SonicWALL's configuration.

Remote Office Gateway

WAN Interface - NAT Enabled (Static Assigned)
IP Address: 10.0.93.17
Subnet Mask: 255.255.255.0
Gateway: 10.0.0.254
DNS: 172.16.31.1, 10.50.128.53

WLAN Interface - Gateway 172.16.31.1 with DHCP Server Enabled
SSID: sonicwall
Channel: 11
WiFiSec VPN Security: Enabled
Group VPN: Enabled
Wireless Guest Services: Disabled

LAN Interface - Enabled
IP Address: 192.168.168.17
Subnet Mask: 255.255.255.0

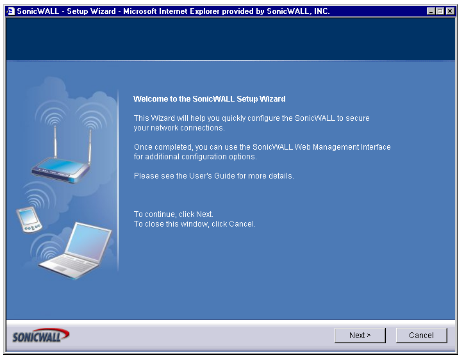
To apply these settings, click Apply.

When the settings are applied to the SonicWALL, the **Congratulations** page is displayed. Click **Restart** to complete the configuration.

Configuring the TZ 170 Wireless using a Custom Deployment

Log into the TZ 170 Wireless using your administrator's name and password. Click **Wizards**.

Welcome to the SonicWALL Setup Wizard



SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
Next >
Cancel

Welcome to the SonicWALL Setup Wizard

This Wizard will help you quickly configure the SonicWALL to secure your network connections.

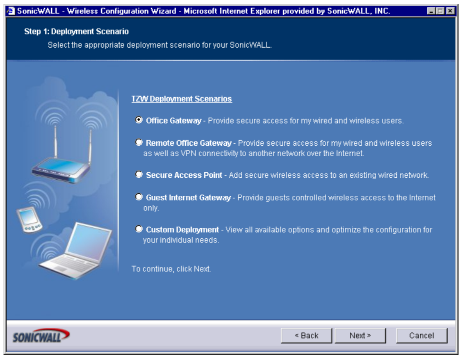
Once completed, you can use the SonicWALL Web Management Interface for additional configuration options.

Please see the User's Guide for more details.

To continue, click Next.
To close this window, click Cancel.

1. To begin configuration, click **Next**. Click **Cancel** to close the wizard.

Selecting the Deployment Scenario



SonicWALL - Wireless Configuration Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
< Back
Next >
Cancel

Step 1: Deployment Scenario
Select the appropriate deployment scenario for your SonicWALL.

TZW Deployment Scenarios

● **Office Gateway** - Provide secure access for my wired and wireless users.

○ **Remote Office Gateway** - Provide secure access for my wired and wireless users as well as VPN connectivity to another network over the Internet.

○ **Secure Access Point** - Add secure wireless access to an existing wired network.

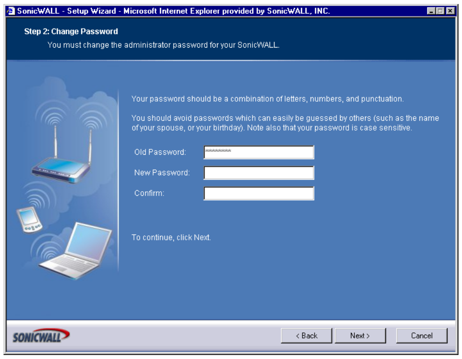
○ **Guest Internet Gateway** - Provide guests controlled wireless access to the Internet only.

○ **Custom Deployment** - View all available options and optimize the configuration for your individual needs.

To continue, click Next.

2. Select **Custom Deployment** as the deployment scenario. Click **Next**.

Changing the Password



SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.
SONICWALL
< Back
Next >
Cancel

Step 2: Change Password
You must change the administrator password for your SonicWALL.

Your password should be a combination of letters, numbers, and punctuation.

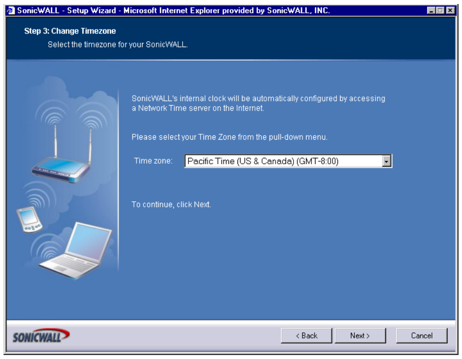
You should avoid passwords which can easily be guessed by others (such as the name of your spouse, or your birthday). Note also that your password is case sensitive.

Old Password: *********
New Password:
Confirm:

To continue, click Next.

3. Type a new password in the **New Password** field. The password should be a unique combination of letters, or number, or symbols, or a combination of all three for the most secure password. Avoid names, birthdays, or any obvious words. Retype the password in the **Confirm** field. Click **Next**.

Selecting Your Time Zone


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 3: Change Timezone

Select the timezone 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.

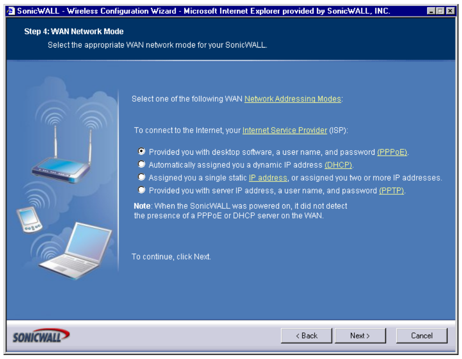
Time zone: Pacific Time (US & Canada) (GMT-8:00)

To continue, click Next.

SONICWALL
< Back
Next >
Cancel

4. Select your Time Zone from the **Time Zone** menu. The SonicWALL uses an internal clock to timestamp logs and other functions requiring time. Click **Next**.

Configuring the WAN Network Mode


SonicWALL - Wireless Configuration Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 4: WAN Network Mode

Select the appropriate WAN network mode for your SonicWALL.

Select one of the following WAN Network Addressing Modes:

To connect to the Internet, your Internet Service Provider (ISP):

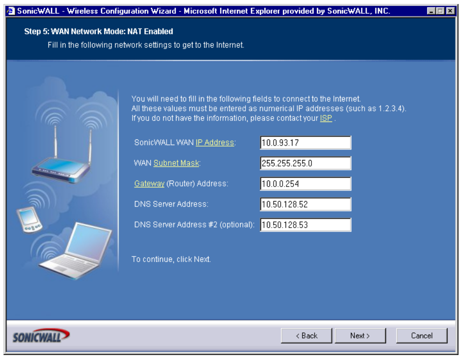
- ● Provided you with desktop software, a user name, and password (PPPoE).
- ○ Automatically assigned you a dynamic IP address (DHCP).
- ○ Assigned you a single static IP address, or assigned you two or more IP addresses.
- ○ Provided you with server IP address, a user name, and password (PPTP).

