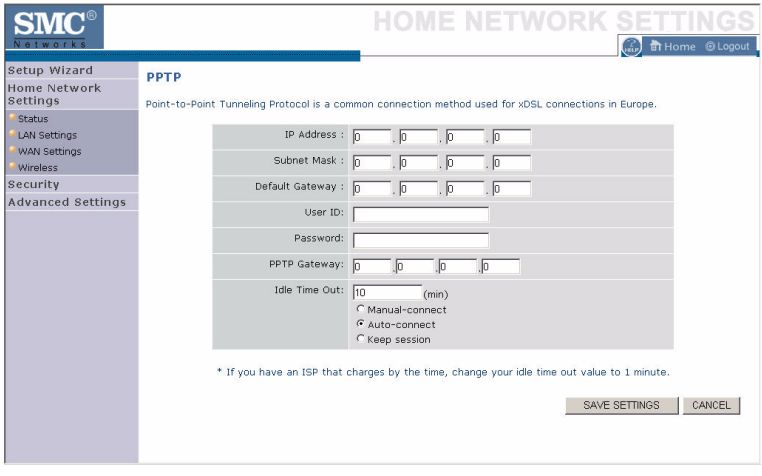
PPTP

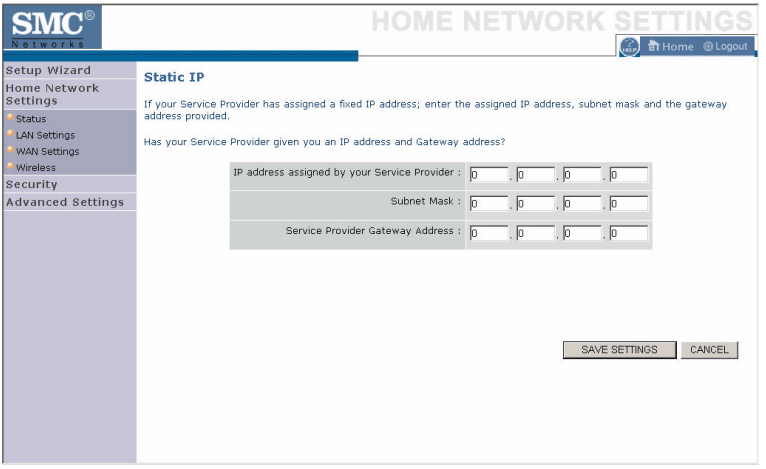
The PPTP screen displays the IP Address, Subnet Mask and Default Gateway of your Barricade. Enter the User ID and Password assigned by your ISP in the appropriate fields. Enter the Idle Time Out for the Internet connection. This is the period of time for which the connection to the Internet is maintained during inactivity. The default setting is 10 minutes. If your ISP charges you by the minute, you should change the Idle Time Out to one minute. After the Idle Time Out has expired, set the action you wish the Barricade to take. You can tell the device to connect manually or automatically as soon as you try to access the Internet again, or to keep the session alive.



Click **Save Settings** to proceed, or **Cancel** to change your settings.

Static IP

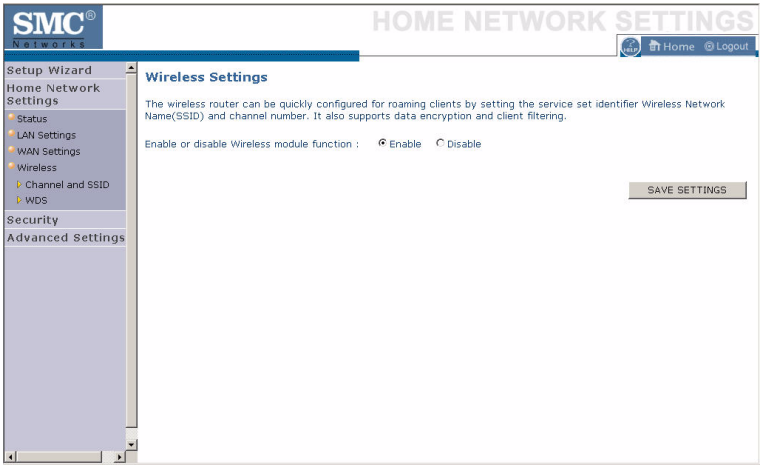
If your Service Provider has assigned a fixed IP address, enter the assigned IP address, subnet mask and the gateway address on this screen.



Click **Save Settings** to proceed, or **Cancel** to change your settings.

