Configuring the PCX4500 Gateway

The following sections describe how to configure the network and security settings for the PCX4500. You should be able to access these settings once you have completed the Ethernet or USB installation for your computer. In most cases, you will not need to change the default settings of the PCX4500.

If you plan to use the wireless access capability of the PCX4500, please review the “**PCX4500 Wireless Configuration**” section to set your security parameters. The default settings do not protect your home network from an attack by an unauthorized wireless user.

The PCX4500 contains an embedded Web server that allows you to change its configuration. The PCX4500 configuration web pages may be accessed through any Internet browser such as Microsoft Internet Explorer (5.0 or later recommended).

These web pages are password protected to prevent unauthorized changes.

The PCX4500 configuration options are available in these web page locations:

Configuration Option:		PCX4500 Web-based Management page location:
Turn the firewall On/Off (default: On)	see	Security
Setup access rules		Security -> Access Control
Setup DMZ (Demilitarized Zone)		Security -> DMZ host
Setup host name		Advanced -> System Settings
Setup fixed IP addresses for modem, PC’s		
Change modem’s DHCP server settings		Advanced -> DHCP Server
Change modem’s password		Advanced -> Users Settings
Upgrade firewall security		
Enable wireless encryption		

You may also check the PCX4500 status:

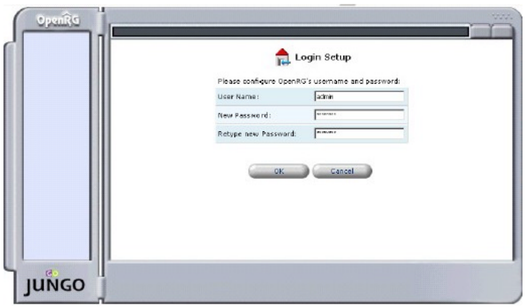
View firewall report	see	Security -> Firewall Log
View system log report		System Monitoring -> System Log
View traffic statistics		System Monitoring -> Traffic

Accessing Web-based Management

To access the management console:

Note: If your computer is running an operating system that supports UPnP, such as Windows Me or Windows XP, you can easily add the computer to your home network and access the Management Console directly from within Windows. See Pxx for information about connecting UPnP-enabled computers.

1. Launch a Web-browser on a PC in the LAN.
2. Type 'http://192.168.100.1',or 'http://mypox' in the address bar (Internet Explorer) or location bar (Netscape Navigator). The *Login* screen will appear.



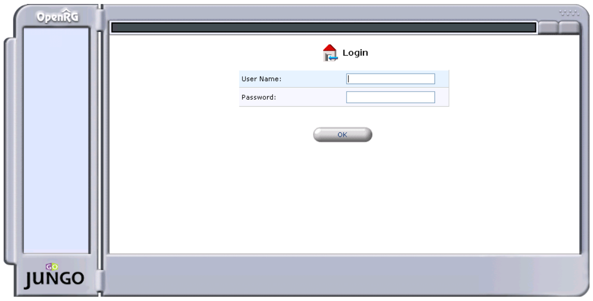
Login Setup

Please configure OpenRG's username and password:

User Name: admin

New Password:

Retype new Password:



Login

User Name:

Password:

Figure 14: Login Setup

Figure15: Login

3. Enter your username and password to log on to the web-based management.

   Note: for security reasons, you should change these settings after the initial login. See Pxx for details.

   Note: Your session will automatically finish after a few minutes of inactivity. If you try to operate the management console after the session has expired the *Login* screen will appear and you will have to reenter your user name and password before proceeding. This feature helps to prevent unauthorized users from accessing the web-based management and changing the gateway's settings.

The *Network Map* screen will appear.

Your Home Network Map

When you log into the management console you will see the *Network Map* screen.

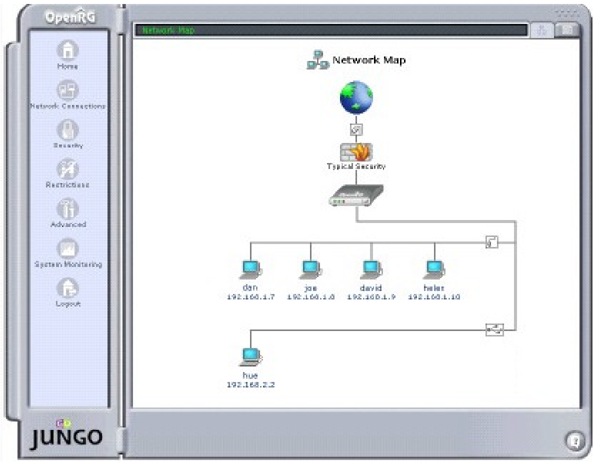


Figure 16: Network Map

The network map depicts each of the computers in your home network, PCX4500, the Firewall (inside the Gateway) and the external network (Internet). The following table explains the meaning of each part of the network map:

Represents the Internet

Represents your WAN (Wide Area Network) connection - your connection to the Internet - when using an Ethernet Gateway. Click this icon to configure the WAN interface (see P35).

Represents your WAN(Wide Area Network) connections - your connection to the Internet - when using a Wireless Interface. Click this icon to configure the WAN interface (see P41).

Represents the firewall built into PCX4500. The height of the wall corresponds to the security level currently selected: Minimum, Typical or Maximum. Click this icon to configure security settings (see P44).

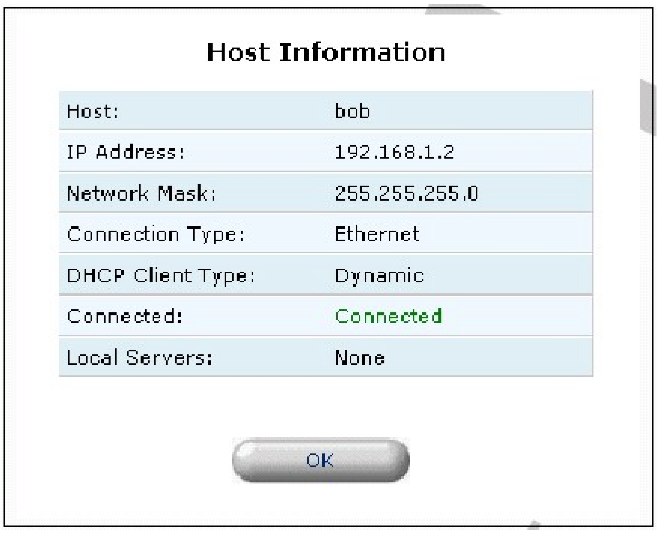
If PCX4500 is equipped with multiple LAN devices then the home network will be shown sub-divided into sub-networks (or subnets) and you will be able to see which computers are part of each sub-network. Click the icon listed below that represents the subnet you wish to configure.

Represents your Ethernet LAN (Local Area Network) connection. Click this icon to configure network parameters for the Ethernet LAN device (see P38).

Represents your USB LAN connection. Click this icon to configure network parameters for the USB LAN device.

Represents your Wireless LAN connection. Click this icon to configure network parameters for the Wireless LAN device.

Represents a computer (host) connected in the home network. Click this icon to view network information for the corresponding computer (see figure 17).



Host Information

Host:	bob
IP Address:	192.168.1.2
Network Mask:	255.255.255.0
Connection Type:	Ethernet
DHCP Client Type:	Dynamic
Connected:	Connected
Local Servers:	None

Figure 17: Host Information

Represents a computer (host) that is disabled or temporarily disconnected from the home network.

Left Sidebar

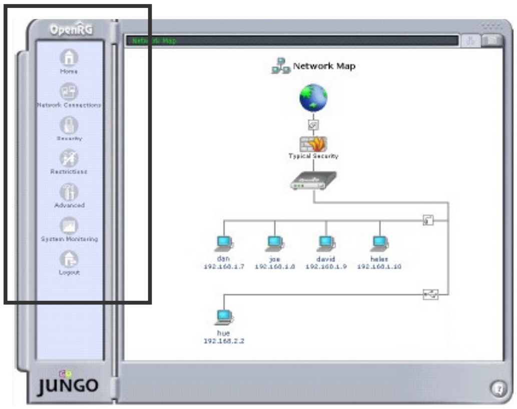


Figure 18: Left Sidebar

The web-based management screens have been grouped into several subject areas and may be accessed by clicking on the appropriate icon in the left sidebar. The subject areas are:

Home: Return to the Network Map

Network Connections: Create networks connections (see P35 or P38)

Wireless Connection: Configure the Wireless interface (see P41)

Security: Configure the firewall and regulate communications between the Internet and the home network (see P44)

Restriction: Block access to specific Internet web sites (see P56)

Advanced: Control network parameters (DHCP server, DNS) and perform administrative functions, including changing password and setting date & time (see P58)

System Monitoring: View network status, traffic statistics and the system log (see P71)

Logout: Log out from PCX4500

Navigational Aids

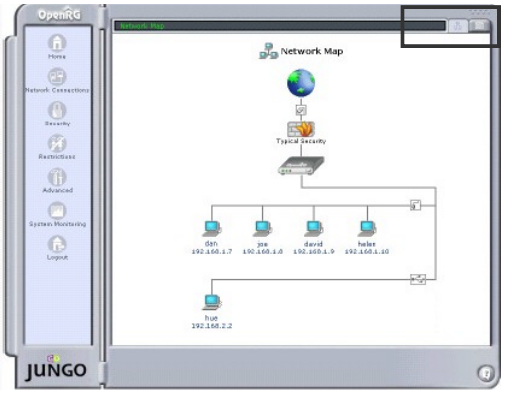


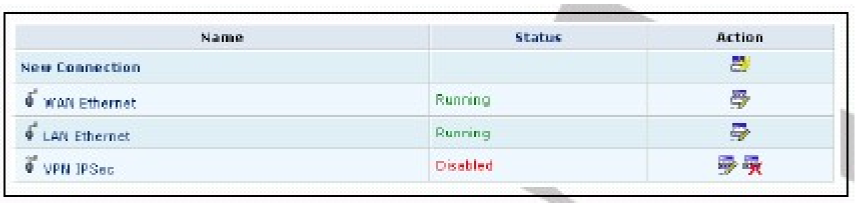
Figure 19: Host Information

The black navigator bar, located at the top of the management console, provides an easy way to locate the current screen in the hierarchy of web-based management screens. You may use it to quickly return to a screen that is *above* the current screen.

The icons listed below make it easy to quickly jump to key information about your home network. They are located on the right side of the management console.

Return to the *Network Map* screen

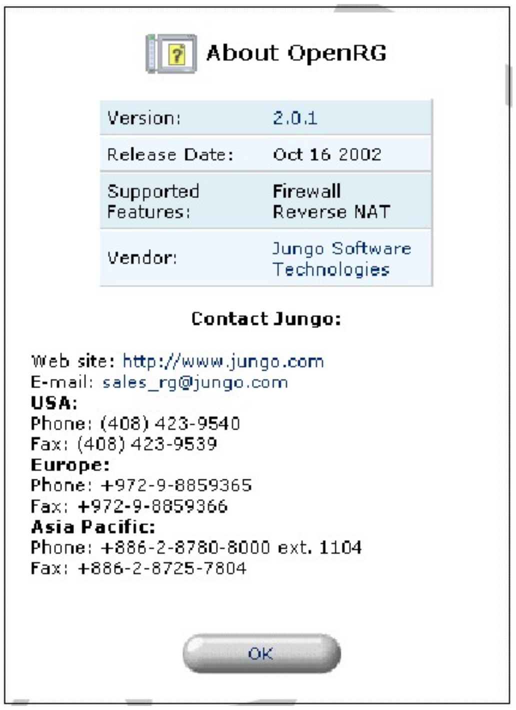
View a list of computers in the home network and the connection status of each. Also listed is the status of the Internet connection and the LAN connection.