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

To continue, click Next.

5. If a DCHP server is detected on the WAN, the SonicWALL defaults to **NAT with DHCP Client** network mode. All WAN network settings are automatically detected and used for the network mode. If a PPPoE server is detected on the WAN, type the user name and password provided to you by your ISP in the **User Name** and **Password** fields. If your ISP has provided you with a single public IP address and other network information, use it to configure the SonicWALL WAN settings. Click **Next**.

Configuring WAN Settings


SonicWALL - Wireless Configuration Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 5: WAN Network Mode: NAT Enabled

Fill in the following network settings to get to the Internet.

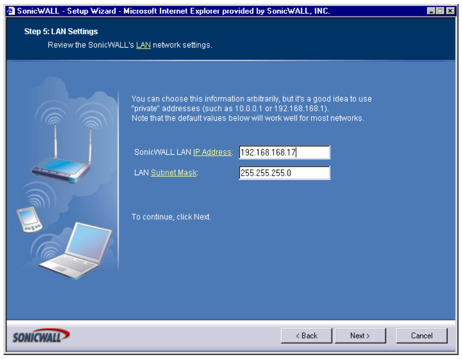
You will need to fill in the following fields to connect to the Internet.
All these values must be entered as numerical IP addresses (such as 1.2.3.4).
If you do not have the information, please contact your ISP .

SonicWALL WAN IP Address:	10.0.93.17
WAN Subnet Mask:	255.255.255.0
Gateway (Router) Address:	10.0.0.254
DNS Server Address:	10.50.128.52
DNS Server Address #2 (optional):	10.50.128.53

To continue, click Next.

6. If you selected **Assigned you a single, static IP address, or assigned you two more IP addresses**, you must have your IP address information from your ISP to fill in the above fields.

Configuring LAN Settings



SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 5: LAN Settings

Review the SonicWALL's LAN network settings.

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).
Note that the default values below will work well for most networks.

SonicWALL LAN IP Address: 192.168.168.17

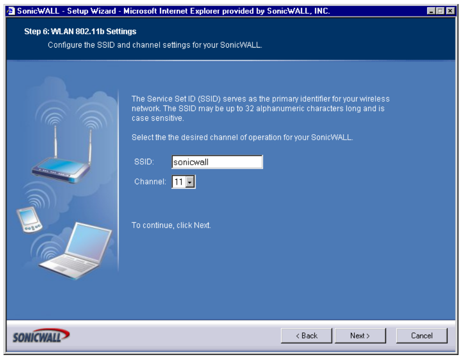
LAN Subnet Mask: 255.255.255.0

To continue, click Next.

SONICWALL
< Back
Next >
Cancel

7. Type a private IP address in the **SonicWALL LAN IP Address** field. The default private IP address is acceptable for most configurations. Type the subnet in the **Subnet Mask** field. Click **Next**.

Configuring WLAN 802.11b Settings



SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 6: WLAN 802.11b Settings

Configure the SSID and channel settings for your SonicWALL.

The Service Set ID (SSID) serves as the primary identifier for your wireless network. The SSID may be up to 32 alphanumeric characters long and is case sensitive.

Select the the desired channel of operation for your SonicWALL.

SSID: sonicwall

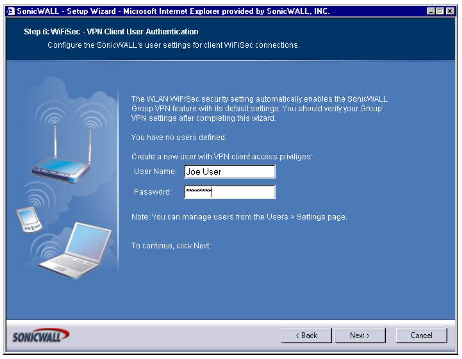
Channel: 11

To continue, click Next.

SONICWALL
< Back
Next >
Cancel

8. The Service Set ID (**SSID**) identifies your wireless network. It can be up to 32 alphanumeric characters long and is case-sensitive. Select the desired channel for your wireless port. Channel 11 is selected by default and is the most commonly used channel. Click **Next**.

Configuring WiFiSec - VPN Client User Authentication



SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 6: WiFiSec - VPN Client User Authentication

Configure the SonicWALL's user settings for client WiFiSec connections.

The WLAN WiFiSec security setting automatically enables the SonicWALL Group VPN feature with its default settings. You should verify your Group VPN settings after completing this wizard.

You have no users defined.

Create a new user with VPN client access priviliges:

User Name: Joe User

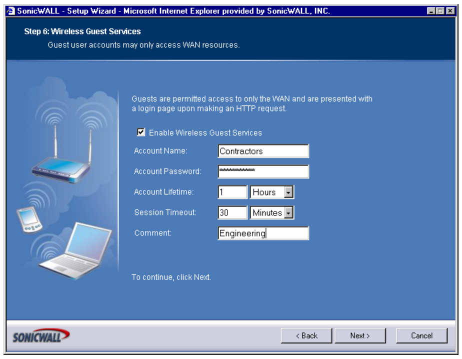
Password: ********

Note: You can manage users from the Users > Settings page.

To continue, click Next.

9. WiFiSec and Group VPN are automatically enabled on the SonicWALL using the default settings associated with each feature. To add a user with VPN Client privileges, type a user name and password in the **User Name** and **Password** fields. When users access the SonicWALL using the VPN client, they are prompted for a user name and password. Click **Next**.

Configuring Wireless Guest Services


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 6: Wireless Guest Services

Guest user accounts may only access WAN resources.

Guests are permitted access to only the WAN and are presented with
a login page upon making an HTTP request.

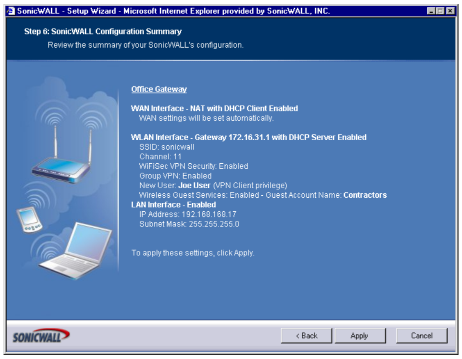
☑ Enable Wireless Guest Services

Account Name:	Contractors
Account Password:	************
Account Lifetime:	1 Hours
Session Timeout:	30 Minutes
Comment:	Engineering

To continue, click Next.