Wireless

The Barricade can be quickly configured for roaming clients by setting the Service Set Identifier (SSID) and channel number. It supports data encryption and client filtering.

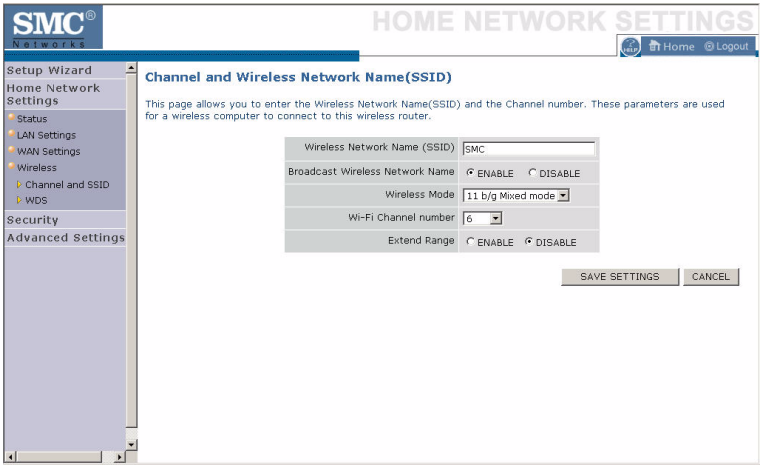


To use the wireless feature, check the **Enable** check box and click **Save Settings**. After clicking **Save Settings**, you will be asked to log in again.

See "Security" on page 4-27 for details on how to configure wireless security.

Channel and SSID

Enter your wireless network settings on this screen. You must specify a common radio channel and SSID (Service Set ID) to be used by the Barricade and all of its wireless clients. Be sure you configure all of its clients to the same value. For security purposes, you should change the default SSID immediately.

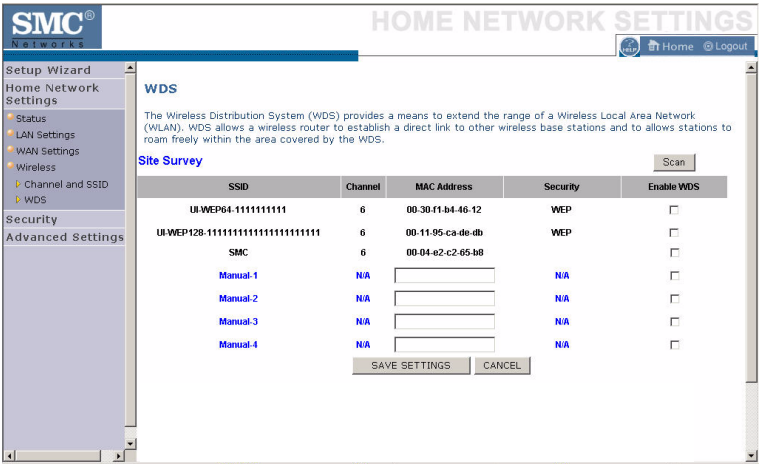


Parameter	Description
Wireless Network Name (SSID)	The Service Set ID (SSID) is the name of your wireless network. The SSID must be the same on the Barricade and all of its wireless clients. (Default: SMC)
Broadcast Wireless Network Name	Enable or disable the broadcasting of the SSID. If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies the wireless network "discovery" feature of some products such as Windows XP. (Default: Enable)
Wireless Mode	This device supports the following modes; 11g only, 11b only, 11b/g mixed mode, Super G-Dynamic Turbo and Super G-Static Turbo. (Default: 11b/g mixed mode)

Parameter	Description
Wi-Fi Channel Number	The radio channel used by the Barricade and its clients to communicate with each other. This channel must be the same on the Barricade and all of its wireless clients. The Barricade will automatically assign itself a radio channel, or you may select one manually. (Default: 6)
Extend Range	Extends the range of the Barricade. (Default: Disable)

WDS

The Wireless Distribution System (WDS) provides a means to extend the range of a Wireless Local Area Network (WLAN). WDS allows the Barricade to establish a direct link to other wireless base stations and allows clients to roam freely within the area covered by the WDS. To carry out a site survey of available wireless base stations, click **Scan**.