Name	Status	Action
New Connection		
WAN Ethernet	Running	
LAN Ethernet	Running	
VPN IPSec	Disabled	

Figure 20: Network Connection

View technical information about the system that you are running, including version number and contact information.



About OpenRG

Version:	2.0.1
Release Date:	Oct 16 2002
Supported Features:	Firewall Reverse NAT
Vendor:	Jungo Software Technologies

Contact Jungo:

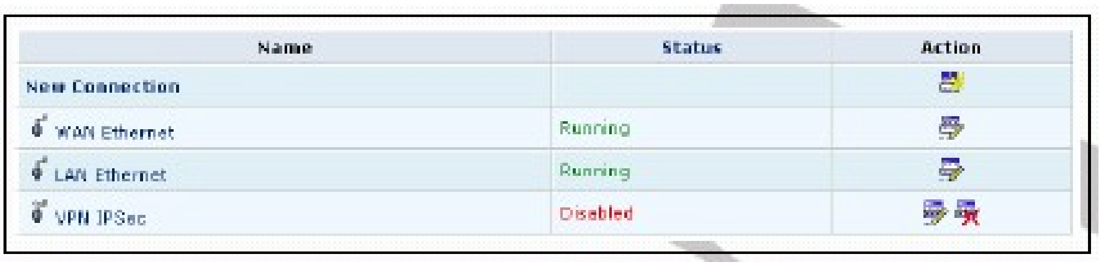
Web site: http://www.jungo.com
E-mail: sales_rg@jungo.com
USA:
Phone: (408) 423-9540
Fax: (408) 423-9539
Europe:
Phone: +972-9-8859365
Fax: +972-9-8859366
Asia Pacific:
Phone: +886-2-8780-8000 ext. 1104
Fax: +886-2-8725-7804

Figure 21: Host Information

Note: The management screens depicted in this manual may differ somewhat from the screens visible in your Management Console. This is primarily due to hardware differences between the various platforms for which PCX4500 is available.

Managing Lists

Lists are structures used throughout the web-based management. Lists handle user defined entries relating to elements such as network connections, local servers, restrictions and more. The principles outlined in this section apply to all list structures in the web-based management.



Name	Status	Action
New Connection		
WAN Ethernet	Running	
LAN Ethernet	Running	
VPN IPSec	Disabled	

Figure 22: Typical List Structure

Figure 22 illustrates a typical list structure. Each row defines an entry in the list. The following buttons located in the 'Action' column enable adding, editing and deleting list entries:

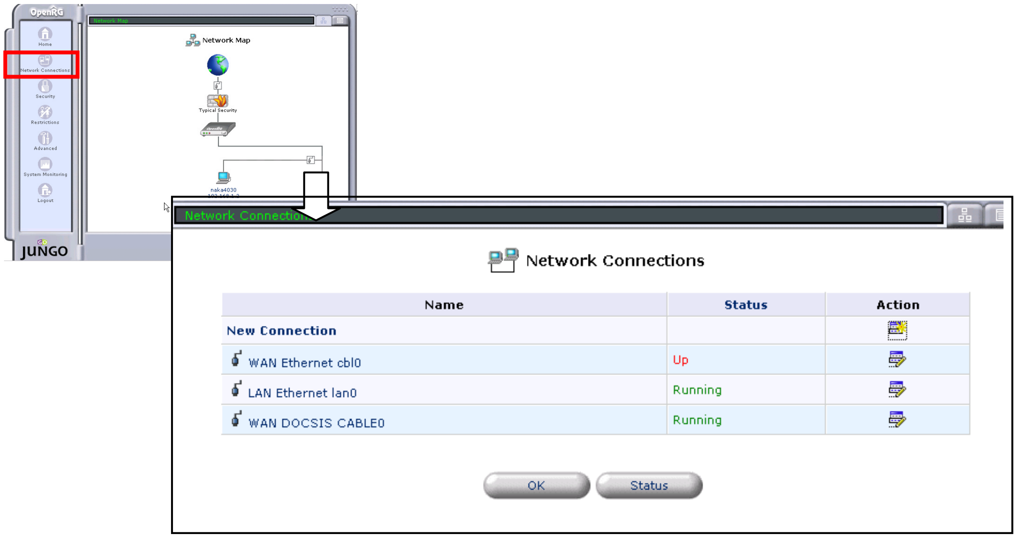
Use the **Add** button to add an item to the list. Fill in the list entry's fields, and click the **OK** button to add the entry to the list.

Use the **Edit** button to edit an item from the list.

Use the **Delete** button to remove an item from the list.

PCX4500 WAN Device Configuration

Click the **Network Connections** icon on the left side of the *PCX4500 Web-based Management* screen to display the *Network Connections* screen (see figure 23).



Network Connections

Name	Status	Action
New Connection		
WAN Ethernet cbl0	Up	
LAN Ethernet lan0	Running	
WAN DOCSIS CABLE0	Running	

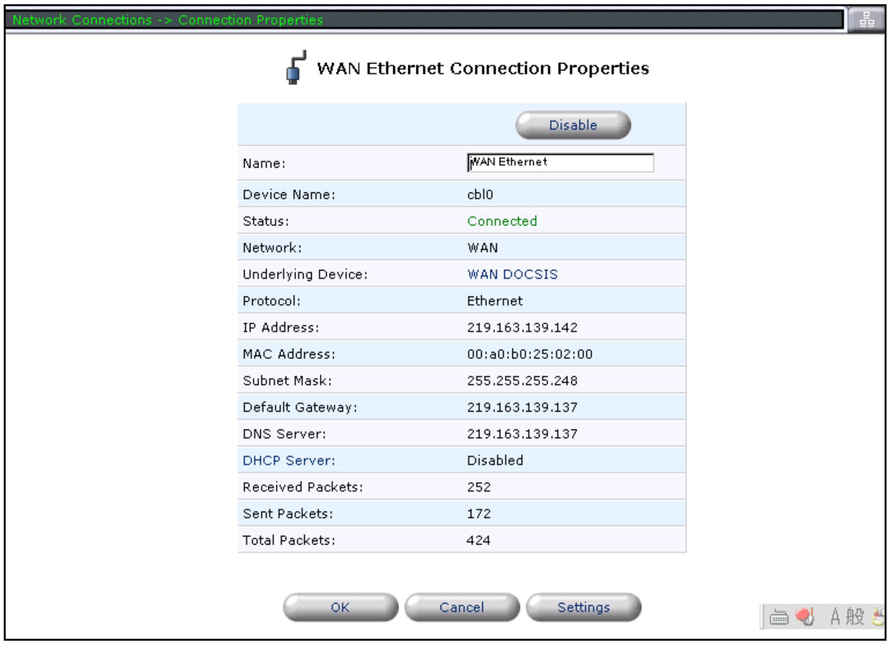
Figure 23: Network Connections

In *the Network Connections* screen, click **WAN Side**. The displayed screen allows you to set connection parameters and configure the appropriate protocol to be used for the WAN connection, according to the information provided by your service provider.
You can also use the *Network Connections* screen to monitor connection status.

Note: Some of the changes require knowledge of network communication protocols. Making changes without understanding the expected results could cause communication problems within your network.

Configuring the WAN Ethernet Device

1. In the *Network Connection* screen, click the **WAN Side**, or click the **Edit** button in the "Action" column for “WAN Side ” (see figure 23).
   The *Network Connection WAN Side* screen will appear (see figure 24).



Network Connections -> Connection Properties

WAN Ethernet Connection Properties

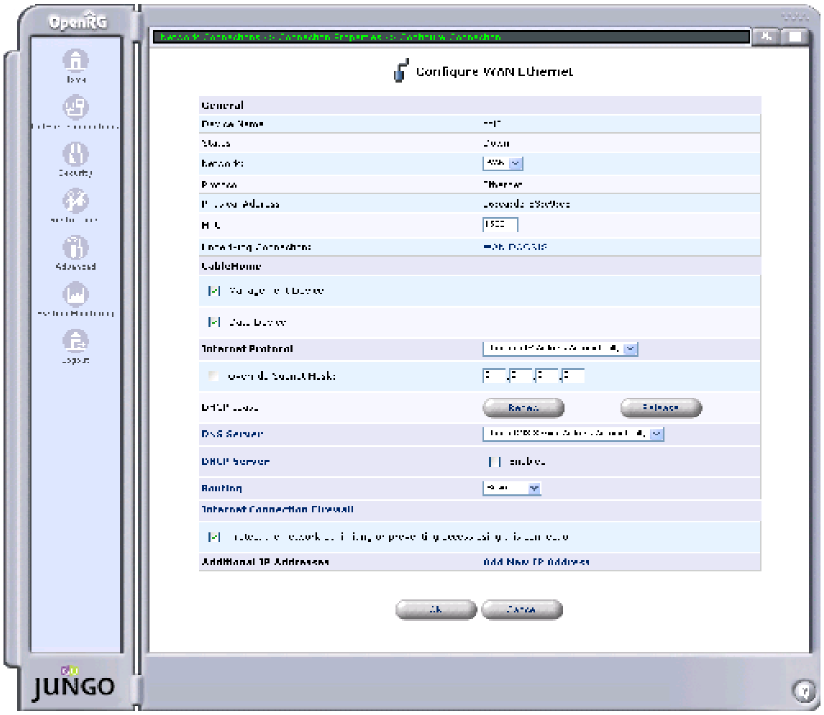
Disable

Name:	WAN Ethernet
Device Name:	cbl0
Status:	Connected
Network:	WAN
Underlying Device:	WAN DOCSIS
Protocol:	Ethernet
IP Address:	219.163.139.142
MAC Address:	00:a0:b0:25:02:00
Subnet Mask:	255.255.255.248
Default Gateway:	219.163.139.137
DNS Server:	219.163.139.137
DHCP Server:	Disabled
Received Packets:	252
Sent Packets:	172
Total Packets:	424

OK Cancel Settings

Figure 24: Network Connection WAN Side

2. The most recent network configuration for the WAN Ethernet Device is displayed. Click the **Settings** button to change the settings; the *Configure WAN Ethernet cbl0* screen will appear (see figure 25).