10. When Wireless Guest Services is selected, guests on your WLAN are permitted access only to the WAN and are required to log in when accessing the Internet. Up to 10 users by default can use the same guest account. Type in the account name and password in the **Account Name** and **Password** fields. Configure the **Account Lifetime** and the **Session Timeout** times.

SonicWALL Configuration Summary


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 6: SonicWALL Configuration Summary

Review the summary of your SonicWALL's configuration.

Office Gateway

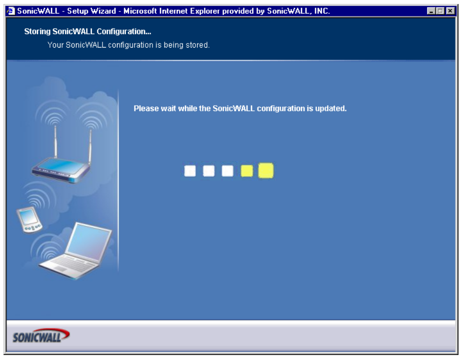
WAN Interface - NAT with DHCP Client Enabled
WAN settings will be set automatically.

WLAN Interface - Gateway 172.16.31.1 with DHCP Server Enabled
SSID: sonicwall
Channel: 11
WiFiSec VPN Security: Enabled
Group VPN: Enabled
New User: **Joe User** (VPN Client privilege)
Wireless Guest Services: Enabled - Guest Account Name: **Contractors**
LAN Interface - Enabled
IP Address: 192.168.168.17
Subnet Mask: 255.255.255.0

To apply these settings, click Apply.

11. The **Configuration Summary** page displays all of the settings configured using the **Deployment Scenario Wizard**. To change any of the settings, click **Back** until you see the settings you want to change. To apply the current settings to the SonicWALL, click **Apply**.

Storing SonicWALL Configuration


SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

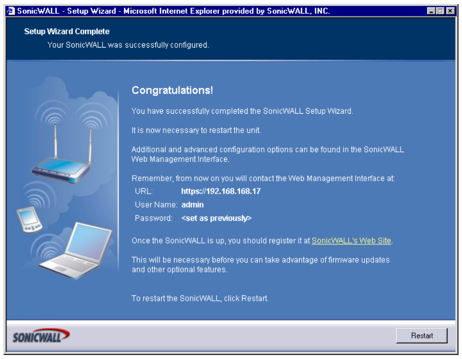
Storing SonicWALL Configuration...

Your SonicWALL configuration is being stored.

Please wait while the SonicWALL configuration is updated.

12. Wait for the settings to take effect on the SonicWALL.

Congratulations!



SonicWALL - Setup Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Setup Wizard Complete

Your SonicWALL was successfully configured.

Congratulations!

You have successfully completed the SonicWALL Setup Wizard.

It is now necessary to restart the unit.

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

Remember, from now on you will contact the Web Management Interface at:

URL:	**https://192.168.168.17**
User Name:	**admin**
Password:	**<set as previously>**

Once the SonicWALL is up, you should register it at SonicWALL's Web Site.

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

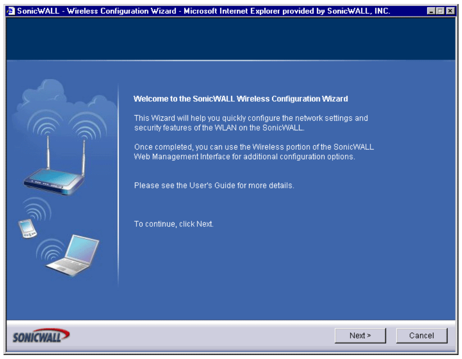
To restart the SonicWALL, click Restart.

When the settings are applied to the SonicWALL, the **Congratulations** page is displayed. Click **Restart** to complete the configuration.

Using the Wireless Wizard

You can use the Wireless Wizard to quickly and easily set up your wireless network. Log into the TZ 170 Wireless, and click **Wireless** on the menu bar. Click **Wireless Wizard** to launch the wizard and begin the configuration process. Or click **Wizards**, and select **Wireless Wizard.**

Welcome to the SonicWALL Wireless Configuration Wizard



SonicWALL - Wireless Configuration Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Welcome to the SonicWALL Wireless Configuration Wizard

This Wizard will help you quickly configure the network settings and security features of the WLAN on the SonicWALL.

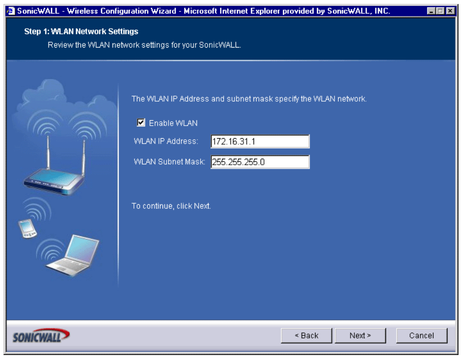
Once completed, you can use the Wireless portion of the SonicWALL Web Management Interface for additional configuration options.

Please see the User's Guide for more details.

To continue, click Next.

1. When the Wireless Wizard launches, the **Welcome** page is displayed. Click **Next** to continue configuration.

WLAN Network



SonicWALL - Wireless Configuration Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 1: WLAN Network Settings

Review the WLAN network settings for your SonicWALL.

The WLAN IP Address and subnet mask specify the WLAN network.

☑ Enable WLAN

WLAN IP Address: 172.16.31.1

WLAN Subnet Mask: 255.255.255.0

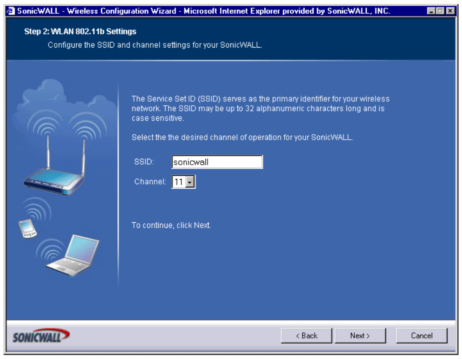
To continue, click Next.

2. Select the **Enable WLAN** check box to activate the wireless feature of the TZ 170 Wireless. Use the default IP address for the WLAN or choose a different private IP address. The default value works for most networks. Click **Next** to continue.

⚠

Alert! *You cannot use the same private IP address range as the LAN port of the TZ 170 Wireless.*

WLAN 802.11b Settings



SonicWALL - Wireless Configuration Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 2: WLAN 802.11b Settings

Configure the SSID and channel settings for your SonicWALL.