Parameter	Description
SSID	The Service Set ID (SSID) is the name of your wireless network. The SSID must be the same on the Barricade and all of its wireless clients.
Channel	This device supports the following modes 11g only, 11b only, and 11b/g mixed mode.
MAC Address	The media access control address (MAC address) is a unique identifier attached to each wireless base station.
Security	Displays the security mechanism in use.
Enable WDS	Enables the WDS feature. When enabled, up to 4 WDS links can be set by specifying their Wireless MAC addresses in the MAC address table. Make sure the same channel is in use on all devices. (Default: Disable)

Security

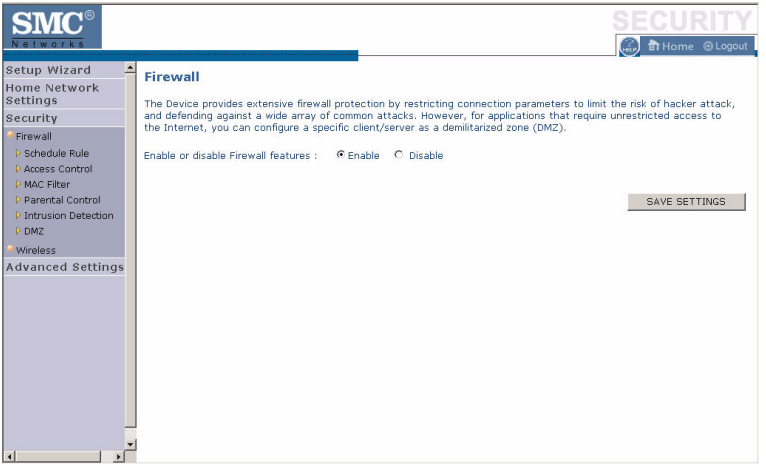
The first menu item in the Security section is Firewall. The Barricade provides a stateful inspection firewall which is designed to protect against Denial of Service (DoS) attacks when activated. Its purpose is to allow a private local area network (LAN) to be securely connected to the Internet.

The second menu item is Wireless. This section allows you to configure wireless security settings according to your environment and the privacy level required.

To configure your firewall settings, click **Firewall** in the left-hand menu.

Firewall

The Barricade's firewall inspects packets at the application layer, maintains TCP and UDP session information including time-outs and the number of active sessions, and provides the ability to detect and prevent certain types of network attacks.



Network attacks that deny access to a network device are called Denial-of-Service (DoS) attacks. 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 resources.

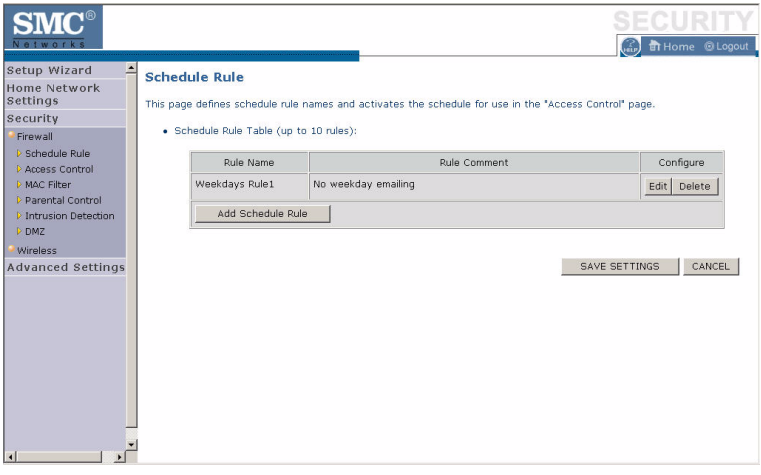
The Barricade protects against the following DoS attacks: IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding. (See "Intrusion Detection" on page 4-35 for details.)

The firewall does not significantly affect system performance, so we advise leaving it enabled to protect your network.

Enable the firewall feature, and click **Save Settings** to proceed.

Schedule Rule

The first item listed in the Firewall section is Schedule Rule. You may filter Internet access for local clients based on rules.



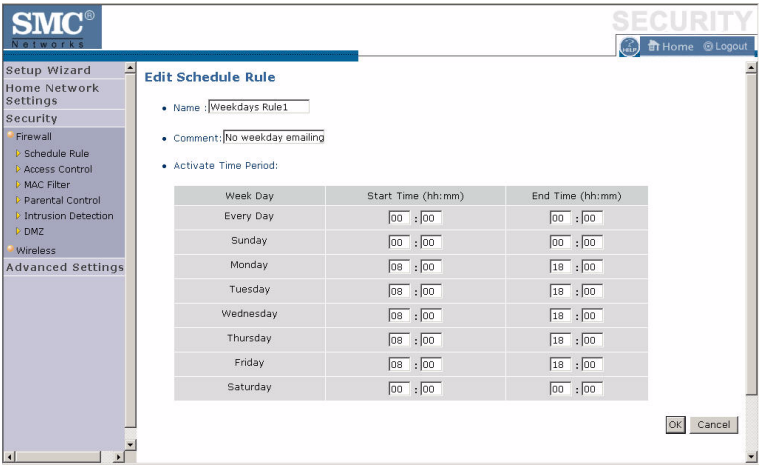
You may filter Internet access for local clients based on rules.

