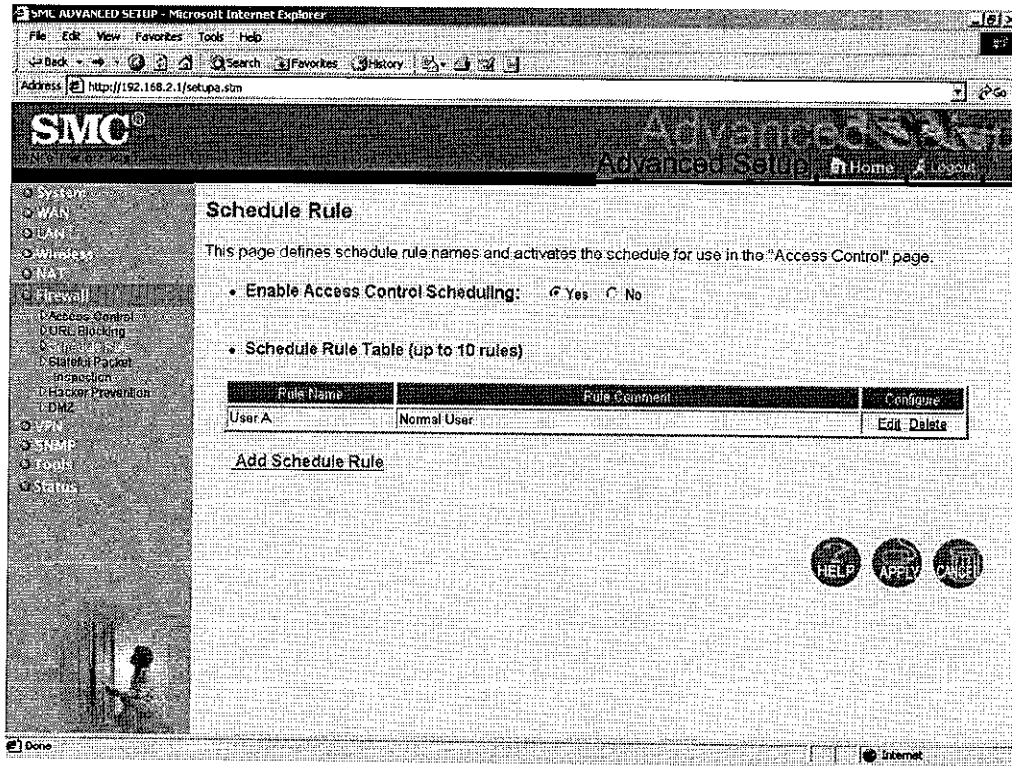


Schedule Rule



You can filter Internet access for local clients based on the “Rule Name,” and time of day.

1. Click on “Add Schedule Rule”

2. Define the appropriate settings for a schedule rule (as shown in the following screen).
3. Click "OK" and then the "APPLY" button to save your settings. (as shown on previous page)

Edit Schedule Rule

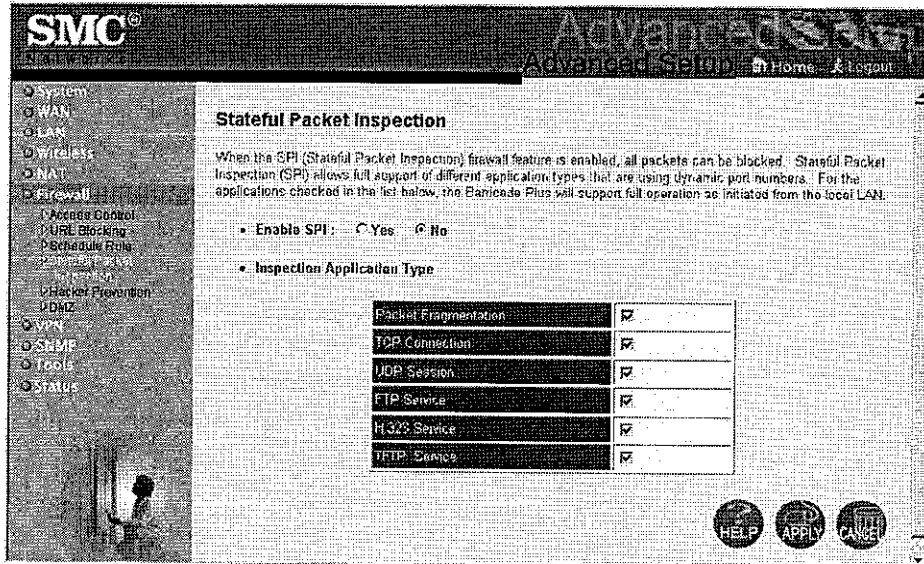
Name:

Comment:

Activate Time Period:

Week Day	Start Time (hh:mm)	End Time (hh:mm)
Every Day	18 : 00	8 : 00
Sunday	:	:
Monday	:	:
Tuesday	:	:
Wednesday	:	:
Thursday	:	:
Friday	:	:
Saturday	:	:

Stateful Packet Inspection



The Stateful Packet Inspection (SPI) feature of the Barricade Plus limits the access of the incoming traffic from the WAN port. When the SPI feature is turned on, all the incoming packets will be blocked unless certain types of traffic types are checked by the users. When the user checks certain types of traffic, only the particular type of traffic initiated from the Internal LAN will be allowed. For example, if the user only checks “FTP service” from the Stateful Packet Inspection page, all the incoming traffic will be blocked except the FTP connection initiated from the local LAN.

This option allows you to select different application types that are using dynamic port numbers. If you need to use the Stateful Packet Inspection (SPI) for blocking packets, click on the “Yes” radio button in the “SPI Enable” field and then check the “Inspection Application Type” that you need, such as Packet Fragmentation, TCP Connection, UDP Session, FTP Service, H.323 Service and TFTP Service.

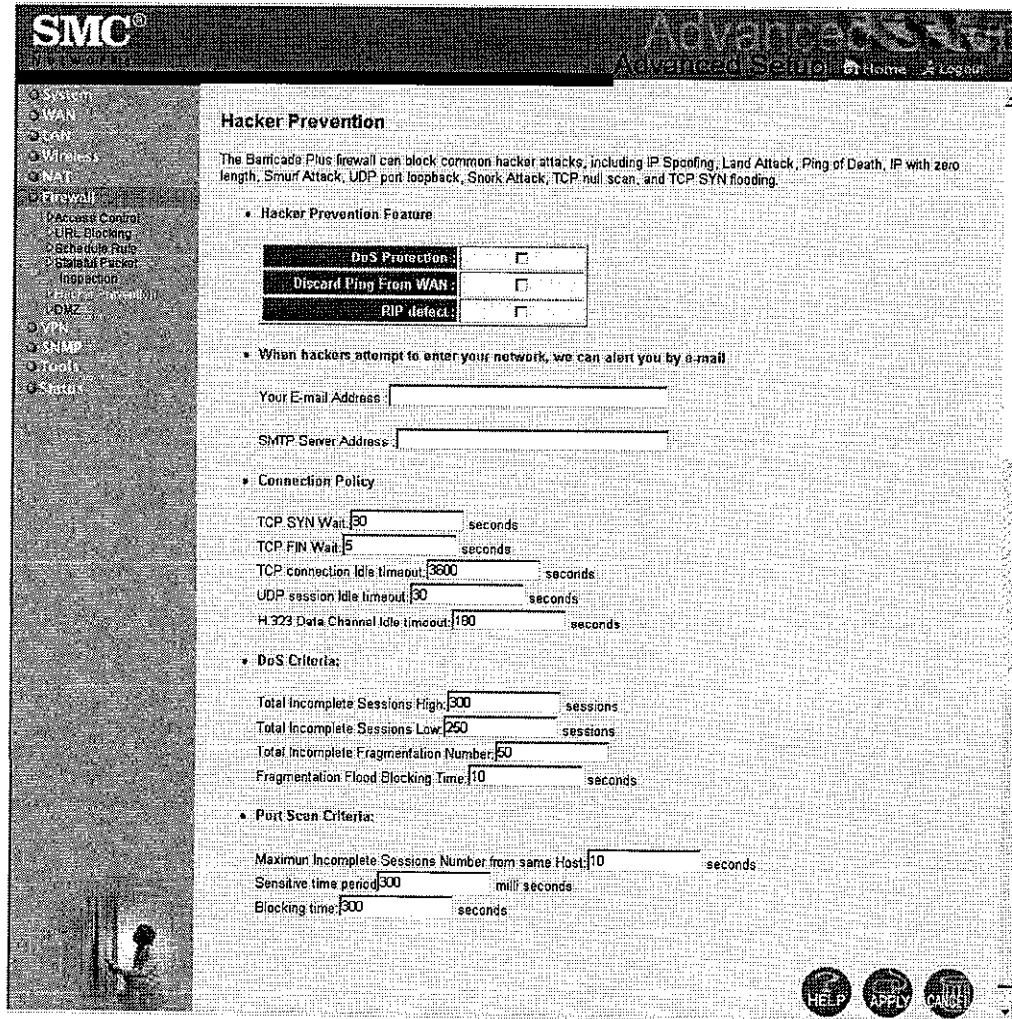
Hacker Prevention

The Barricade Plus' firewall inspects packets at the application layer. It maintains TCP and UDP session information, including timeouts and number of active sessions, and provides the ability to detect and prevent certain types of network attacks such as DoS attacks.

Network attacks that deny access to a network device are called denial-of-service (DoS) attacks. Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resource.

By using the above inspected information and timeout/threshold criteria, the Barricade Plus provides the following DoS attack preventions: Ping of Death (Ping flood) attack, SYN flood attack, IP fragment attack (Teardrop Attack), Brute-force attack, Land Attack, IP Spoofing attack, IP with zero length, TCP null scan (Port Scan Attack), UDP port loopback, Snork Attack etc..

The firewall does not significantly affect system performance, so we advise enabling the prevention features to protect your network users.



- *Hacker Prevention Feature*

Check the prevention items as required

- *When hackers attempt to enter your network, we can alert you by e-mail*

Enter your E-mail address for alerting hacker access

Specify your E-mail server.