The Service Set ID (SSID) serves as the primary identifier for your wireless network. The SSID may be up to 32 alphanumeric characters long and is case sensitive.

Select the the desired channel of operation for your SonicWALL.

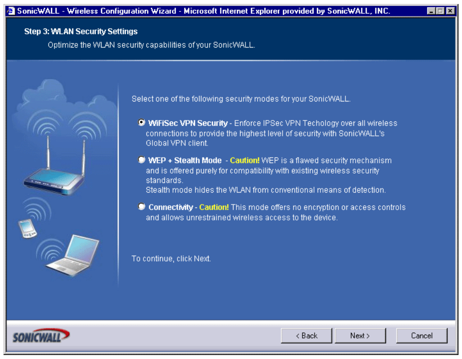
SSID: sonicwall

Channel: 11

To continue, click Next.

3. Type a unique identifier for the TZ 170 Wireless in the SSID field. It can be up to 32 alphanumeric characters in length and is case-sensitive. The default value is **sonicwall**.

WLAN Security Settings



SonicWALL - Wireless Configuration Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 3: WLAN Security Settings

Optimize the WLAN security capabilities of your SonicWALL.

Select one of the following security modes for your SonicWALL.

● **WiFiSec VPN Security** - Enforce IPSec VPN Techology over all wireless connections to provide the highest level of security with SonicWALL's Global VPN client.

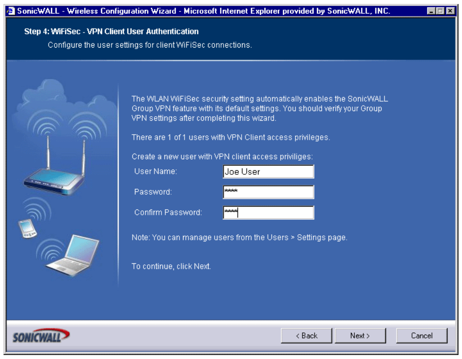
○ **WEP + Stealth Mode** - Caution! WEP is a flawed security mechanism and is offered purely for compatibility with existing wireless security standards.
Stealth mode hides the WLAN from conventional means of detection.

○ **Connectivity** - Caution! This mode offers no encryption or access controls and allows unrestrained wireless access to the device.

To continue, click Next.

4. Choose the desired security setting for the TZ 170 Wireless. **WiFiSec** is the most secure and enforces IPSec over the wireless network. If you have an existing wireless network and want to use the TZ 170 Wireless, select **WEP + Stealth Mode**.

WiFiSec - VPN Client User Authentication



SonicWALL - Wireless Configuration Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 4: WiFiSec - VPN Client User Authentication

Configure the user settings for client WiFiSec connections.

The WLAN WiFiSec security setting automatically enables the SonicWALL Group VPN feature with its default settings. You should verify your Group VPN settings after completing this wizard.

There are 1 of 1 users with VPN Client access privileges.

Create a new user with VPN client access priviliges:

User Name: Joe User

Password: ****

Confirm Password: ****

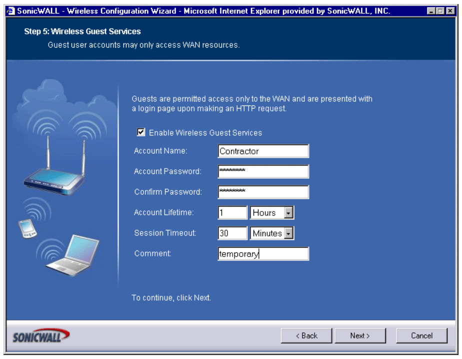
Note: You can manage users from the Users > Settings page.

To continue, click Next.

5. Create a new user with VPN Client privileges by typing a user name and password in the **User Name** and **Password** fields.

Alert! *Selecting WiFiSec automatically enables the SonicWALL Group VPN feature and its default settings. Verify your Group VPN settings after configuring your wireless connection.*

Wireless Guest Services



SonicWALL - Wireless Configuration Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 5: Wireless Guest Services

Guest user accounts may only access WAN resources.

Guests are permitted access only to the WAN and are presented with a login page upon making an HTTP request.

☑ Enable Wireless Guest Services

Account Name: Contractor

Account Password: ********

Confirm Password: ********

Account Lifetime: 1 Hours

Session Timeout: 30 Minutes

Comment: temporary

To continue, click Next.

6. The **Enable Wireless Guest Services** check box is selected by default. You can create guest wireless accounts to grant access to the WAN only.

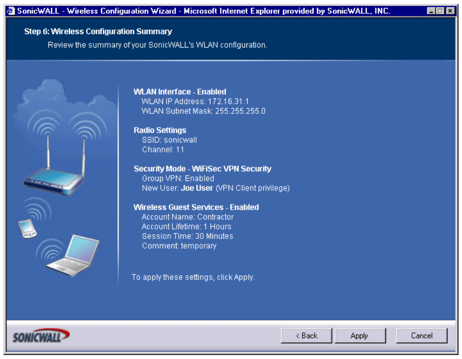
   If you enable Wireless Guest Services, type a name for the account in the **Account Name** field, and a password in the **Account Password** field.

   The **Account Lifetime** is set to one hour by default, but you can configure **Minutes**, **Hours**, or **Days** to determine how long the guest account is active.

   Type the value in the **Session Timeout** field. Select **Minutes**, **Hours**, or **Days**.

   Any comments about the connection can be typed in the **Comment** field.

Wireless Configuration Summary



SonicWALL - Wireless Configuration Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 6: Wireless Configuration Summary

Review the summary of your SonicWALL's WLAN configuration.

WLAN Interface - Enabled
WLAN IP Address: 172.16.31.1
WLAN Subnet Mask: 255.255.255.0

Radio Settings
SSID: sonicwall
Channel: 11

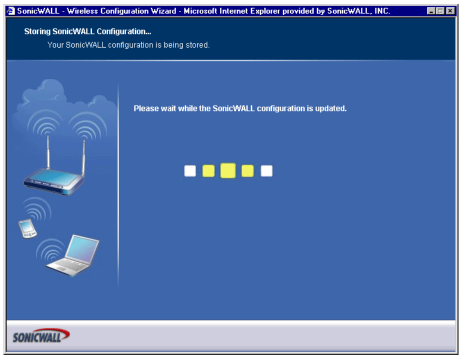
Security Mode - WiFiSec VPN Security
Group VPN: Enabled
New User: **Joe User** (VPN Client privilege)

Wireless Guest Services - Enabled
Account Name: Contractor
Account Lifetime: 1 Hours
Session Time: 30 Minutes
Comment: temporary

To apply these settings, click Apply.

7. Review your wireless settings for accuracy. If you want to make changes, click **Back** until the settings are displayed. Then click **Next** until you reach the **Summary** page.

