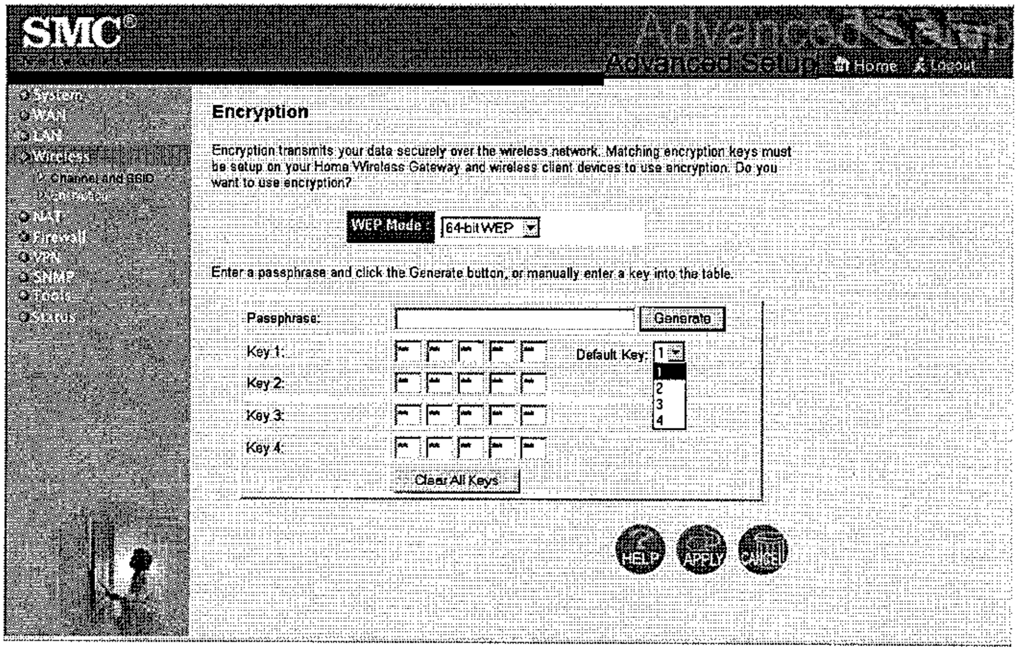
You can automatically generate encryption keys or you can manually enter the keys. For automatic 64-bit security, you enter a passphrase that is used to create four keys (as shown below). The automatic 128-bit security generates a single key by entering a passphrase.



Encryption

Encryption transmits your data securely over the wireless network. Matching encryption keys must be setup on your Home Wireless Gateway and wireless client devices to use encryption. Do you want to use encryption?

WEP Mode : 64-bit WEP

Enter a passphrase and click the Generate button, or manually enter a key into the table.

Passphrase:

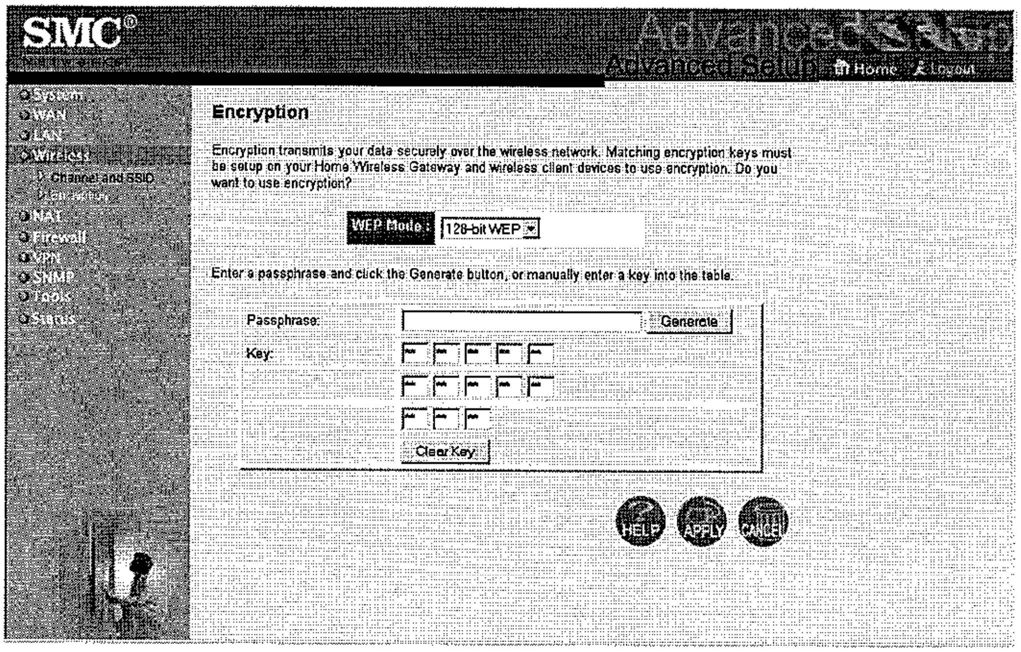
Key 1:

Key 2:

Key 3:

Key 4:

Default Key: 1 (1, 2, 3, 4)



Encryption

Encryption transmits your data securely over the wireless network. Matching encryption keys must be setup on your Home Wireless Gateway and wireless client devices to use encryption. Do you want to use encryption?

WEP Mode : 128-bit WEP

Enter a passphrase and click the Generate button, or manually enter a key into the table.

Passphrase:

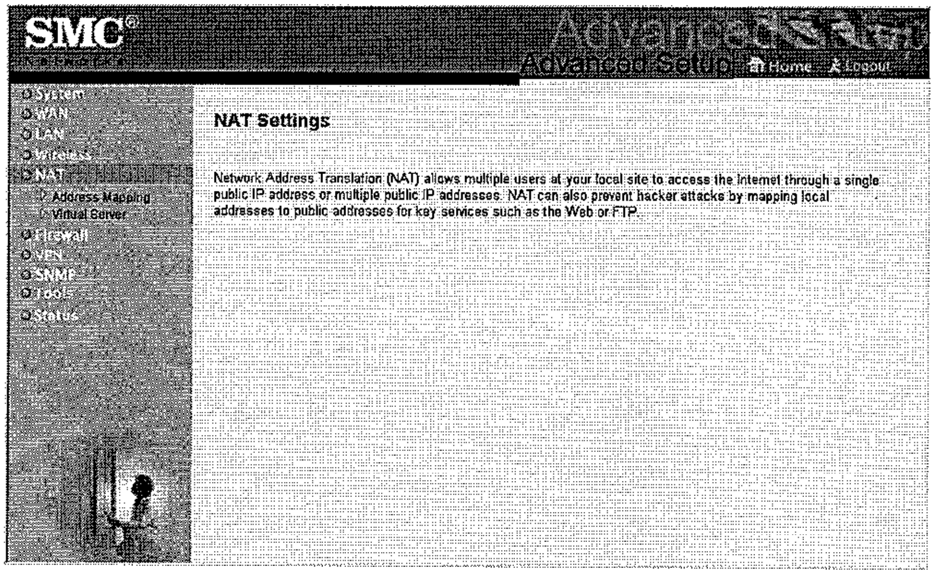
Key:

If you use encryption, configure the same keys used for the Barricade Plus on each of your wireless clients. Note that the Wired Equivalent Privacy (WEP) protects data transmitted between wireless nodes, but does not protect any transmissions over your wired network or over the Internet.

Configuring Client Services

The Barricade Plus includes a broad range of client services, including firewall protection, one VPN tunnel, network address translation, virtual server, address mapping, DMZ, and restricted Internet access for specified clients. You can configure these functions by selecting specific items from the menu on the left of the screen.