Configure WAN Ethernet

General	
Device Name	[illegible]
Status	[illegible]
Network	[illegible]
Protocol	Ethernet
[illegible] Address	[illegible]
MTU	[illegible]
Underlying Connection	WAN DOCSIS
CableHome	
☑ [illegible]	
☑ [illegible]	
Internet Protocol	[illegible]
□ Override Subnet Mask:	[illegible]
DHCP Lease	Renew Release
DNS Server	[illegible]
DHCP Server	□ enabled
Routing	[illegible]
Internet Connection Firewall	
☑ [illegible]	
Additional IP Addresses	Add New IP Address

OK Cancel

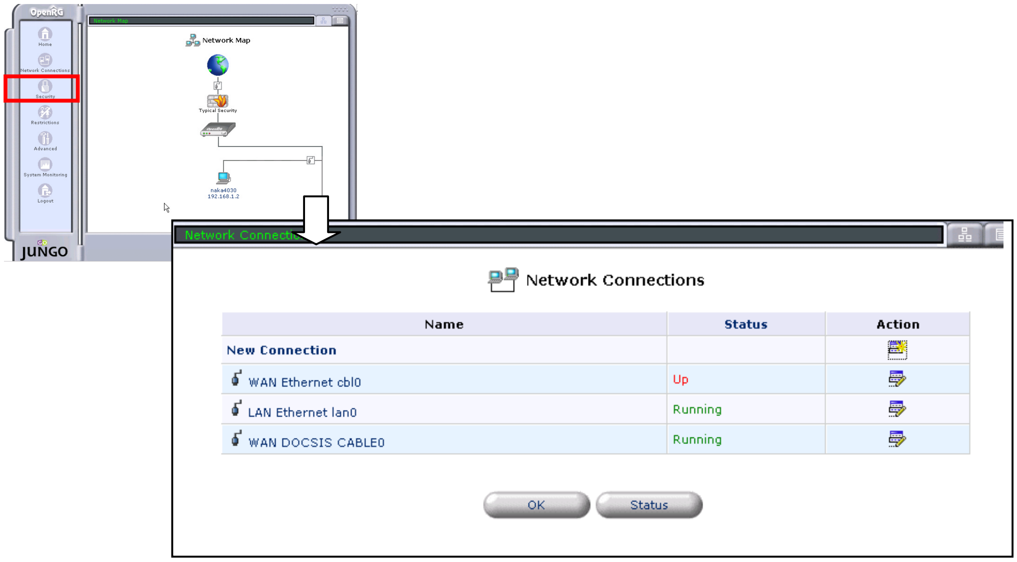
Figure 25: Configure WAN Side

3. Under “Internet Protocol”, select one of the following three methods to specify the desired address.
   - No IP Address: IP address is not specified at the WAN side. In this case, the system does not operate as a NAT.
   - Obtain an IP Address Automatically: The IP address is automatically obtained from the network side DHCP server (Factory default).

     * Override Subnet Mask: Select the check box and enter the value to manually specify an address without using the subnet mask obtained from the DHCP server.
   - Use The Following IP Address: Enter values in the “IP Address”, ”Subnet Mask” and ”Default Gateway” fields.
4. Under “DNS Server”, select one of the following two methods to specify a DNS server.
   - Obtain DNS Server Address Automatically: The DNS server address is automatically obtained from the DHCP server.
   - Use The Following DNS Server Address: Enter values in the “Primary DNS Server” and ”Secondary DNS Server” fields.
5. Under “Routing”, select one of the following two methods to specify the routing method.
   - Basic: Factory default
   - Advanced: Choose a routing mode in the “Routing Mode”, and enter values in the “ Device Metric”. If you use the default route, check the box next to the “Default Route”.
6. Click the **OK** button to save your changes.

PCX4500 LAN Device Configuration

Click the **Network Connections** icon on the left side of the *PCX4500 Web-based Management* screen to display *the Network Connections* screen (see figure 26).



Network Connections

Name	Status	Action
New Connection		
WAN Ethernet cbl0	Up	
LAN Ethernet lan0	Running	
WAN DOCSIS CABLE0	Running	

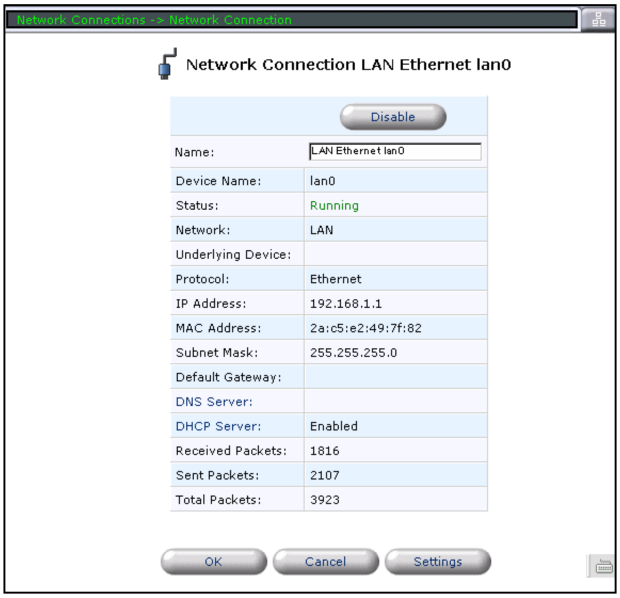
Figure 26:Network Connections

In the *Network Connections* screen, click **LAN Ethernet lan0**. The displayed screen allows you to modify the Local IP Address and/or Subnet Mask for the PCX4500's LAN device.
You can also use the *Network Connections* screen to monitor connection status.

Note: Some of the changes require knowledge of network communication protocols. Making changes without understanding the expected results could cause communication problems within your network. If something goes wrong you can always restore the PCX4500 factory default settings. Keep in mind, though, that you must be able to access the PCX4500 Web-based Management area in order to do so.

Configuring the LAN Device

1. In the *Network Connection* screen, click the **LAN Ethernet lan0**, or click the **Edit** button in the "Action" column for “LAN Ethernet lan0” (see figure 26).
   The *Network Connection LAN Ethernet lan0* screen will appear (see figure 27).



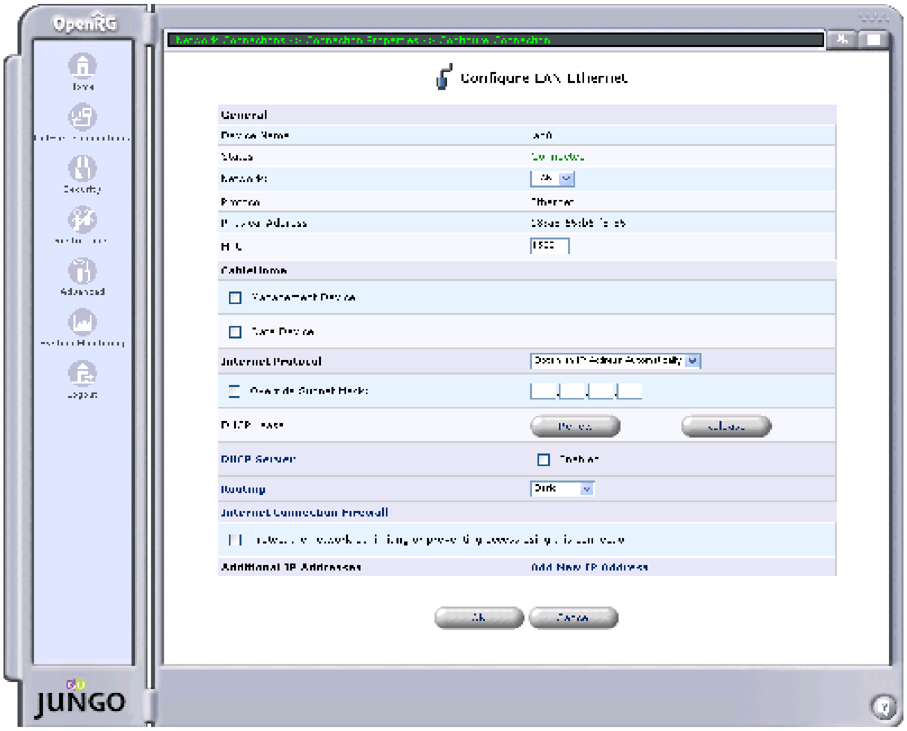
Network Connections -> Network Connection

Network Connection LAN Ethernet lan0

Name:	LAN Ethernet lan0
Device Name:	lan0
Status:	Running
Network:	LAN
Underlying Device:	
Protocol:	Ethernet
IP Address:	192.168.1.1
MAC Address:	2a:c5:e2:49:7f:82
Subnet Mask:	255.255.255.0
Default Gateway:	
DNS Server:	
DHCP Server:	Enabled
Received Packets:	1816
Sent Packets:	2107
Total Packets:	3923

Figure 27: Network Connection LAN Ethernet lan0

2. The most recent network configuration for the LAN Ethernet Device is displayed. Click the **settings** button to change the settings; the *Configure LAN Ethernet lan0* screen will appear (see figure 28).



Configure LAN Ethernet

General

Cable Home

Internet Protocol

DHCP Server

Routing

Internet Connection Firewall

Additional IP Addresses | Add New IP Address

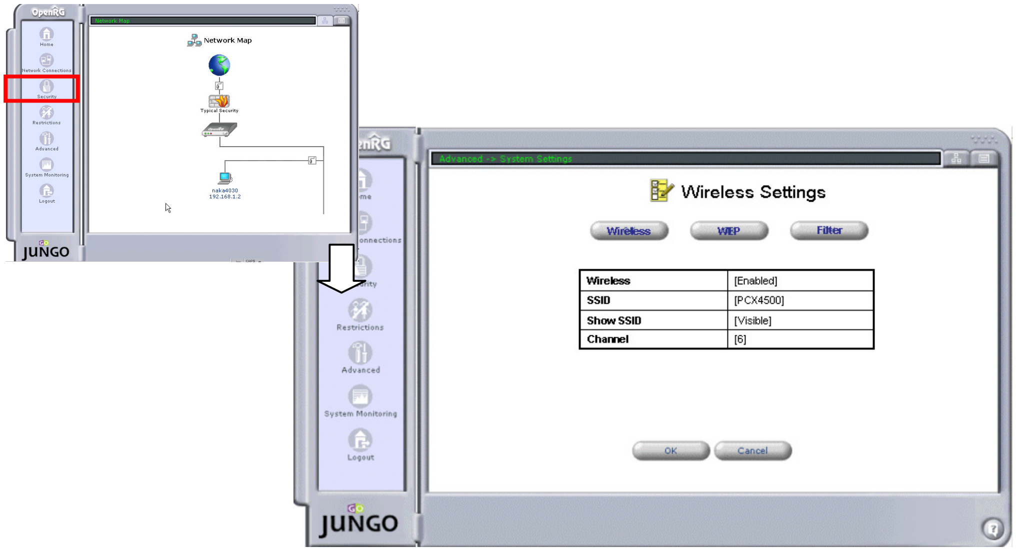
Figure 28: Configure LAN Ethernet lan0

3. Under "Internet Protocol", to specify the IP address, enter value in the “IP Address”, ”Subnet Mask” and ”Default Gateway” fields.
4. Under “DNS Server”, select one of the following methods to specify the DNS server.
   - Obtain DNS Server Address Automatically: The DNS server address is automatically obtained from the DHCP server.
   - Use The Following DNS Server Address: Enter values in the “Primary DNS Server” and ”Secondary DNS Server” fields.
5. Under “DHCP Server”, configure the desired DHCP settings.
   - Enabled: Select this check box to use the DHCP server.
   - Start/End: Enter values in the ”Start” and ”End” fields to specify the range of IP addresses provided by the DHCP server.

     Note: The DHCP server can provide a maximum of 253 addresses, not including LAN side IP addresses. You can include LAN side IP addresses in the IP address range specified here.
   - Lease Time in Minutes: Enter the lease time (in minutes).
   - Provide host name if not specified by client: When you select this check box, PCX4500 defines the host name when the host name cannot be obtained.
6. Configure "Additional IP Address" as needed.
7. Click the **OK** button to save your changes.

PCX4500 Wireless Configuration

You can use the *Wireless Settings* screen to set parameters related to the PCX4500 wireless interface.Click the **Wireless** icon on the left side of *the PCX4500 Web-based Management* screen to display the *Wireless Settings* screen (see figure 29).