Updating the TZ 170 Wireless!



SonicWALL - Wireless Configuration Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

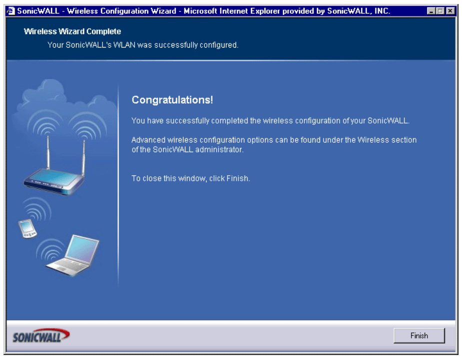
Storing SonicWALL Configuration...

Your SonicWALL configuration is being stored.

Please wait while the SonicWALL configuration is updated.

8. The TZ 170 Wireless is now updating the wireless configuration with your settings.

Congratulations!



SonicWALL - Wireless Configuration Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Wireless Wizard Complete

Your SonicWALL's WLAN was successfully configured.

Congratulations!

You have successfully completed the wireless configuration of your SonicWALL.

Advanced wireless configuration options can be found under the Wireless section of the SonicWALL administrator.

To close this window, click Finish.

9. Congratulations! You have successfully completed configuration of your wireless settings. Click **Finish** to exit the Wizard.

Configuring Additional Wireless Features

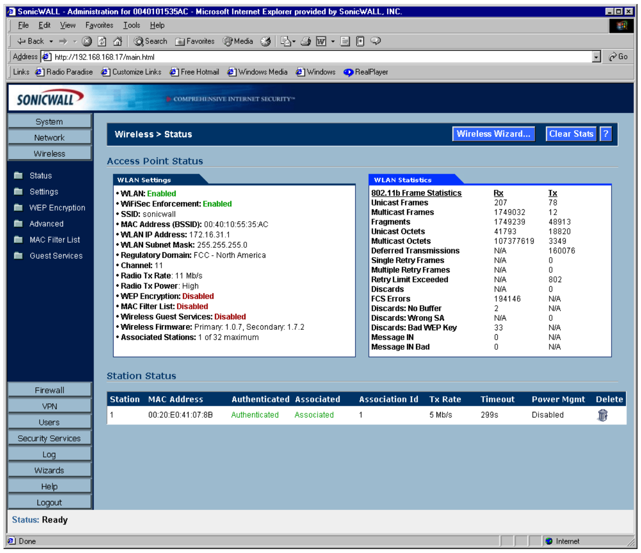
The SonicWALL TZ 170 Wireless has the following features available:

- **WiFiSec Enforcement** - an IPSec-based VPN overlay for wireless networking
- **WEP Encryption** - configure Wired Equivalent Privacy (WEP) Encryption
- **Beaconing and SSID Controls** - manage transmission of the wireless signal.
- **Wireless Client Communications** - configure wireless client settings.
- **Advanced Radio Settings** - fine-tune wireless broadcasting on the TZ 170 Wireless
- **MAC Filtering** - use MAC addresses for allowing access or blocking access to the TZ 170 Wireless.

In addition to providing different status views for **Access Point** and **Wireless Bridge** modes, two new functions have been added to the **Wireless > Status** page:

- **Hyperlinked WLAN Settings** - All configurable WLAN settings are now hyperlinked to their respective pages for configuration. (Present in both Access Point and Wireless Bridge modes). Enabled features are displayed in green, and disabled features are displayed in red.
- **Automated Station Blocking** - Previously, the **Station Status** view allowed for stations to be added to the MAC allow list, or disassociated from the TZ 170 Wireless. The disassociated station, however, could easily re-associate unless other prohibitive actions were taken. This functionality has been

enhanced by adding the **Block** icon. Clicking this icon disassociates the station and adds the station to the MAC block list.To begin configuring advanced features on the TZ 170 Wireless, log into the management interface, and click **Wireless**. The **Status** page is displayed and contains information relating to the WLAN connection.


SonicWALL - Administration for 0040101535AC - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.17/main.html
Go
Links Radio Paradise Customize Links Free Hotmail Windows Media Windows RealPlayer
SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Wireless
Status
Settings
WEP Encryption
Advanced
MAC Filter List
Guest Services
Firewall
VPN
Users
Security Services
Log
Wizards
Help
Logout
Wireless Wizard...
Clear Stats
?
Done
Internet

Wireless > Status

Access Point Status

WLAN Settings

- **WLAN:** Enabled
- **WiFiSec Enforcement:** Enabled
- **SSID:** sonicwall
- **MAC Address (BSSID):** 00:40:10:55:35:AC
- **WLAN IP Address:** 172.16.31.1
- **WLAN Subnet Mask:** 255.255.255.0
- **Regulatory Domain:** FCC - North America
- **Channel:** 11
- **Radio Tx Rate**: 11 Mb/s
- **Radio Tx Power**: High
- **WEP Encryption:** Disabled
- **MAC Filter List:** Disabled
- **Wireless Guest Services:** Disabled
- **Wireless Firmware:** Primary: 1.0.7, Secondary: 1.7.2
- **Associated Stations:** 1 of 32 maximum

WLAN Statistics

802.11b Frame Statistics	Rx	Tx
Unicast Frames	207	78
Multicast Frames	1749032	12
Fragments	1749239	48913
Unicast Octets	41793	18820
Multicast Octets	107377619	3349
Deferred Transmissions	N/A	160076
Single Retry Frames	N/A	0
Multiple Retry Frames	N/A	0
Retry Limit Exceeded	N/A	802
Discards	N/A	0
FCS Errors	194146	N/A
Discards: No Buffer	2	N/A
Discards: Wrong SA	N/A	0
Discards: Bad WEP Key	33	N/A
Message IN	0	N/A
Message IN Bad	0	N/A

Station Status

Station	MAC Address	Authenticated	Associated	Association Id	Tx Rate	Timeout	Power Mgmt	Delete
1	00:20:E0:41:07:8B	Authenticated	Associated	1	5 Mb/s	299s	Disabled	🗑

Status: Ready

Access Point Status

WLAN Settings	Value
WLAN:	Enabled or Disabled
WiFiSec:	Enabled or Disabled
SSID:	Network Identification Information
MAC Address:	Serial Number of the TZ 170 Wireless
WLAN IP Address:	IP address of the WLAN port
WLAN Subnet Mask:	Subnet information
Regulatory Domain	**FCC - North America** for domestic appliances **ETSI - Europe** for international appliances
Channel	Channel Number selected for transmitting wireless signal
Radio Tx Rate	Network speed in Mbps
Radio Tx Power	the current power level of the radio signal transmission
Link Status:	Network speed in mbps, full or half duplex
WEP Encryption:	Enabled or Disabled
ACL:	Enabled or Disabled
Wireless Guest Services	Enabled or Disabled
Wireless Firmware:	Firmware versions on the radio card
Associated Stations:	Number of clients associated with the TZ 170 Wireless