NAT - Network Address Translation

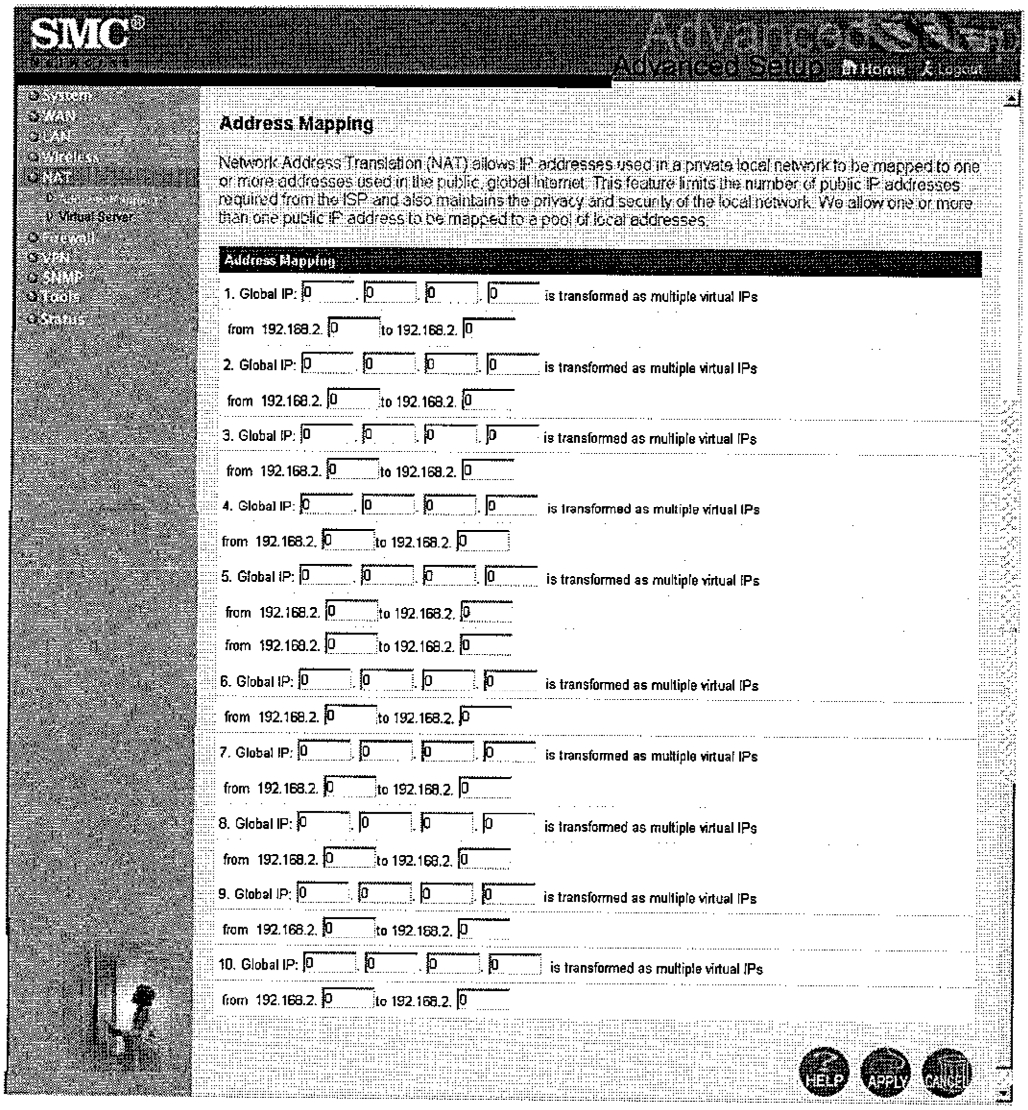


NAT Settings

Network Address Translation (NAT) allows multiple users at your local site to access the Internet through a single public IP address or multiple public IP addresses. NAT can also prevent hacker attacks by mapping local addresses to public addresses for key services such as the Web or FTP.

Network Address Translation (NAT) provides multiple Internet connections using single IP address. If you need multiple connections, use the following screen to specify the public IP addresses to be opened for your client users. NAT can also prevent hacker attacks by mapping local addresses to public addresses for key services such as the Web or FTP.

Address Mapping



Address Mapping

Network Address Translation (NAT) allows IP addresses used in a private local network to be mapped to one or more addresses used in the public, global Internet. This feature limits the number of public IP addresses required from the ISP and also maintains the privacy and security of the local network. We allow one or more than one public IP address to be mapped to a pool of local addresses.