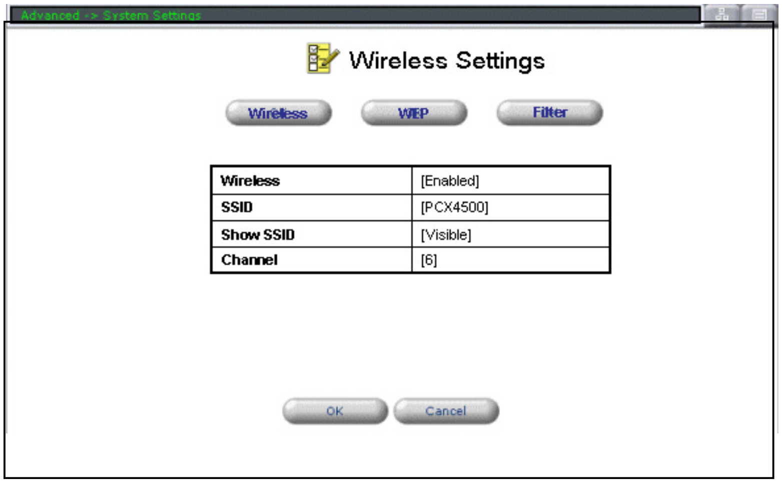
Wireless	[Enabled]
SSID	[PCX4500]
Show SSID	[Visible]
Channel	[6]

Figure 29: Wireless Settings

You use this screen to select the wireless interface you want to use and to set the SSID.

Configuring the Wireless Interface setting

1. Click the **Wireless** button on the *Wireless Settings* screen. The *Wireless Settings* screen that configures wireless interface setting will appear (see figure 30).



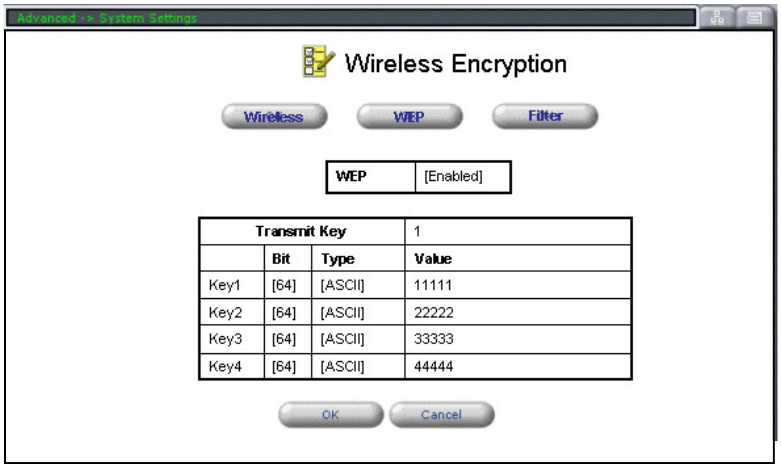
Wireless	[Enabled]
SSID	[PCX4500]
Show SSID	[Visible]
Channel	[6]

Figure 30: Wireless Settings Screen – Configuring the wireless interface

2. Complete the following the fields:
   - Wireless: Select "Enabled" or "Disabled" for the Access Point. The factory default is "Enabled".
   - SSID: Enter text for SSID Access Point within 31 characters. The factory default is "PCX4500".
   - Channel: From 1 to 11, select a channel to be used for communication between the Access Point and wireless station. The factory default is “10“.
3. Click the **OK** button to save your changes.

Configuring the WEP setting

1. Click the **WEP** button on the *Wireless Settings* screen. The *Wireless Encryption* screen that configures a WEP (wireless encryption and authentication) will appear (see figure 31).



WEP	[Enabled]

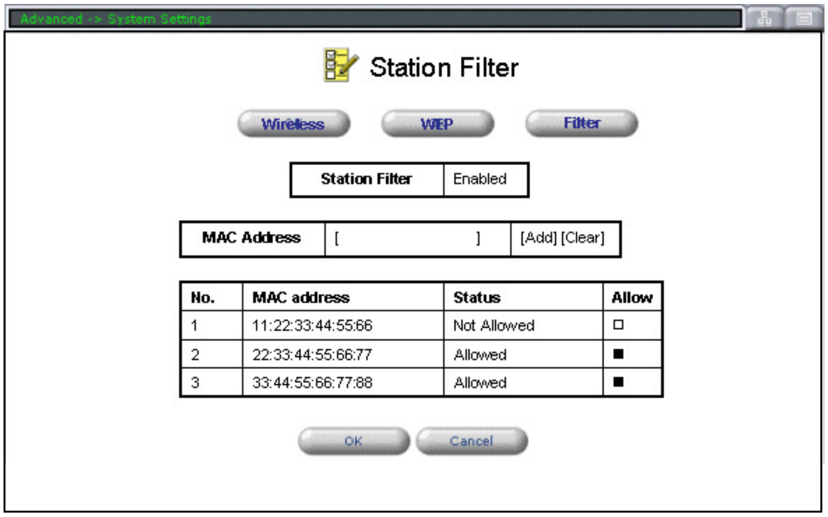
Transmit Key			1
	Bit	Type	Value
Key1	[64]	[ASCII]	11111
Key2	[64]	[ASCII]	22222
Key3	[64]	[ASCII]	33333
Key4	[64]	[ASCII]	44444

Figure 31: Wireless Encryption Screen

2. Complete the following the fields:
   - WEP: Select "Enabled" or "Disabled" for WEP. The factory default is "Disabled".
   - Transmit Key: Select WEP Key1 to Key4 that will be used for transmission.
   - Bit: Select 64, 128, or 256 for the WEP key length.
   - Type: Select Hex or ASCII for the data entry format of the WEP key.
   - Value: Enter the value of the WEP key.
3. Click the **OK** button to save your changes.

Configuring the Station Filter setting

1. Click the **Filter** button on the *Wireless Settings* screen.The *Station Filter* screen that configures a wireless interface will appear (see figure 32).



Station Filter	Enabled

MAC Address	[ ]	[Add] [Clear]

No.	MAC address	Status	Allow
1	11:22:33:44:55:66	Not Allowed	□
2	22:33:44:55:66:77	Allowed	■
3	33:44:55:66:77:88	Allowed	■

Figure 32: Station Filter

2. In the Station Filter field, select "Enabled" or "Disabled" for station filtering. The factory default is "Enabled".
3. The MAC address of the wireless terminal that is accessing the network is automatically registered in the "MAC address" field. In default status, access by the terminal is not allowed. However, if there is no other "Allowed" terminal, access by this terminal is temporarily allowed when "Temporary Allowed" status is in effect. When even one terminal is registered as "Allowed", other "Temporary Allowed" terminals change to "Not Allowed" status.
4. To manually register an address, enter the Mac address subject to filtering in the "Mac Address" field and then click the **Add** button.The entered Mac address is added in the table under the entry field with “**Allowed**” status.

Note: When you select the "Allow" check box, the registered Mac address becomes accessible. Until the **OK** button is pressed, this setting is not effective in operation.

5. Click the **OK** button to save your changes.

Security

PCX4500's Security Suite includes comprehensive, robust security services: Stateful inspection Firewall, user authentication protocols and password protection mechanisms. These features taken together allow users to connect their computers to the Internet and simultaneously be protected from the security threats of the Internet.

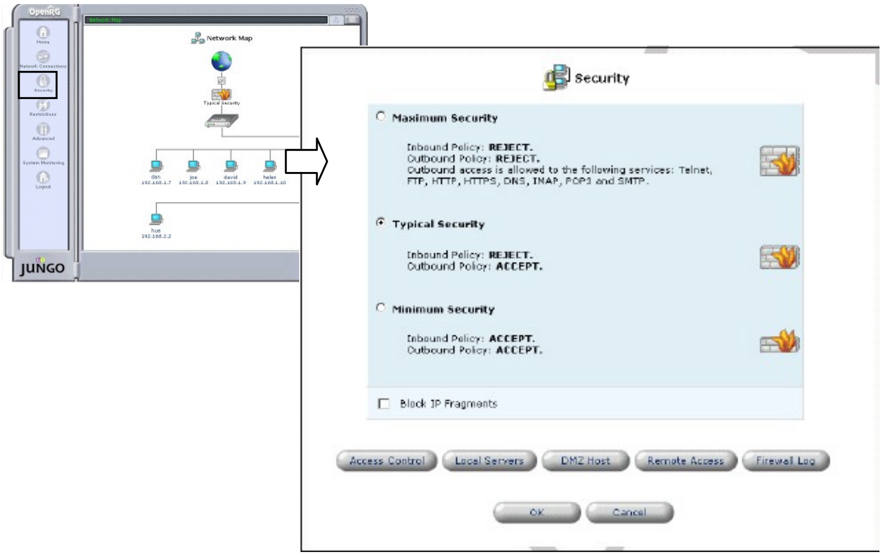
PCX4500's Firewall (RG-FW^{TM}), the cornerstone of PCX4500's security suite, has been exclusively tailored to the needs of the residential user and has been pre-configured to provide optimum security. In addition, the Firewall has many advanced features which allow you to further customize it to your needs.

Using the management screens in the Security section, you can:

- Choose the Security Level for the Firewall (see P44)
- Set Access Controls to prohibit computers in the home network from accessing services on the Internet (see P46)
- Configure the Local Servers available in the home network (see P48)
- Designate a local computer as a DMZ Host so that network traffic associated with certain Internet applications can bypass the Firewall (see P52)
- Configure Remote Access to enable remote configuration of PCX4500 from any Internet accessible computer (see P53)
- View and configure the Firewall Log (see P54)

Security Level Setting

Use the *Security* screen to configure PCX4500 's basic security settings (see figure 33).



○ **Maximum Security**

Inbound Policy: **REJECT.**
Outbound Policy: **REJECT.**
Outbound access is allowed to the following services: Telnet, FTP, HTTP, HTTPS, DNS, INAP, POP3 and SMTP.

● **Typical Security**

Inbound Policy: **REJECT.**
Outbound Policy: **ACCEPT.**

○ **Minimum Security**

Inbound Policy: **ACCEPT.**
Outbound Policy: **ACCEPT.**

□ Block IP Fragments

Figure 33: Security

The Firewall regulates the flow of data between the home network and the Internet.
Both incoming and outgoing data are inspected and then accepted (allowed to pass through PCX4500) or rejected (barred from passing through PCX4500) according to a flexible and configurable set of rules. These rules are designed to prevent unwanted intrusions from the outside while allowing home users access to the Internet services that they require.

The Firewall rules specify what types of services available on the Internet may be accessed from the home network and what types of services available in the home network may be accessed from the Internet. Each request for a service that the Firewall receives, whether originating in the Internet or from a computer in the home network, must be checked against the set of Firewall rules to determine whether the request should be allowed to pass through the Firewall. If the request is permitted to pass, then all subsequent data associated with this request (a "session") will also be allowed to pass, regardless of its direction.

For example, when you point your Web browser to a Web page on the Internet a request is sent out to the Internet for this page. When the request reaches PCX4500, the Firewall will identify the request type and origin-HTTP and a specific PC in your home network, in this case. Unless you have configured access control to block requests of this type from this computer, the Firewall will allow this request to pass out onto the Internet (see Pxx for more on setting access controls). When the Web page is returned from the Web server the Firewall will associate it with this session and allow it to pass, regardless of whether HTTP access from the Internet to the home network is blocked or permitted.

The important thing to note here is that it is the origin of the request, not subsequent responses to this request, that determines whether a session can be established or not.