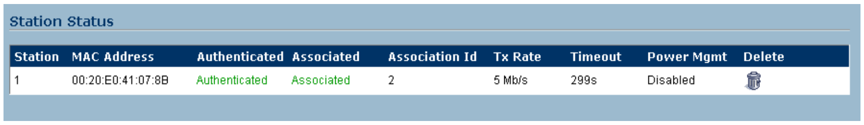
WLAN Statistics

802.11b Frame Statistics	Rx/TX
Unicast Frames	Number of frames received and transmitted
Multicast Frames	Total number of frames received and transmitted as broadcast or multicast. Typically a lower number than Unicast frames.
Fragments	Total number of fragmented frames received and sent. This is a general indication of activity at this wireless device.
Unicast Octets	Total number of bytes received and transmitted as part of unicast messages.
Multicast Octets	Total number of bytes received and transmitted as multicast messages.
Deferred Transmissions	Number of times a transmission was deferred to avoid collisions with messages from other devices. Deferral is normal and a high value is typical.
Signal Retry Frames	Number of messages retransmitted a single time being acknowledged by the receiving device. Retransmission is normal for 802.11b to quickly recover from lost messages.
Multiple Retry Frames	Number of messages retransmitted multiple times before acknowledgement by the receiving device. A relatively high value can indicate interference or a heavy wireless data load.

802.11b Frame Statistics	Rx/TX
Retry Limit Exceeded	Number of messages undelivered after the maximum number of transmissions. Along with Discards, it can indicate a wireless network under heavy interference or excessive load of wireless data traffic.
Discards	Number of messages untransmitted due to congestion. Normally, the messages are temporarily stored in an internal buffer until transmitted. When the buffer is full, frames are discarded until the buffer is cleared. When the number is high, it may indicate a wireless network with a heavy load of traffic.
FCS Errors	Number of received frames or frame parts containing an erroneous checksum requiring deletion. Messages are recovered using ACK and retransmitted by the sending device.
Discards: No Buffer	Number of times an incoming message could not be received due to a shortage of received buffers. A non-zero value identifies heavy data for your wireless network.
Discards: Wrong SA (Station Address)	Number of times a message was not transmitted because a wrong MAC address was used by the protocol stack. A non-zero value indicates an error situation in the communication between your driver and the protocol stack.
Discards: Bad WEP Key	Number of times a received message was discarded because it could not be decrypted. This could indicate mismatched keys or one device does not support encryption or does not have encryption enabled.
Message In	A measure of the amount of overlapped communications on your network.
Message In Bad	This number is expected to be zero. Non-zero values indicate a heavily loaded system.

Station Status

The **Station Status** table displays information about wireless connections associated with the TZ 170 Wireless.



Station Status

Station	MAC Address	Authenticated	Associated	Association Id	Tx Rate	Timeout	Power Mgmt	Delete
1	00:20:E0:41:07:8B	Authenticated	Associated	2	5 Mb/s	299s	Disabled	🗑

- **Station** - the name of the connection used by the MAC address
- **MAC Address** - the wireless network card MAC address
- **Authenticated** - status of 802.11b authentication
- **Associated** - status of 802.11b association
- **Association ID** - assigned by the SonicWALL
- **Tx Rate** - in Mbps
- **Timeout** - number of seconds left on the session
- **Power Mgmt** - if power management is enabled on your wireless network card, the setting is displayed here.
- **Delete** - delete the entry from the MAC Filter List.

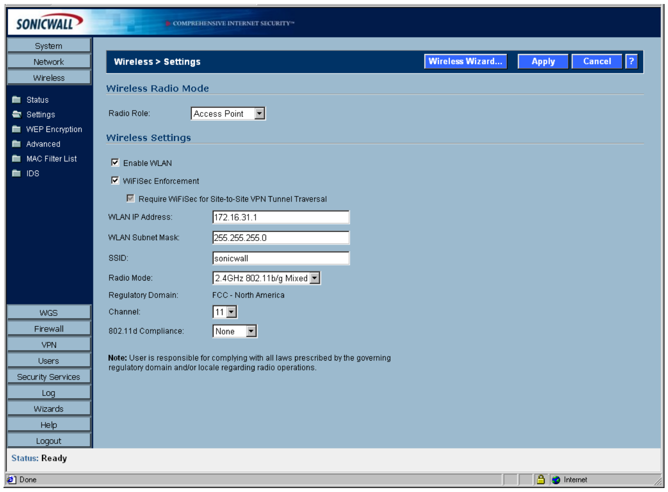
Wireless > Settings

Wireless Radio Mode

Select either Access Point to configure the SonicWALL as the default gateway on your network or select Bridge Mode to configure the SonicWALL to act as an intermediary wireless device.

Wireless>Settings

On the **Wireless>Settings** page, you can enable or disable the WLAN port by selecting or clearing the **Enable WLAN** checkbox.



Wireless > Settings

Wireless Radio Mode

Radio Role: Access Point

Wireless Settings

☑ Enable WLAN

☑ WiFiSec Enforcement

☑ Require WiFiSec for Site-to-Site VPN Tunnel Traversal

WLAN IP Address: 172.16.31.1

WLAN Subnet Mask: 255.255.255.0

SSID: sonicwall

Radio Mode: 2.4GHz 802.11b/g Mixed

Regulatory Domain: FCC - North America

Channel: 11

802.11d Compliance: None

Note: User is responsible for complying with all laws prescribed by the governing regulatory domain and/or locale regarding radio operations.

Status: Ready

WiFiSec Enforcement

Select **WiFiSec Enforcement** to use IPSec-based VPN for access from the WLAN to the LAN, and also provide access from the WLAN to WAN independent of Wireless Guest Services. If selected, wireless clients must download a copy of the Global VPN Client software to install on their computer. You must also configure and enable the Group VPN Security Association. When **WiFiSec Enforcement** is selected, a second check box, **Require WiFiSec for Site-to-Site VPN Tunnel Traversal** is selected by default. When **Require WiFiSec for Site-to-Site VPN Tunnel Traversal** is selected, any wireless traffic destined for a remote network with a VPN tunnel is secured by WiFiSec. If **WiFiSec Enforcement** is not selected, you can select or clear the **Require WiFiSec for Site to Site VPN Tunnel Traversal** checkbox.