Address Mapping

1. Global IP: 0 . 0 . 0 . 0 is transformed as multiple virtual IPs

from 192.168.2. 0 to 192.168.2. 0

2. Global IP: 0 . 0 . 0 . 0 is transformed as multiple virtual IPs

from 192.168.2. 0 to 192.168.2. 0

3. Global IP: 0 . 0 . 0 . 0 is transformed as multiple virtual IPs

from 192.168.2. 0 to 192.168.2. 0

4. Global IP: 0 . 0 . 0 . 0 is transformed as multiple virtual IPs

from 192.168.2. 0 to 192.168.2. 0

5. Global IP: 0 . 0 . 0 . 0 is transformed as multiple virtual IPs

from 192.168.2. 0 to 192.168.2. 0

from 192.168.2. 0 to 192.168.2. 0

6. Global IP: 0 . 0 . 0 . 0 is transformed as multiple virtual IPs

from 192.168.2. 0 to 192.168.2. 0

7. Global IP: 0 . 0 . 0 . 0 is transformed as multiple virtual IPs

from 192.168.2. 0 to 192.168.2. 0

8. Global IP: 0 . 0 . 0 . 0 is transformed as multiple virtual IPs

from 192.168.2. 0 to 192.168.2. 0

9. Global IP: 0 . 0 . 0 . 0 is transformed as multiple virtual IPs

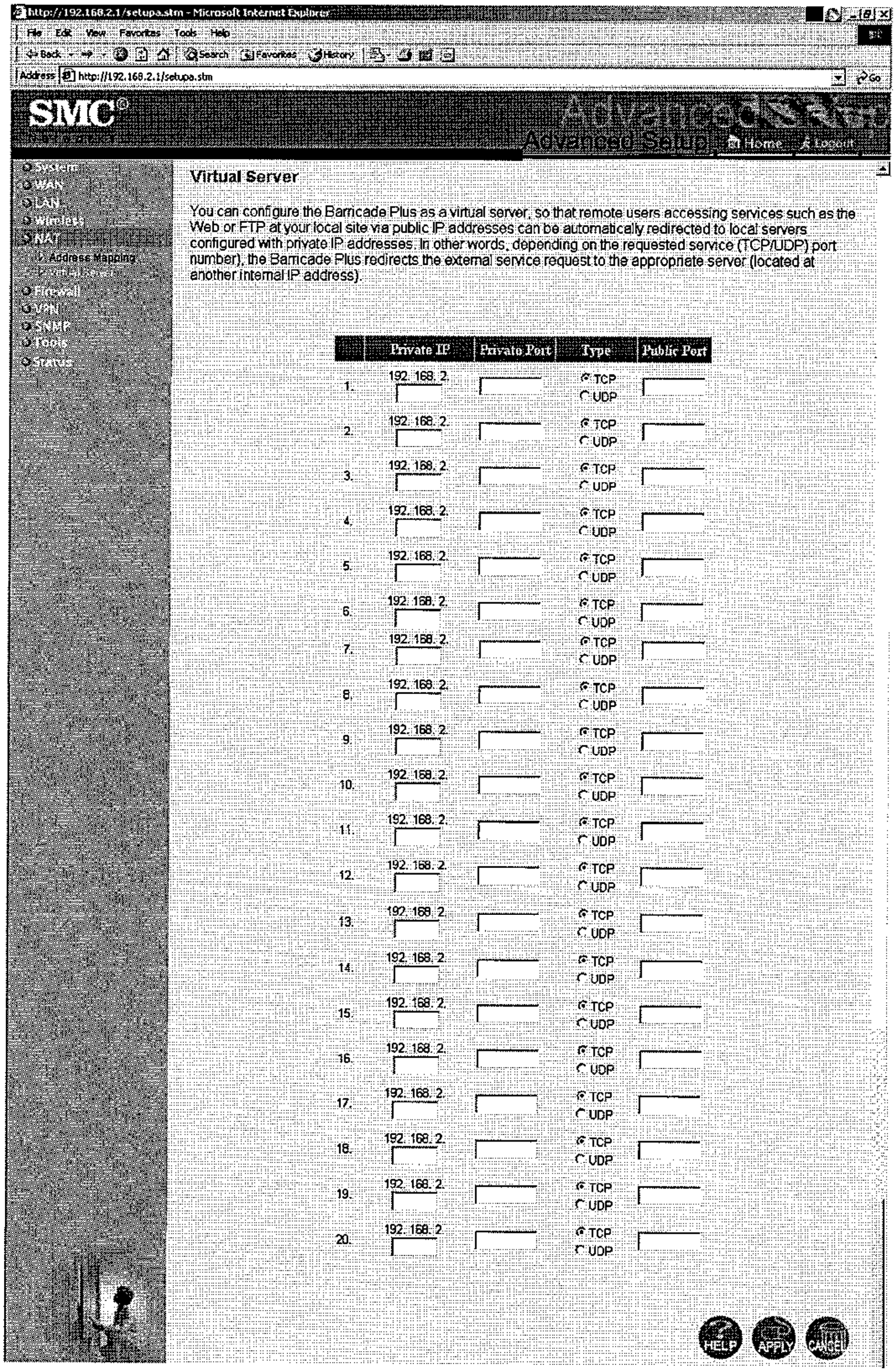
from 192.168.2. 0 to 192.168.2. 0

10. Global IP: 0 . 0 . 0 . 0 is transformed as multiple virtual IPs

from 192.168.2. 0 to 192.168.2. 0

Use the “Address Mapping” option to limit the number of public IP addresses required from the ISP and maintain the privacy and security of the local network.