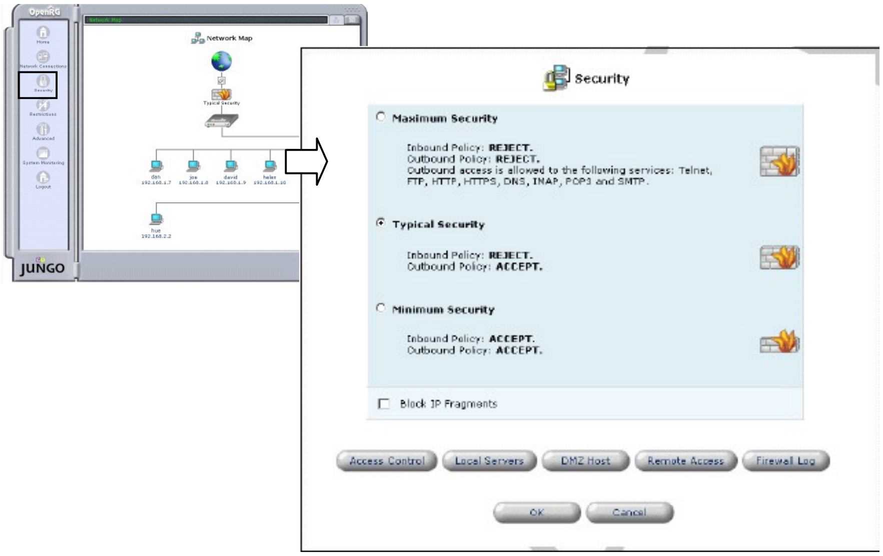
You may choose from among three pre-defined security levels for PCX4500: Minimum, Typical (the default setting) and Maximum. The table below summarizes the behavior of PCX4500 for each of the three security levels. Note that the Access Control, Local Servers and Remote Access screens may be used to further customize PCX4500's security settings.

- The *Access Control* screen can be used to further restrict access from the home network to the Internet (see P46).
- The *Local Servers* screen can be used to enable access from the Internet to specified services provided by computers in the home network and special Internet applications (see P48).
- The *Remote Access* screen can be used to enable remote configuration of PCX4500 from any Internet-accessible computer (see P53).

Security Level	**Requests Originating in the WAN**	**Requests Originating in the LAN**
Maximum	*Blocked*: No access to home network from Internet, except as configured in the Local Servers and Remote Access screens	*Limited*: Only commonly-used services, such as Web-browsing and e-mail, are permitted*
Typical (Default)	*Blocked*: No access to home network from Internet, except as configured in the Local Servers and Remote Access screens	*Unrestricted*: All services are permitted, except as configured in the Access Control screen
Minimum	*Unrestricted*: Permits full access from Internet to home network all connection attempts permitted.	*Unrestricted*: All services are permitted, except as configured in the Access Control Screen

*These services include Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3 and SMTP

- **To configure PCX4500's security settings (see figure 34)**



Security

○ **Maximum Security**

Inbound Policy: **REJECT.**
Outbound Policy: **REJECT.**
Outbound access is allowed to the following services: Telnet, FTP, HTTP, HTTPS, DNS, INAP, POP3 and SMTP.

● **Typical Security**

Inbound Policy: **REJECT.**
Outbound Policy: **ACCEPT.**

○ **Minimum Security**

Inbound Policy: **ACCEPT.**
Outbound Policy: **ACCEPT.**

☐ Block IP Fragments

Figure 34: Security

1. Choose from among the three pre-defined security levels described in the table above. *Typical Security* is the default setting.

   Note: Using the *Minimum Security* setting may expose the home network to significant security risks, and thus should only be used, when necessary, for short periods time.

2. Check the **Block IP Fragments** box in order to protect your home network from a common type of hacker attack that could make use of fragmented data packets to sabotage your home network. Note that VPN over IPSec and some UDP-based services make legitimate use of p fragments. You will need to allow IP fragments to pass into the home network in order to make use of these select services.

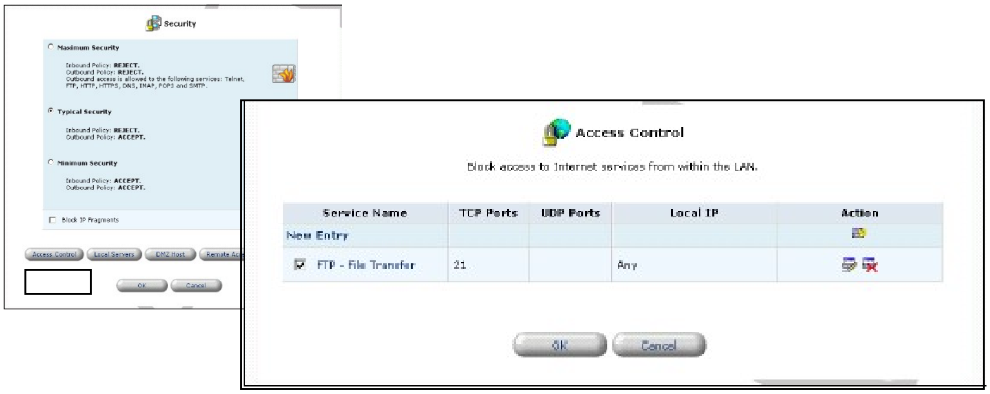
3. Click the **OK** button to save your changes.

Adding Access Controls

You may want to block specific computers within the home network (or even the whole network) from accessing certain services on the Internet. For example, you may want to prohibit one computer from surfing the Web, another computer from transferring files using FTP, and the whole network from receiving incoming e-mail.

Access Controls work by placing restrictions on the types of requests that requests pass from the home network out to the Internet, and thus may block traffic flowing in both directions. In the e-mail example given above, you may prevent computers in the home network from receiving incoming e-mail by blocking their *outgoing* requests to POP3 servers on the Internet.

Click the **Access Control** button in the *Security* screen to view a list of services that have been restricted (see figure 34).



Security

○ Maximum Security

Inbound Policy: **REJECT.**
Outbound Policy: **REJECT.**
Outbound access is allowed to the following services: Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3 and SMTP.

● Typical Security

Inbound Policy: **REJECT.**
Outbound Policy: **ACCEPT.**

○ Minimum Security

Inbound Policy: **ACCEPT.**
Outbound Policy: **ACCEPT.**

□ Block IP Fragments

Access Control

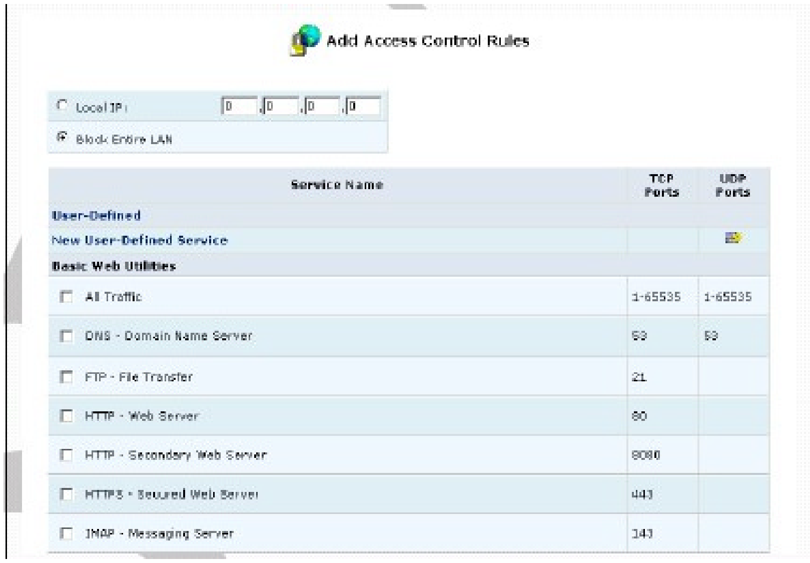
Block access to Internet services from within the LAN.

Service Name	TCP Ports	UDP Ports	Local IP	Action
New Entry				
☑ FTP - File Transfer	21		Any	

Figure 34: Access Control

- **To add a new service or services to the Access Control table:**

1. Click the **New Entry** button in the *Access Control* screen (see figure 34). The *Add Access Control Rules* screen will appear (see figure 35).



Add Access Control Rules

○ Local IP : 0 . 0 . 0 . 0

● Block Entire LAN

Service Name	TCP Ports	UDP Ports
User-Defined		
New User-Defined Service		
Basic Web Utilities		
□ All Traffic	1-65535	1-65535
□ DNS - Domain Name Server	53	53
□ FTP - File Transfer	21	
□ HTTP - Web Server	80	
□ HTTP - Secondary Web Server	8080	
□ HTTPS - Secured Web Server	443	
□ IMAP - Messaging Server	143	

Figure 35: Add Access Control Rule

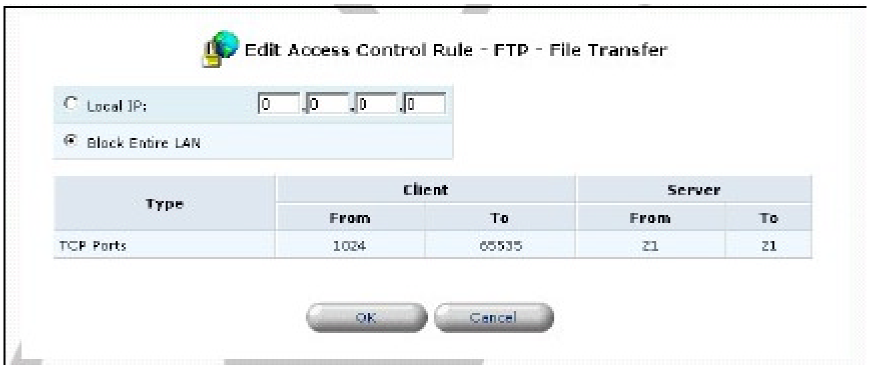
2. Select the service or services that you would like to block.
3. Enter the local IP address of the computer that you would like to block from accessing the service (s). "0.0.0.0' will block all computers.
4. Click the **OK** button to save your changes and return to the *Access Control* screen.

Note: To block a service that is not included in the list, click the **Add User Defined Service** button. The *Edit Service* screen will appear. Define the service, and click the **OK** button to save your changes (see P51 for details). The service will then be automatically added to the *Add Access Control Rules* screen. You may now select the service, just as you would a pre-defined service.

You may change the computer (or computers) prohibited from accessing a particular service by modifying the appropriate entry in the Access Control table.

- **To modify an entry in the Access Control table:**

1. Click the **Edit** button for the service in the *Access Control* screen (see figure 34). The *Edit Access Control Rule* screen will appear (see figure 36).



Edit Access Control Rule - FTP - File Transfer

○ Local IP: 0 . 0 . 0 . 0

● Block Entire LAN

Type	Client		Server	
	From	To	From	To
TCP Ports	1024	65535	21	21

Figure 36: Edit Access Control Rule

2. Enter the IP address of the computer that you would like to block from accessing the service(s), or select ‘Block Entire LAN’ to block all LAN computers.
3. Click the **OK** button to save your changes and return to the *Access Control* screen.

You may disable an access control without removing the service from the Access Control table. This may be useful if you wish to make the service available only temporarily and expect that you will want to reinstate the restriction in the future.

- **To temporarily disable an access control:**

1. Clear the check box next to the service name. The status for the service will change to **Disabled**.

- **To reinstate the restriction at a later time:**

1. Select the check box to next to the service name. The status for the service will change to **Enabled**.

- **To remove an access restriction from the Access Control table:**

1. Click the **Remove** button for the service. The service will be removed from the Access Control table.

Local Servers

In its default state, PCX4500 blocks all external users from connecting to or communicating with your network. Therefore the system is safe from hackers who may try to intrude on the network and damage it. However, you may need to expose your network to the Internet in certain limited and controlled ways in order to enable some applications to work from the LAN (game, voice and chat applications, for example) and to establish servers in the home network. PCX4500 's Local Servers feature supports both of these functionalities.