You can configure a different IP address for the WLAN by typing another private IP address in the **WLAN IP Address** field. Type the subnet in the **Subnet Mask** field. Click **Apply** for the changes to take effect on the SonicWALL.

The default value, **sonicwall**, for the SSID can be changed to any alphanumeric value with a maximum of 32 characters.

Select your preferred radio mode from the **Radio Mode** menu. The TZ 170 Wireless supports the following modes:

- **Mixed** - Supports 802.11b and 802.11g clients simultaneously. If your wireless network comprises both types of clients, select this mode.
- **802.11g Only** - If your wireless network consists only of 802.11g clients, you may select this mode for increased 802.11g performance. You may also select this mode if you wish to prevent 802.11b clients from associating.

- **802.11b Only** - Select this mode if only 802.11b clients access your wireless network.

FCC - North America is displayed as the **Regulatory Domain**. This field is determined by the ROM code.

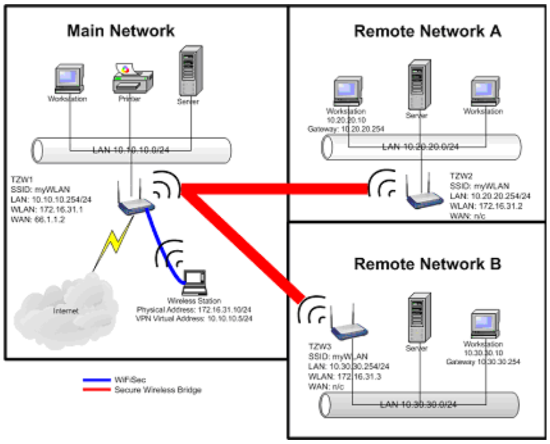
Select the channel for transmitting the wireless signal from the **Channel** menu. An **AutoChannel** setting allows the TZ170Wireless to automatically detect and set the optimal channel for wireless operation based upon signal strength and integrity. AutoChannel is the default channel setting, and it displays the selected channel of operation to the right. Alternatively, an operating channel within the range of your regulatory domain can be explicitly defined.

802.11d Compliance 802.11d is a regulatory domain update wherein physical and MAC layer signalling automatically behaves in accordance with geographic requirements for such settings as channels of operation and power. The TZ170 has three settings:

- **None** - The wireless device communicates with any other available wireless device, regardless of 802.11d compliance. This is useful for peer-to-peer (IBSS) networking which currently is not supported by the 802.11d standard.
- **Flexible** - The wireless device communicates with any other available wireless device, and abides by 802.11d information if it is presented.
- **Strict** - The wireless device only communicates with devices that support the 802.11d standard.

Secure Wireless Bridging

Wireless Bridging is a feature that allows two or more physically separated networks to be joined over a wireless connection. The TZ 170 Wireless provides this capability by shifting the radio mode at remote networks from **Access Point** mode to **Wireless Bridge** mode. Operating in Wireless Bridge mode, the TZ 170 Wireless connects to another TZ 170 Wireless acting as an access point, and allows communications between the connected networks via the wireless bridge.



Secure Wireless Bridging employs a WiFiSec VPN policy, providing security to all communications between the wireless networks. Previous bridging solutions offered no encryption, or at best, WEP encryption.

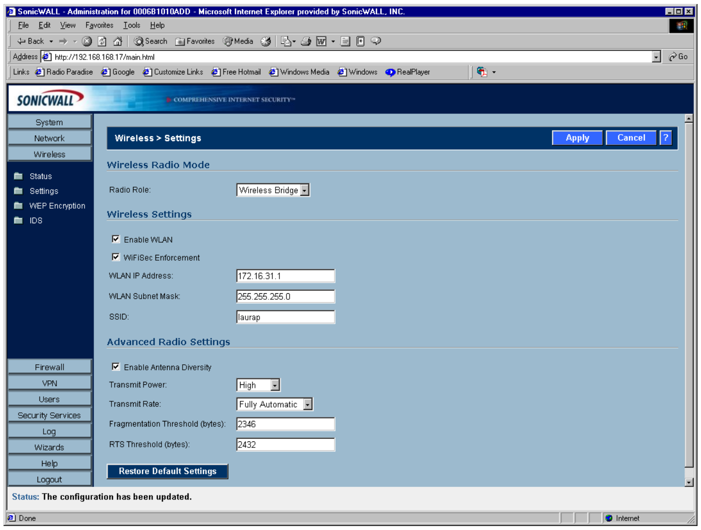
Wireless Bridging (without WiFiSec)

To provide compatibility with other non-WiFiSec wireless access points, the TZ 170 Wireless supports a non-secure form of wireless bridging, but insecure wireless communications should only be employed when data is non-sensitive. By default, **WiFiSec Enforcement** is enabled on **Wireless Settings** for **Wireless Bridge** Mode. To connect to a non-WiFiSec access point, this checkbox must be disabled. Since VPN tunnels are not established in non-secure Wireless Bridging deployments, traffic routes must be clearly defined for both the Access Point and the Bridge Mode sites:

- The default route on the Bridge Mode TZ 170 Wireless must from the WLAN interface to the WLAN interface of the connecting Access Point TZ 170 Wireless.
  - Referring to the example above, the default route on TZ 170 Wireless2 and TZ 170 Wireless3 is set via their WLAN interfaces to 172.16.31.1.
- Static routes must be entered on the Access Point TZ 170 Wireless to route back to the LAN subnets of the Bridge Mode TZ 170 Wireless.
  - Referring to the example network, TZ 170 Wireless1 must have static routes to 10.20.20.x/24 via 172.16.31.2 and to 10.30.30.x/24 via 172.16.31.3

Configuring a Secure Wireless Bridge

When switching from Access Point mode to Wireless Bridge mode, all clients are disconnected, and the navigation panel on the left changes to reflect the new mode of operation.


SonicWALL - Administration for 000681010ADD - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.17/main.html
Go
Links Radio Paradise Google Customize Links Free Hotmail Windows Media Windows RealPlayer
SONICWALL
COMPREHENSIVE INTERNET SECURITY™
System
Network
Wireless
Status
Settings
WEP Encryption
IDS
Firewall
VPN
Users
Security Services
Log
Wizards
Help
Logout
Apply
Cancel
?
Restore Default Settings
Done
Internet

Wireless > Settings

Wireless Radio Mode

Radio Role: Wireless Bridge

Wireless Settings

☑ Enable WLAN

☑ WiFiSec Enforcement

WLAN IP Address: 172.16.31.1

WLAN Subnet Mask: 255.255.255.0

SSID: laurap

Advanced Radio Settings

☑ Enable Antenna Diversity

Transmit Power: High

Transmit Rate: Fully Automatic

Fragmentation Threshold (bytes): 2346

RTS Threshold (bytes): 2432

Status: The configuration has been updated.