Virtual Server


http://192.168.2.1/setupa.stm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.2.1/setupa.stm
Go
SMC®
Advanced Setup
Home
Logout
System
WAN
LAN
Wireless
NAT
Address Mapping
Virtual Server
Firewall
VPN
SNMP
Tools
Status
HELP
APPLY
CANCEL

Virtual Server

You can configure the Barricade Plus as a virtual server, so that remote users accessing services such as the Web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP addresses. In other words, depending on the requested service (TCP/UDP) port number), the Barricade Plus redirects the external service request to the appropriate server (located at another internal IP address).

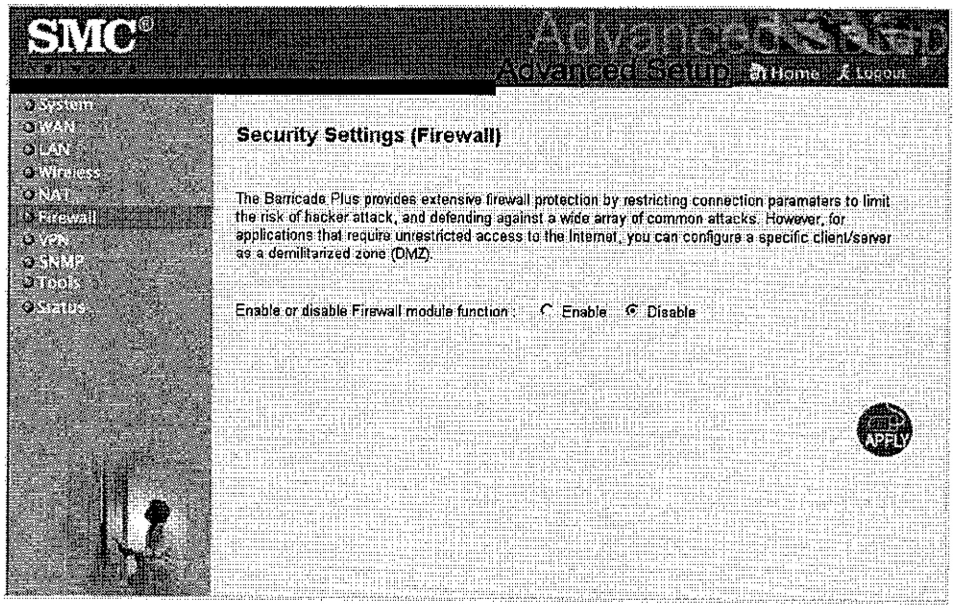
	Private IP	Private Port	Type	Public Port
1.	192. 168. 2.		● TCP ○ UDP	
2.	192. 168. 2.		● TCP ○ UDP	
3.	192. 168. 2.		● TCP ○ UDP	
4.	192. 168. 2.		● TCP ○ UDP	
5.	192. 168. 2.		● TCP ○ UDP	
6.	192. 168. 2.		● TCP ○ UDP	
7.	192. 168. 2.		● TCP ○ UDP	
8.	192. 168. 2.		● TCP ○ UDP	
9.	192. 168. 2.		● TCP ○ UDP	
10.	192. 168. 2.		● TCP ○ UDP	
11.	192. 168. 2.		● TCP ○ UDP	
12.	192. 168. 2.		● TCP ○ UDP	
13.	192. 168. 2.		● TCP ○ UDP	
14.	192. 168. 2.		● TCP ○ UDP	
15.	192. 168. 2.		● TCP ○ UDP	
16.	192. 168. 2.		● TCP ○ UDP	
17.	192. 168. 2.		● TCP ○ UDP	
18.	192. 168. 2.		● TCP ○ UDP	
19.	192. 168. 2.		● TCP ○ UDP	
20.	192. 168. 2.		● TCP ○ UDP	

If you configure the Barricade Plus as a virtual server, remote users accessing services such as Web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP addresses. In other words, depending on the requested service (TCP/UDP port number), the Barricade Plus redirects the external service request to the appropriate server (located at another internal IP address).