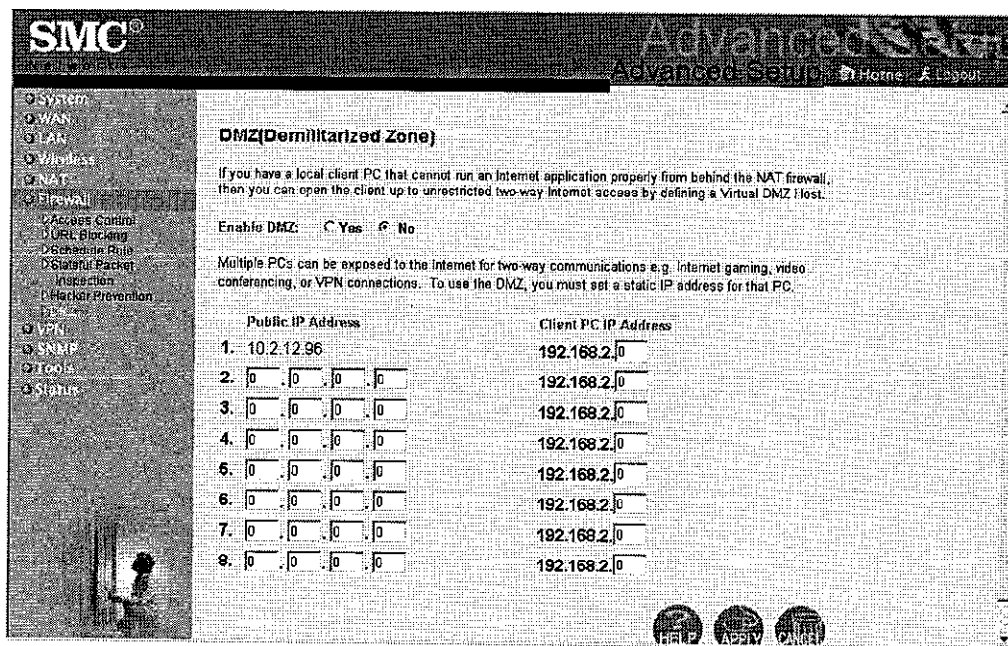
- *Connection Policy*

Enter the appropriate values for TCP/UDP sessions

- *DoS Criteria and Port Scan Criteria*

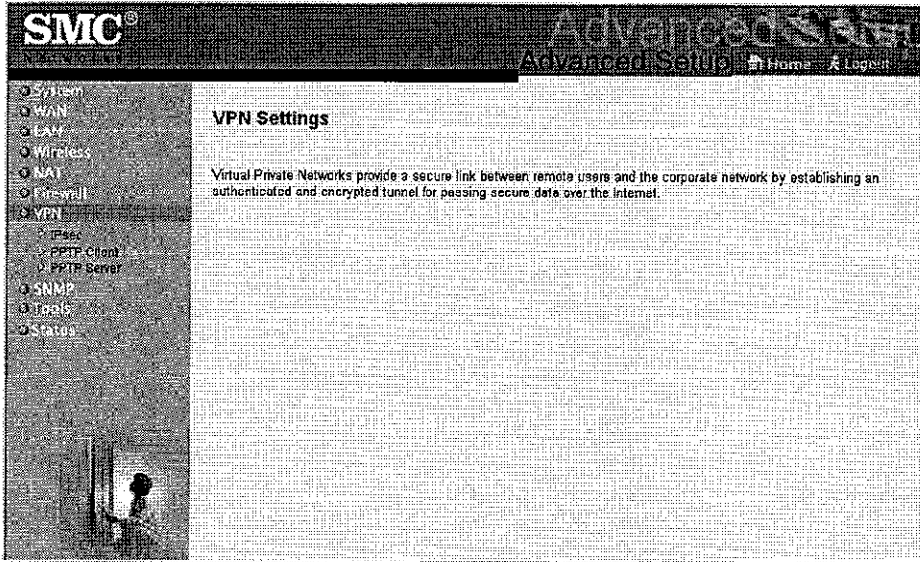
Setup DoS and port scan criteria in the spaces provided.

DMZ (Demilitarized Zone)



If you have a client PC that cannot run an Internet application properly from behind the firewall, then you can open the client up to unrestricted two-way Internet access. Enter the IP address of a DMZ host to this screen. Adding a client to the DMZ (Demilitarized Zone) may expose your local network to a variety of security risks, so only use this option as a last resort.

Virtual Private Networks (VPN) Tunnel



VPN provides a flexible and secure network to the authenticated users through IPsec (IP Security) and PPTP (Point-to-Point Tunneling Protocol) sessions.

IPsec

IPsec is a set of protocols that offers advanced security services in the extranet VPNs.

You have to define the authentication algorithms of the Security Association (SA) by entering appropriate values in the “Inbound SA” and “Outbound SA” fields for using IPsec security control.

SMC
Advanced Setup | Home | Logout

IPsec

IPsec allows users to define a single secure IPsec tunnel with a remote end point. This page includes the setting for both ends of the secure tunnel and the inbound/outbound Security Association (SA).

Enable IPsec: No Yes

Inbound SA:

SPI: 512

Local IP Address: 192.168.1.118
Subnet Mask: 255.255.255.255

Remote IP Address: 192.168.1.119
Subnet Mask: 255.255.255.255

Security Gateway: 192.168.1.119

Hash Algorithm: None MD5 SHA1
Key: 123456789abcde02468ace013579bc

Encrypt Algorithm: None 3DES_CBC DES_CBC
Key: 0123456789abcde02468ace13579bc

Outbound SA:

SPI: 512

Local IP Address: 192.168.1.118
Subnet Mask: 255.255.255.255

Remote IP Address: 192.168.1.119
Subnet Mask: 255.255.255.255

Security Gateway: 192.168.1.119

Hash Algorithm: None MD5 SHA1
Key: 123456789abcde02468ace013579bc

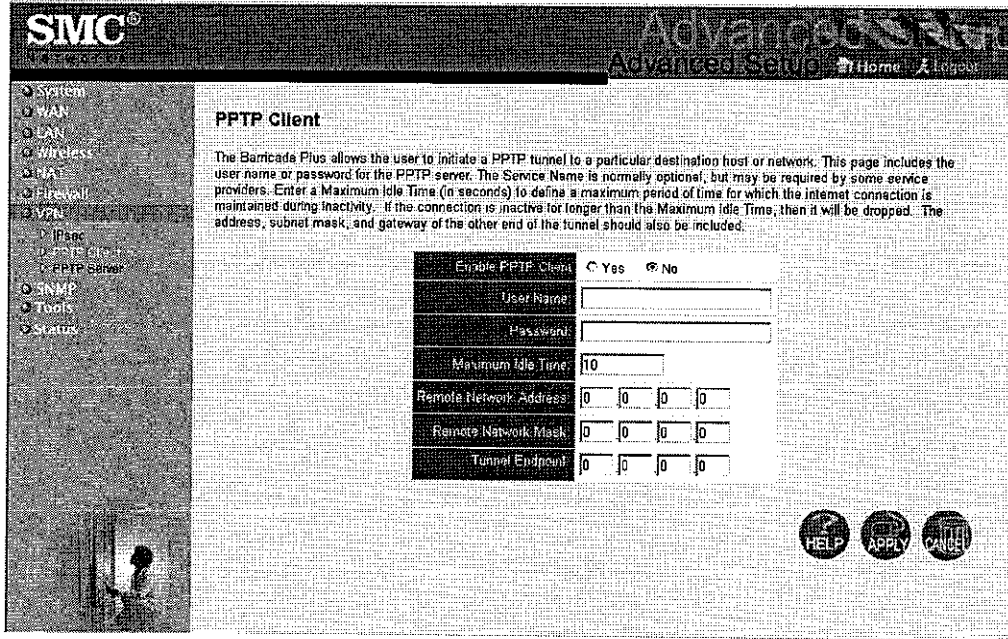
Encrypt Algorithm: None 3DES_CBC DES_CBC
Key: 0123456789abcde02468ace13579bc

Buttons: HELP, APPLY, CANCEL

Done | Internet

PPTP Client

Point-to-Point Tunneling Protocol (PPTP) allows the secure remote access over the Internet by simply dialing in a local point provided by an ISP.



Using the above screen allows client PCs to establish a normal PPTP session and provides hassle-free configuration of the PPTP client on each client PC.

Provide the “Use PPTP Authentication” information to remotely log on the network.

PPTP Server

SMC
Barricade Plus
Advanced Setup Home Logout

- System
- WAN
- LAN
- Wireless
- NAT
- Firewall
- VLAN
- IPsec
- PPTP Client
- PPTP Server**
- SNMP
- Tools
- Status

PPTP Server

The Barricade Plus allows PCs from the Internet to remotely log into the LAN using the PPTP tunneling protocol. This page includes the user name and password for the remote users who are authorized to log into the local LAN and the IP address range to assign to those users.

Authentication			
Index	Username	Password	Re-Enter
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>
11	<input type="text"/>	<input type="text"/>	<input type="text"/>
12	<input type="text"/>	<input type="text"/>	<input type="text"/>
13	<input type="text"/>	<input type="text"/>	<input type="text"/>
14	<input type="text"/>	<input type="text"/>	<input type="text"/>
15	<input type="text"/>	<input type="text"/>	<input type="text"/>
16	<input type="text"/>	<input type="text"/>	<input type="text"/>
17	<input type="text"/>	<input type="text"/>	<input type="text"/>
18	<input type="text"/>	<input type="text"/>	<input type="text"/>
19	<input type="text"/>	<input type="text"/>	<input type="text"/>
20	<input type="text"/>	<input type="text"/>	<input type="text"/>

Address Pool:

Start address:

End address:

HELP APPLY CANCEL

Use the above screen to authorize remote access for assigned IP addresses on the host server.