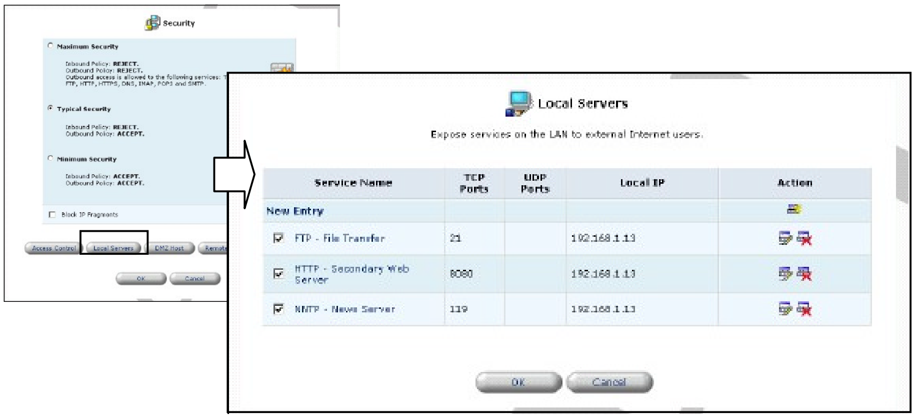
The *Local Servers* screen in the Management Console provides a list of the most commonly used applications that require special handling by PCX4500 -all you have to do is identify which of them you want to use and the local I P address of the computer that will be using the service. For example, if you wanted to use the Net2Phone voice application on one of your PCs, you would simply select 'Net2Phone' from the list and enter the local IP address of that computer in the right-hand column. All Net2Phone-related data arriving at PCX4500 from the Internet will henceforth be forwarded to the specified computer.

Similarly, if you want to grant Internet users access to servers inside your home network, you must identify each service that you want to provide and the PC that will provide it. For example, if you want to host a Web server inside the home network you must select 'HTTP - Web Server' from the list and enter the local IP address of the computer that will host the Web server in the right-hand column. Then when an Internet user points her browser to the external IP address of PCX4500 the Gateway will forward the incoming http request to the computer that is hosting the Web server.

Note that if an Internet application that you wish to use or a service that you wish to provide is not already in the list, you can easily add it (see P51).

Note: Application Level Gateways (ALGs)
Some applications, such as FTP, TFTP, PPTP and H323, require the support of special application-specific ALC (Application Level Gateway) modules in order to work inside the home network. Data packets associated with these applications contain information that allows them to be routed correctly. An ALG is needed to handle these packets and ensure that they reach their intended destinations. PCX4500 is equipped with a robust list of ALG modules in order to enable maximum functionality in the home network.

Click the **Local Servers** button in the *Security* screen to view the list of special services and local servers that are currently enabled in the home network (see figure 37).



Security

○ Maximum Security

Inbound Policy: **REJECT.**
Outbound Policy: **REJECT.**
Outbound access is allowed to the following services: T
FTP, HTTP, HTTPS, DNS, IMAP, POP3 and SMTP.

● Typical Security

Inbound Policy: **REJECT.**
Outbound Policy: **ACCEPT.**

○ Minimum Security

Inbound Policy: **ACCEPT.**
Outbound Policy: **ACCEPT.**

□ Block IP Fragments

Local Servers

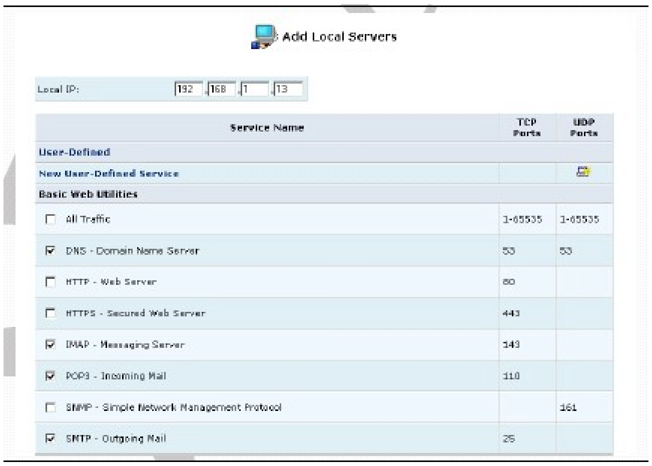
Expose services on the LAN to external Internet users.

Service Name	TCP Ports	UDP Ports	Local IP	Action
New Entry				
☑ FTP - File Transfer	21		192.168.1.13	
☑ HTTP - Secondary Web Server	8080		192.168.1.13	
☑ NNTP - News Server	119		192.168.1.13	

Figure 37: Local Servers

- **To add a new service to the list of active local servers:**

1. Click the **New Entry** button in the *Local Servers* screen (see figure 37). The *Add Local Servers* screen will appear (see figure 38).



Add Local Servers

Local IP: 192 .168 .1 .13

Service Name	TCP Ports	UDP Ports
User-Defined		
New User-Defined Service		
Basic Web Utilities		
□ All Traffic	1-65535	1-65535
☑ DNS - Domain Name Server	53	53
□ HTTP - Web Server	80	
□ HTTPS - Secured Web Server	443	
☑ IMAP - Messaging Server	143	
☑ POP3 - Incoming Mail	110	
□ SNMP - Simple Network Management Protocol		161
☑ SMTP - Outgoing Mail	25	

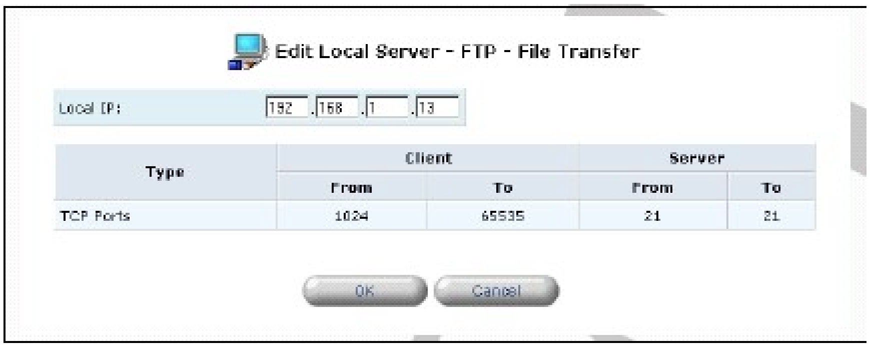
Figure 38: Add Local Servers

2. Select the service that you would like to provide.
3. Enter the local IP address of the computer that will provide the service (the "server”). Note that only one LAN computer can be assigned to provide a specific service or application.
4. Click the **OK** button to save your changes and return to the *Local Servers* screen.

Note: To add a service that is not included in the list click the **Add User Defined Service** button. The *Edit Local Server* screen will appear (see figure 39). Define the service and click the **OK** button to save your changes (see P51 for detaila). The service will then be automatically added to the *Add Local Servers* screen. You may now select the service, just as you would a pre-defined service.

- **To edit an entry in the Local Servers table so that a service can be provided by a different local computer:**

1. Click the **Edit** button for the service in the *Local Servers* screen (see figure 37). The *Edit Local Server* screen will appear (see figure 39).



Edit Local Server - FTP - File Transfer

Local IP: 192 . 168 . 1 . 13

Type	Client		Server	
	From	To	From	To
TCP Ports	1024	65535	21	21

Figure 39: Edit Local server

2. Enter the IP address of the computer that you would like to provide this service.
3. Click the **OK** button to save your changes and return to the *Local Servers* screen.

You may disable a service without removing the service from the Local Servers table. This may be useful if you wish to make the service unavailable only temporarily and expect that you will want to make it available again in the future.

- **To temporarily disable an access control:**

1. Clear the check box next to the service name.

- **To reinstate the restriction at a later time:**

1. Select the check box next to the service name.

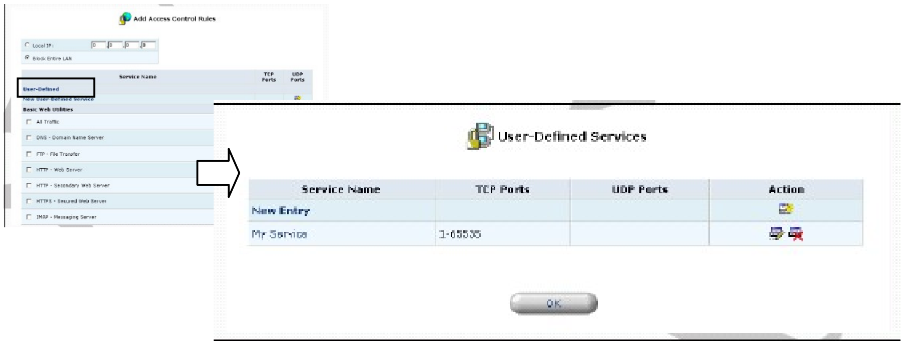
- **To remove an access restriction from the Access Control table:**

1. Click the **Remove** button for the service. The service will be removed from the Access Control table.

Note: How many computers can use a service or play a game simultaneously? Well, the answer may be a bit confusing. All the computers on the network can use a specific service as clients simultaneously. Being a client means that the computer within the network initiates the connection – for example, opens an FTP connection with an FTP server on the Internet. But only one computer can serve as a server, meaning responding to requests from computers on the Internet. Assigning a specific computer as a server is done in the Local Servers sectinon of Web-based management.

User-defined Service

The tables that appear on the *Add Access Control Rules* and *Add Local Servers* screens are pre-configured to include most of the services that users may wish to block or activate. Sometimes, however, the need arises to add non a pre-defined service. PCX4500 provides the *User-Defined Services* list (see figure 40) for this purpose. All of the services in this list also appear at the top of the *Add Access Control Rules* and *Add Local Servers* screens. When a service is added to one list it automatically appears in the others. In this way, user-defined services never need to be entered twice.



Add Access Control Rules

○ Local IP: 0 . 0 . 0 . 0
● Block Entire LAN

Service Name	TCP Ports	UDP Ports
User-Defined		
New User-Defined Service		
Basic Web Utilities		
□ All Traffic		
□ DNS - Domain Name Server		
□ FTP - File Transfer		
□ HTTP - Web Server		
□ HTTP - Secondary Web Server		
□ HTTPS - Secured Web Server		
□ IMAP - Messaging Server		

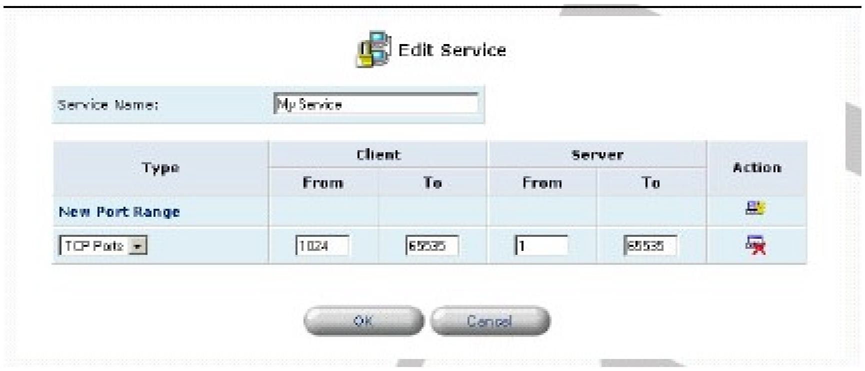
User-Defined Services

Service Name	TCP Ports	UDP Ports	Action
New Entry			
My Service	1-65535		

Figure 40: User-Defined Services

- **To add a new service to the list:**

1. Click the **New Entry** button in the *User-Defined Services* screen (see figure 40). The *Edit Service* screen will appear (see figure 41).