The WAN interface must have a fixed IP address to utilize this function. For example, if you set Type/Public Port to TCP/80 (HTTP or Web) and the Private IP/Port to 192.168.2.2/80, then all HTTP request from outside users will be transferred to 192.168.2.2. Therefore, by just entering the IP Address provided by the ISP, Internet users can access the service they need at the local address to which you redirect them.

Some of the more common TCP service ports include:
HTTP: 80, FTP: 21, Telnet: 23 and POP3: 110.

Firewall Protection



Security Settings (Firewall)

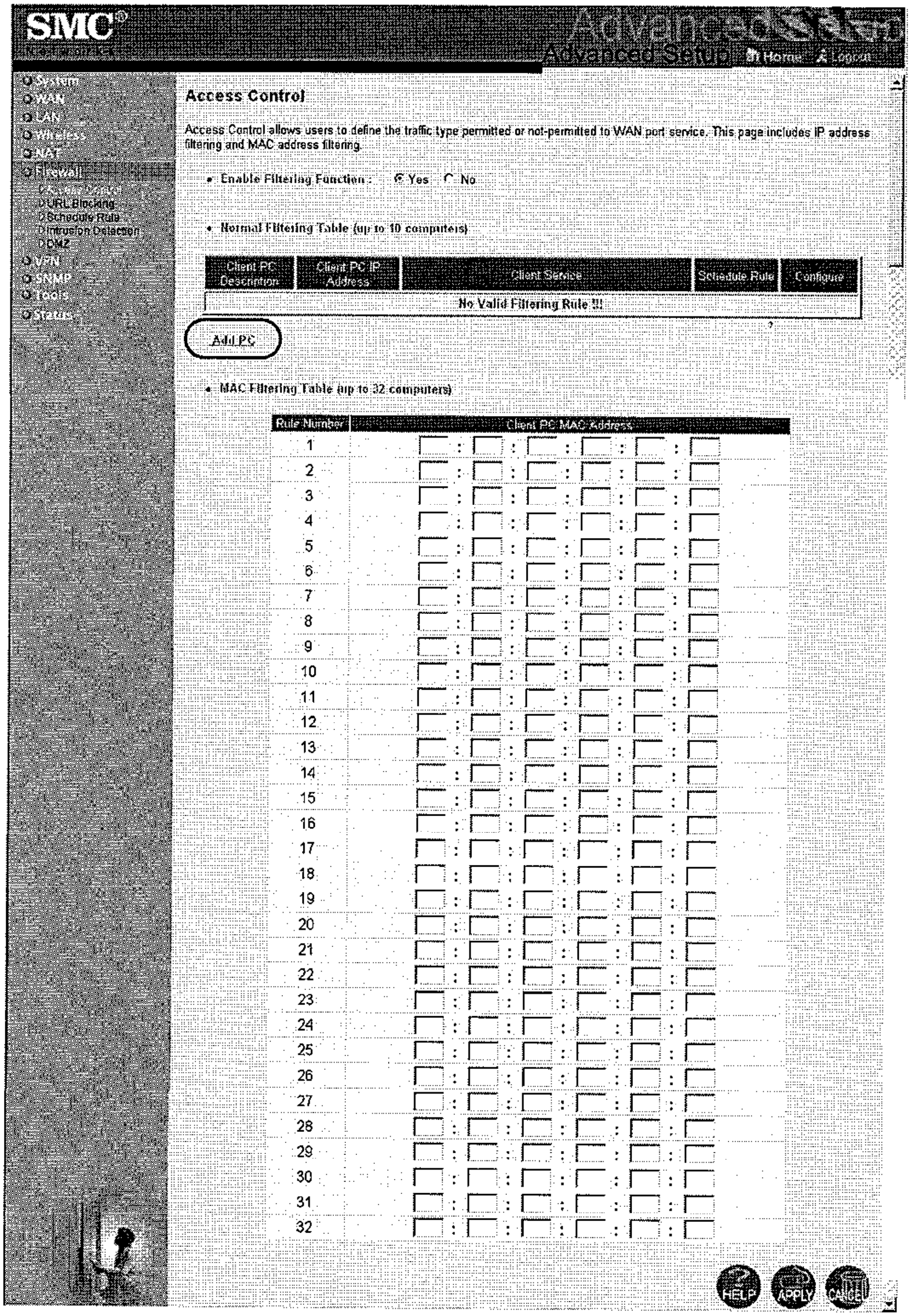
The Barricade Plus provides extensive firewall protection by restricting connection parameters to limit the risk of hacker attack, and defending against a wide array of common attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a demilitarized zone (DMZ).