To configure a secure wireless bridge, follow these steps:

1. Click **Wireless**, then **Advanced**.
2. In the **Wireless Radio Mode** section, select **Wireless Bridge** from the **Radio Role** menu. The TZ 170 Wireless updates the interface.
3. Click **Status**. Any available access point is displayed at the bottom of the **Status** page. Click **Connect** to establish a wireless bridge to another TZ 170 Wireless.
4. Click **Settings**. Configure the WLAN settings for the wireless connection as follows:
    a. Configure the SSID on all TZ 170 Wireless to the SSID of the Access Point.
    b. Configure the WLAN for all TZ 170 Wireless must be on the same subnet.
    c. LAN IP address for all TZ 170 Wireless must be on different subnets.

For example, in the previous network diagram, the TZ 170 Wireless are configured as follows:

- SSID on all three TZ 170 Wireless are set to “myWLAN”.
- WLAN addressing for all the TZ 170 Wireless's connected via Wireless Bridge must place the WLAN interfaces on the same subnet: 172.16.31.1 for TZ 170 Wireless1, 172.16.31.2 for TZ 170 Wireless2, and 172.16.31.3 for TZ 170 Wireless3.
- TZ 170 Wireless4 must have a different subnet on the WLAN, such as 172.16.32.X/24.
- LAN addressing for all TZ 170 Wireless connected via Wireless Bridge must place the LAN interfaces on different subnets: 10.10.10.x/24 for TZ 170 Wireless1, 10.20.20.x/24 for TZ 170 Wireless2, and 10.30.30.x/24 for TZ 170 Wireless3.
- LAN addressing for TZ 170 Wireless4 must be the same as TZ 170 Wireless3.
- To facilitate Virtual Adapter addressing, the TZ 170 Wireless4 can be set to forward DHCP requests to TZ 170 Wireless3.
- When a TZ 170 Wireless is in Wireless Bridge mode, the channel cannot be configured. TZ 170 Wireless2 and TZ 170 Wireless3 operate on the channel of the connecting Access Point TZ 170 Wireless. For example, TZ 170 Wireless1 is on channel 1.
- A Bridge Mode TZ 170 Wireless cannot simultaneously support wireless client connections. Access Point services at Remote Site B are provided by a second TZ 170 Wireless (4). The channel of operation is set 5 apart from the channel inherited by the TZ 170 Wireless3. For example, Access

Point TZ 170 Wireless1 is set to channel 1, then Bridge Mode TZ 170 Wireless3 inherits channel 1. Access Point TZ 170 Wireless4 should be set to channel 6.

Network Settings for the Example Network

Device	Mode	SSID	Channel	LAN IP Address	WLAN IP Address
TZ 170 Wireless1	Access Point	myWLAN	1	10.10.10.254/24	172.16.31.1/24
TZ 170 Wireless2	Wireless Bridge	myWLAN	1 (auto)	10.20.20.254/24	172.16.31.2/24
TZ 170 Wireless3	Wireless Bridge	myWLAN	1 (auto)	10.30.30.254/24	172.16.31.3/24
TZ 170 Wireless4	Access Point	otherWLAN	6	10.30.30.253/24	172.16.31.1/24

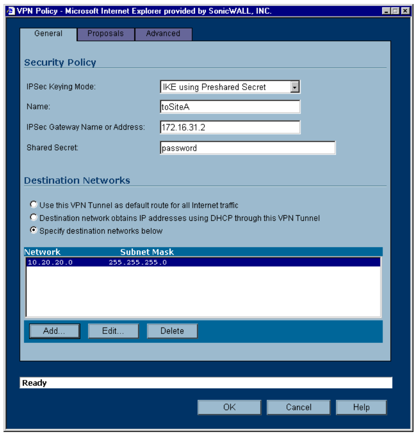
Configuring VPN Policies for the Access Point and Wireless Bridge

Access Point

After Wireless Settings are defined, the WiFiSec connections (VPN Policies) must be configured. The VPN Policies are defined as would any other site-to-site VPN policy, typically with the following in mind:

- The Access Point TZ 170 Wireless must specify the destination networks of the remote sites.
- The Access Point TZ 170 Wireless must specify its LAN management IP address as the **Default LAN Gateway** under the **Advanced** tab.
- The Wireless Bridge Mode TZ 170 Wireless must be configured to use the tunnel as the default route for all internet traffic.

Referring to our example network, the Access Point TZ 170 Wireless has the following two VPN Policies defined:


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Proposals
Advanced
Add...
Edit...
Delete
OK
Cancel
Help

Security Policy

IPSec Keying Mode: IKE using Preshared Secret

Name: toSiteA

IPSec Gateway Name or Address: 172.16.31.2

Shared Secret: password

Destination Networks

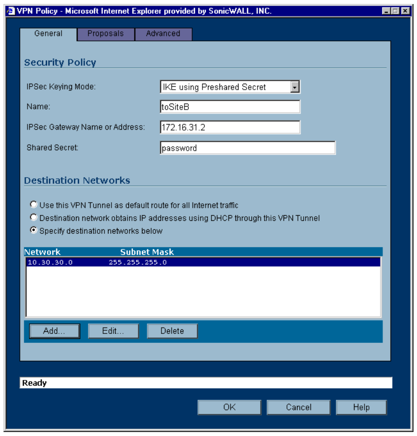
○ Use this VPN Tunnel as default route for all Internet traffic

○ Destination network obtains IP addresses using DHCP through this VPN Tunnel

● Specify destination networks below

Network	Subnet Mask
10.20.20.0	255.255.255.0

Ready


VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC.
General
Proposals
Advanced
Add...
Edit...
Delete
OK
Cancel
Help

Security Policy

IPSec Keying Mode: IKE using Preshared Secret

Name: toSiteB

IPSec Gateway Name or Address: 172.16.31.2

Shared Secret: password

Destination Networks

○ Use this VPN Tunnel as default route for all Internet traffic

○ Destination network obtains IP addresses using DHCP through this VPN Tunnel

● Specify destination networks below

Network	Subnet Mask
10.30.30.0	255.255.255.0

Ready

Advanced Configuration for both VPN Policies

5. Click **Advanced**.
6. Select **Enable Keep Alive** and **Try to bring up all possible tunnels**.
7. Select **Enable Windows Networking (NetBIOS) Broadcast**.
8. Select **Forward Packets to remote VPNs**.
9. Enter the LAN IP address of the Access Point in the **Default LAN Gateway** field.
10. Select **LAN** for **VPN Terminated at.**