Edit Service

Service Name: My Service

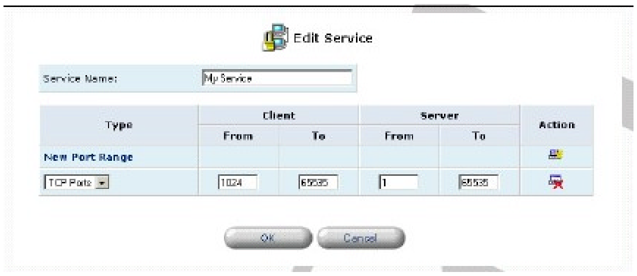
Type	Client		Server		Action
	From	To	From	To	
New Port Range					
TCP Ports	1024	65535	1	65535	

Figure 41: Add or Edit a User-defined Service

2. Enter a name for the service.
3. Choose a port type and enter a port range for this service to use as appropriate. Usually this information is available as part of the documentation that accompanies the program.
4. If necessary, click the **Add port range type** button to enter a port range of another type (UDP or TCP) for the same service.
5. Click the **OK** button to save your changes and return to the *User-Defined Services* screen.

Note: You have now completed defining this service, and may go to the *Add Access Control Rules* or *Add Local Servers* screen to block or activate the service. Refer to P46 and P48 for further instruction.

- To modify a user-defined service already in the list:
  1. Click the **Edit** button for the service in the *User-Defined Services* screen (see figure 40). The *Edit Service* screen will appear (see figure 42).



Edit Service

Service Name: My Service

Type	Client		Server		Action
	From	To	From	To	
New Port Range					
TCP Ports	1024	65535	1	65535	

Figure 42: Add or Edit a User-defined Service

  2. Modify the service name or port information as necessary.
  3. Click the **OK** button to save your changes and return to the *User-Defined Services* screen

- To remove a service from the list:
  1. Click the **Remove** button for the service in the *User-Defined Services* screen (see figure 40). The service will be removed from the list.

Designating a Demilitarzed (DMZ) Host

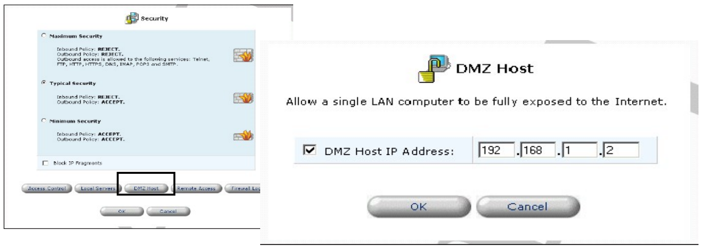
The DMZ Host feature allows one local computer to be exposed to the Internet. Designate a DMZ host when:

- You wish to use a special-purpose Internet service, such as an on-line game or video-conferencing program, that is not present in the Local Servers list and for which no port range information is available.
- You are not concerned with security and wish to expose one computer to all services without restriction

Warning: A DMZ host is not protected by the Firewall and may be vulnerable to attack. Designating a DMZ host may also put other computers in the home network at risk. When designating a DMZ host, you must consider the security implications and protect it if necessary.

An incoming request for access to a service in the home network, such as a Web-server, is fielded by PCX4500. PCX4500 will forward this request to the DMZ host (if one is designated) unless the service is being provided by another PC in the home network (assigned in Local servers), in which case that PC will receive the request instead.

- **To designate a local computer as a DMZ Host:**
  1. Click the **DMZ Host** button in the *Security* screen. The *DMZ Host* screen will appear (see figure 43).



Security

○ Maximum Security

Inbound Policy: **REJECT.**
Outbound Policy: **REJECT.**
Outbound access is allowed to the following services: Telnet, FTP, HTTP, HTTPS, DNS, INAP, POP3 and SMTP.

● Typical Security

Inbound Policy: **REJECT.**
Outbound Policy: **ACCEPT.**

○ Minimum Security

Inbound Policy: **ACCEPT.**
Outbound Policy: **ACCEPT.**

□ Block IP Fragments

DMZ Host

Allow a single LAN computer to be fully exposed to the Internet.

☑ DMZ Host IP Address: 192 . 168 . 1 . 2

Figure 43: DMZ Host

2. Enter the local IP address of the computer that you would like to designate as a DMZ host. Note that only one LAN computer may be a DMZ host at any time.
3. Click the **OK** button to save your changes and return to the *DMZ Host* screen.

You may disable the DMZ host so that it will not be fully exposed to the Internet, but keep its IP address recorded on the *DMZ Host* screen. This may be useful if you wish to disable the DMZ host but expect that you will want to enable it again in the future.

- **To disable the DMZ host so that it will not be fully exposed to the Internet:**

1. Clear the check-box next to the DMZ IP designation. The status of the DMZ host will change to **Disabled**.

- **To enable the DMZ host:**

1. Select the check-box next to the DMZ IP designation.

Controlling Remote Access to PCX4500

It is possible to access and control PCX4500 not only from within the home network, but also from the Internet. This allows you to view or change settings while traveling. It also enables your ISP to change settings or help you troubleshoot functionality or communication issues from a remote location.

Remote access to PCX4500 is blocked by default to ensure the security of your home network. However, remote access is supported by the following services, and you may use the *Remote Access Configuration* screen to selectively enable these services if they are needed.

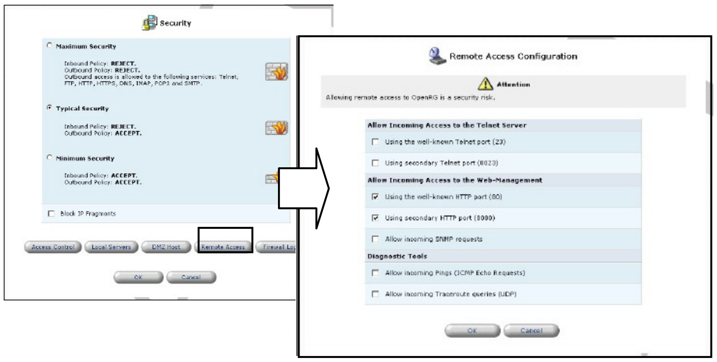
Web-Management/HTTP
Used to obtain access to the Management Console and gain access to all system settings and parameters.

Diagnostic Tools
Used for troubleshooting and remote system management by your Internet Service Provider.

CAUTION: Web-Management may be used to modify settings for or disable the Firewall. The user may also change local IP addresses and other settings making it difficult or impossible to access the gateway from the home network. Therefore, remote access to Telnet or HTTP services on should be blocked and should only be permitted when absolutely necessary.

- To allow remote access to PCX4500 services:

1. Click the **Remote Access** button in the *Security* screen. The *Remote Access Configuration* screen will appear (see figure 44).



Security

○ **Maximum Security**
Inbound Policy: **REJECT.**
Outbound Policy: **REJECT.**
Outbound access is allowed to the following services: Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3 and SMTP.

● **Typical Security**
Inbound Policy: **REJECT.**
Outbound Policy: **ACCEPT.**

○ **Minimum Security**
Inbound Policy: **ACCEPT.**
Outbound Policy: **ACCEPT.**

□ Block IP Fragments

Remote Access Configuration

Attention
Allowing remote access to OpenRG is a security risk.

Allow Incoming Access to the Telnet Server
□ Using the well-known Telnet port (23)
□ Using secondary Telnet port (8023)

Allow Incoming Access to the Web-Management
☑ Using the well-known HTTP port (80)
☑ Using secondary HTTP port (8080)
□ Allow incoming SNMP requests

Diagnostic Tools
□ Allow incoming Pings (ICMP Echo Requests)
□ Allow incoming Traceroute queries (UDP)

Figure 44: Remote Access Configuration

2. Select the services that you would like to make available to computers on the Internet. These services include:

   - Web-based Management - grants access to password-protected web-based management. If a local server is configured to use port 80, select port 8080 to avoid conflicts.

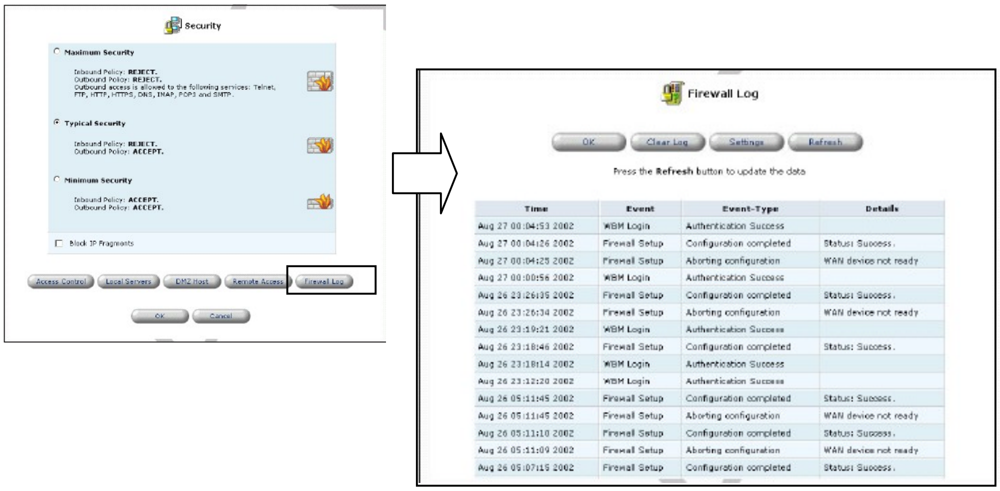
   - Diagnostic tools - includes Ping and Trace route (over UDP). These services may be used for troubleshooting and remote system management by the service provider.

3. Click the **OK** button to save your changes and return to the *Security* screen.

Firewall Log

The Firewall log displays a list of Firewall-related events, including attempts to establish inbound and outbound connections, attempts to authenticate at an administrative interface (Web-based Management), Firewall configuration and system start-up.

To view the Firewall Log, click the **Firewall Log** button in the *Security* screen. The *Firewall Log* screen will appear (see figure 45).



Security

○ **Maximum Security**

Inbound Policy: **REJECT.**
Outbound Policy: **REJECT.**
Outbound access is allowed to the following services: Telnet, FTP, HTTP, HTTPS, DNS, INAP, POP3 and SMTP.

● **Typical Security**

Inbound Policy: **REJECT.**
Outbound Policy: **ACCEPT.**

○ **Minimum Security**

Inbound Policy: **ACCEPT.**
Outbound Policy: **ACCEPT.**

□ Block IP Fragments

Firewall Log

Press the **Refresh** button to update the data

Time	Event	Event-Type	Details
Aug 27 00:04:53 2002	WBM Login	Authentication Success	
Aug 27 00:04:26 2002	Firewall Setup	Configuration completed	Status: Success.
Aug 27 00:04:25 2002	Firewall Setup	Aborting configuration	WAN device not ready
Aug 27 00:00:56 2002	WBM Login	Authentication Success	
Aug 26 23:26:35 2002	Firewall Setup	Configuration completed	Status: Success.
Aug 26 23:26:34 2002	Firewall Setup	Aborting configuration	WAN device not ready
Aug 26 23:19:21 2002	WBM Login	Authentication Success	
Aug 26 23:18:46 2002	Firewall Setup	Configuration completed	Status: Success.
Aug 26 23:18:14 2002	WBM Login	Authentication Success	
Aug 26 23:12:20 2002	WBM Login	Authentication Success	
Aug 26 05:11:45 2002	Firewall Setup	Configuration completed	Status: Success.
Aug 26 05:11:45 2002	Firewall Setup	Aborting configuration	WAN device not ready
Aug 26 05:11:10 2002	Firewall Setup	Configuration completed	Status: Success.
Aug 26 05:11:09 2002	Firewall Setup	Aborting configuration	WAN device not ready
Aug 26 05:07:15 2002	Firewall Setup	Configuration completed	Status: Success.