Enable or disable Firewall module function : ○ Enable ● Disable

The Barricade Plus' firewall can provide the access control of connected client PCs, block common hacker attacks, including IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding. The firewall does not significantly affect system performance, so we advise setting it enabled to protect your network users by selecting "Enable" on the screen.

Note: When you select the "Enable" radio button of the "Enable or disable Firewall module function" field, be sure to press the "APPLY" button.

Access Control



Access Control

Access Control allows users to define the traffic type permitted or not-permitted to WAN port service. This page includes IP address filtering and MAC address filtering.

- Enable Filtering Function : ● Yes ○ No

- Normal Filtering Table (up to 10 computers)

Client PC Description	Client PC IP Address	Client Service	Schedule Rule	Configure
No Valid Filtering Rule !!!				

- MAC Filtering Table (up to 32 computers)

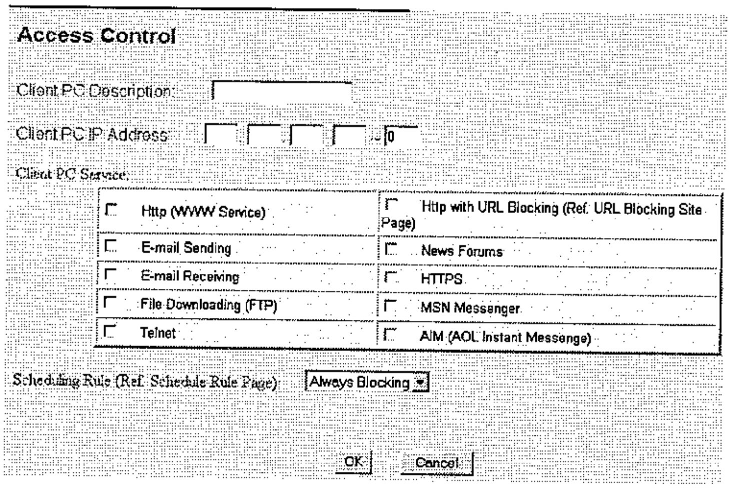
Rule Number	Client PC MAC Address
1	□ : □ : □ : □ : □ : □
2	□ : □ : □ : □ : □ : □
3	□ : □ : □ : □ : □ : □
4	□ : □ : □ : □ : □ : □
5	□ : □ : □ : □ : □ : □
6	□ : □ : □ : □ : □ : □
7	□ : □ : □ : □ : □ : □
8	□ : □ : □ : □ : □ : □
9	□ : □ : □ : □ : □ : □
10	□ : □ : □ : □ : □ : □
11	□ : □ : □ : □ : □ : □
12	□ : □ : □ : □ : □ : □
13	□ : □ : □ : □ : □ : □
14	□ : □ : □ : □ : □ : □
15	□ : □ : □ : □ : □ : □
16	□ : □ : □ : □ : □ : □
17	□ : □ : □ : □ : □ : □
18	□ : □ : □ : □ : □ : □
19	□ : □ : □ : □ : □ : □
20	□ : □ : □ : □ : □ : □
21	□ : □ : □ : □ : □ : □
22	□ : □ : □ : □ : □ : □
23	□ : □ : □ : □ : □ : □
24	□ : □ : □ : □ : □ : □
25	□ : □ : □ : □ : □ : □
26	□ : □ : □ : □ : □ : □
27	□ : □ : □ : □ : □ : □
28	□ : □ : □ : □ : □ : □
29	□ : □ : □ : □ : □ : □
30	□ : □ : □ : □ : □ : □
31	□ : □ : □ : □ : □ : □
32	□ : □ : □ : □ : □ : □

Using this option allows you to specify different privileges for the client PCs.

The following items are included in the "Access Control" screen:

Field	Description
Normal Filtering Table	Displays the IP address and filtering status of the connected client PC
MAC Filtering Table	Displays the MAC address of the client PC

Note: Click on "Add PC" and define the appropriate settings for client PC services (as shown in the following screen).