Figure 45: Firewall Log

The following are the events and event-types that are automatically recorded in the Firewall log:

1. **Inbound/Outbound Traffic**

   - **Connection accepted**: access request complies with the Firewall's security policy.
   - **Accepted - Host probed***: this TCP connection request from a WAN host matches the Firewall's security policy, but the WAN host is not recognized as trusted. The WAN host is being challenged to verify that it is a trusted host.
   - **Accepted - Host trusted***: a reply from a previously challenged WAN host. This client becomes a trusted host.
   - **Accepted - Internal traffic**: all packets are allowed to move freely from one LAN host to another
   - **Blocked - Policy violation**: this access request violates the Firewall's security policy
   - **Blocked - IP Fragment**: if the Firewall is configured to block all IP fragments, this message is recorded for every blocked fragmented packet.

- **Blocked - IP Source-Routes**: this message is recorded whenever a packet is blocked due to a 'Source Route' (either strict or loose) option set in its IP header
- **Blocked - State-table error**: the Firewall encountered an error during State-table lookup or manipulation. Packet was blocked.

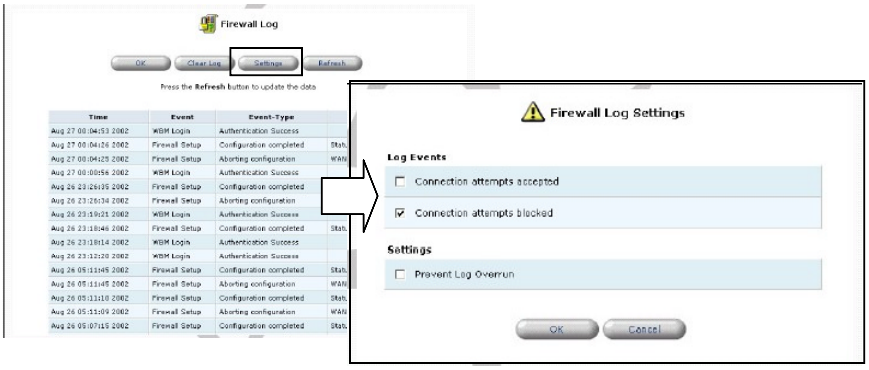
2. **Firewall Setup**
   - Aborting configuration
   - Configuration completed
3. **WBM Login**
   - Authentication Success
   - Authentication Failure
4. **System Up/Down**
   - The system is going DOWN for reboot
   - The system is UP!

*Appears only with regard to inbound traffic.

You can choose additional activities to be recorded in the Firewall log using the *Firewall Log Settings* screen (see figure 46). For each activity type you may choose to view messages associated with successful attempts (Accepted), failed attempts (Blocked) or both.

- To view/change the Firewall Log settings:

1. Click the **Settings** button that appears at the top of the *Firewall Log* screen. The *Firewall Log Settings* screen will appear (see figure 46).



Press the **Refresh** button to update the data

Time	Event	Event-Type	
Aug 27 00:04:53 2002	WBM Login	Authentication Success	
Aug 27 00:04:26 2002	Firewall Setup	Configuration completed	Stat.
Aug 27 00:04:25 2002	Firewall Setup	Aborting configuration	WAN
Aug 27 00:00:56 2002	WBM Login	Authentication Success	
Aug 26 23:26:35 2002	Firewall Setup	Configuration completed	
Aug 26 23:26:34 2002	Firewall Setup	Aborting configuration	
Aug 26 23:19:21 2002	WBM Login	Authentication Success	
Aug 26 23:18:46 2002	Firewall Setup	Configuration completed	Stat.
Aug 26 23:18:14 2002	WBM Login	Authentication Success	
Aug 26 23:12:20 2002	WBM Login	Authentication Success	
Aug 26 05:11:45 2002	Firewall Setup	Configuration completed	Stat.
Aug 26 05:11:45 2002	Firewall Setup	Aborting configuration	WAN
Aug 26 05:11:10 2002	Firewall Setup	Configuration completed	Stat.
Aug 26 05:11:09 2002	Firewall Setup	Aborting configuration	WAN
Aug 26 05:07:15 2002	Firewall Setup	Configuration completed	Stat.

Firewall Log Settings

Log Events

☐ Connection attempts accepted

☑ Connection attempts blocked

Settings

☐ Prevent Log Overrun

Figure 46: Firewall Log Settings

2. Select the types of activities for which you would like to have a log message generated:

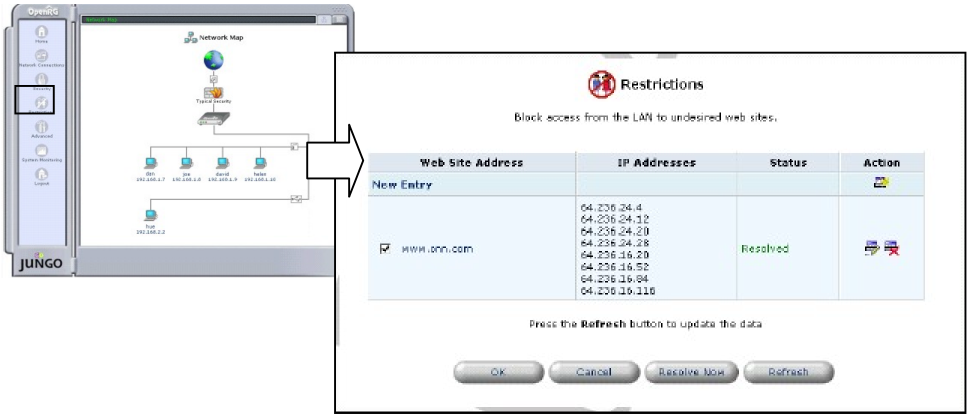
   - Connection Attempts Messages -log a message for each attempt to establish an inbound connection to the home network or vice versa.
   - WBM Connection Attempts Messages -log a message for each attempt to browse to Web-based Management from a browser outside the home network (included in first category).

3. Select the **Prevent Log Overrun** checkbox in order to stop fogging Firewall activities when the memory allocated for the log fills up
4. Click the **OK** button to save your changes and return to the *Firewall Log* screen.

Restriction

You may configure PCX4500 to block specific Internet Web sites so that they cannot be accessed from computers in the home network.
Moreover, restrictions can be applied to a comprehensive automatically updated list of sites to which access is not recommended.

- To view the list of Web sites currently being blocked, click the **Restriction** icon in the left sidebar. The *Restrictions* screen will appear (see figure 47).



Restrictions

Block access from the LAN to undesired web sites.

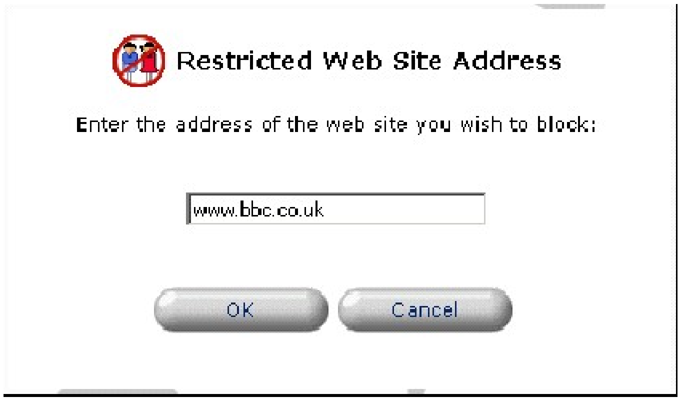
Web Site Address	IP Addresses	Status	Action
New Entry			
☑ www.cnn.com	64.236.24.4 64.236.24.12 64.236.24.20 64.236.24.28 64.236.16.20 64.236.16.52 64.236.16.84 64.236.16.116	Resolved	

Press the **Refresh** button to update the data

Figure 47: Restrictions

- **To add a new Web site to the list:**

1. Click the **New Entry** button in the *Restinctions* screen. The *Restricted Web Site Address* screen will appear (see figure 48).



Restricted Web Site Address

Enter the address of the web site you wish to block:

www.bbc.co.uk

Figure 48: Restricted Web Site Address

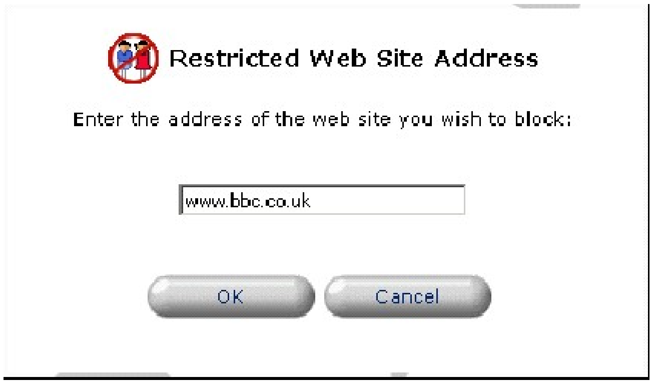
2. Enter the web site address (IP or URL) that you would like to make inaccessible from your home network (all web pages within the site will also be blocked). If the web site address has multiple IP addresses, PCX4500 will resolve all additional addresses and automatically add them to the restrictions list.
3. Click the **OK** button to add this site to the list. You will be returned to the previous screen while PCX4500 attempts to find the site. "Resolving . . . " will appear in the Status column while the site is being located (the URL is being 'resolved' into one or more IP addresses).
4. If the site is successfully located then 'Resolved' will appear in the status bar, otherwise 'Error' will appear. Click the **Refresh** button to update the status if necessary. In case PCX4500 fails to locate the web site, do the following:

- Use a Web browser to verify that the Web site is available. If it is then you probably entered the Web site address incorrectly. Skip to "To modify a Web site address currently in the list" below.

- If the Web site is not available then return to the *Restrictions List* at a later time and click the **Resolve Now** button to verify that the Web site can be found and blocked by PCX4500.

- **To modify a Web site address currently in the list:**

  1. Click the **Edit** button in the *Restrictions* screen. The *Restrictions Web Site Address* screen will appear (see figure 49).



Restricted Web Site Address

Enter the address of the web site you wish to block:

www.bbc.co.uk

Figure 49: Restricted Web Site Address

  2. Modify the Web site address as necessary. If it is long and /or complicated you may want to use your browser's Copy and Paste functions to copy the address from the address bar to the management console. Be sure to omit the "http://" at the beginning and the "/" at the end of the address.
  3. Click the **OK** button to save your changes.

- **To ensure that all current IP addresses corresponding to Web sites in the list are blocked:**

  1. Click the **Resolve Now** button in the *Restrictions* screen. PCX4500 will check each of the Web site addresses in the list and ensure that all IP addresses at which this Web site can be found are included in the IP addresses column.

You may disable a restriction and make the Web site available again without removing the site from the *Restrictions List*. This may be useful if you wish to make the Web site available only temporarily and expect that you will want to block it again in the future.

- **To temporarily disable a restriction:**

  1. Clear the check box next to the restricted URL.

- **To reinstate a restriction at a later time:**

  1. Select the check box next to the URL.

- **To remove a restriction:**

  1. Click the **Remove** button. The restriction will be removed from the Restrictions List.