Access Control

Client PC Description:

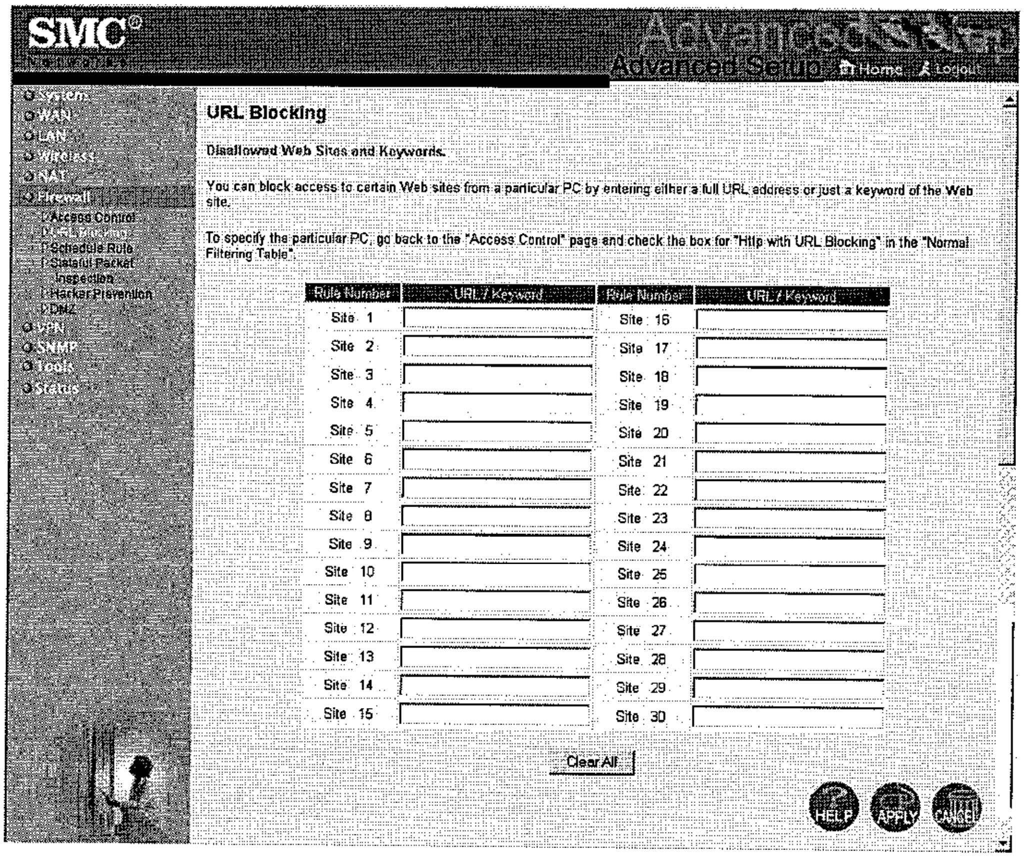
Client PC IP Address: □ . □ . □ . □ ~ 0

Client PC Service:

□ Http (WWW Service)	□ Http with URL Blocking (Ref. URL Blocking Site Page)
□ E-mail Sending	□ News Forums
□ E-mail Receiving	□ HTTPS
□ File Downloading (FTP)	□ MSN Messenger
□ Telnet	□ AIM (AOL Instant Messenge)

Scheduling Rule (Ref. Schedule Rule Page): Always Blocking

URL Blocking



URL Blocking

Disallowed Web Sites and Keywords.

You can block access to certain Web sites from a particular PC by entering either a full URL address or just a keyword of the Web site.

To specify the particular PC, go back to the "Access Control" page and check the box for "Http with URL Blocking" in the "Normal Filtering Table".

Rule Number	URL / Keyword	Rule Number	URL / Keyword
Site 1		Site 16	
Site 2		Site 17	
Site 3		Site 18	
Site 4		Site 19	
Site 5		Site 20	
Site 6		Site 21	
Site 7		Site 22	
Site 8		Site 23	
Site 9		Site 24	
Site 10		Site 25	
Site 11		Site 26	
Site 12		Site 27	
Site 13		Site 28	
Site 14		Site 29	
Site 15		Site 30	

Using the above screen to block access to the Web sites specified in the table.