Each access control rule may be activated at a scheduled time. First, define the schedule on the Schedule Rule page, then apply the rule on the Access Control page.

To add a new rule, click **Add Schedule Rule**. Proceed to the following page.

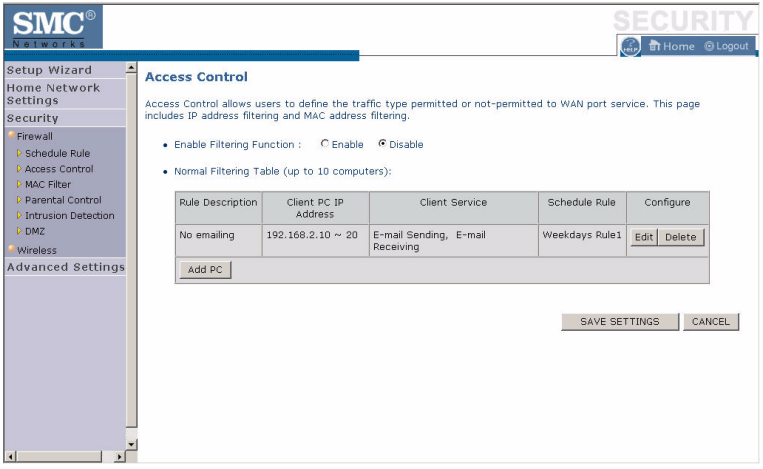
Edit Schedule Rule

1. Define the appropriate settings for a schedule rule (as shown on the following screen).



2. Upon completion, click **OK** to save your schedule rules, and then click **Save Settings** to make your settings to take effect.

Access Control



Used in conjunction with the Schedule Rule screen, the Access Control screen allows users to define the outgoing traffic permitted or not-permitted. The default is to permit all outgoing traffic.

The Barricade can also limit the access of hosts within the local area network (LAN). The MAC Filtering Table allows the Barricade to enter up to 32 MAC addresses that are not allowed access to the WAN port.

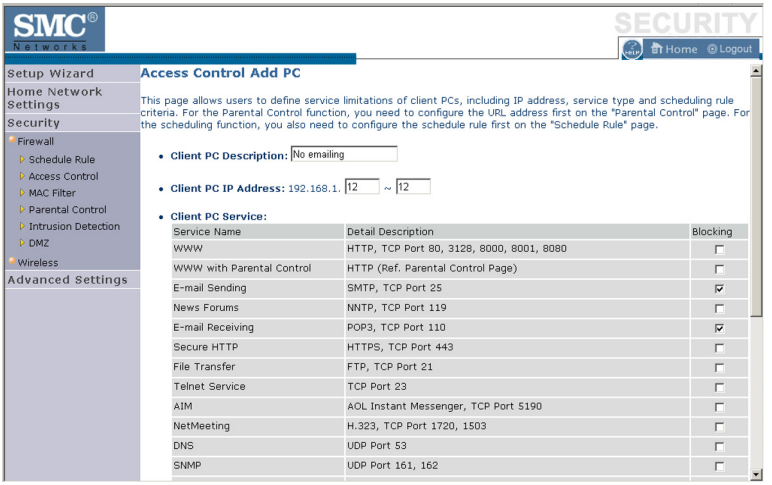
1. Click **Add PC** on the Access Control screen.
2. Define the appropriate settings for client PC services (as shown on the following screen).
3. Click **OK** and then click **Apply** to save your settings.

The following items are displayed on the Access Control screen:

Parameter	Description
Enable Filtering Function	Enables or disables the filtering function.
Normal Filtering Table (up to 10 computers)	Displays the IP address (or an IP address range) filtering table.

Access Control Add PC

Define the access control list in this page. The settings in the screen shot below will block all email sending and receiving during weekdays (except Friday). See "Schedule Rule" on page 4-29.



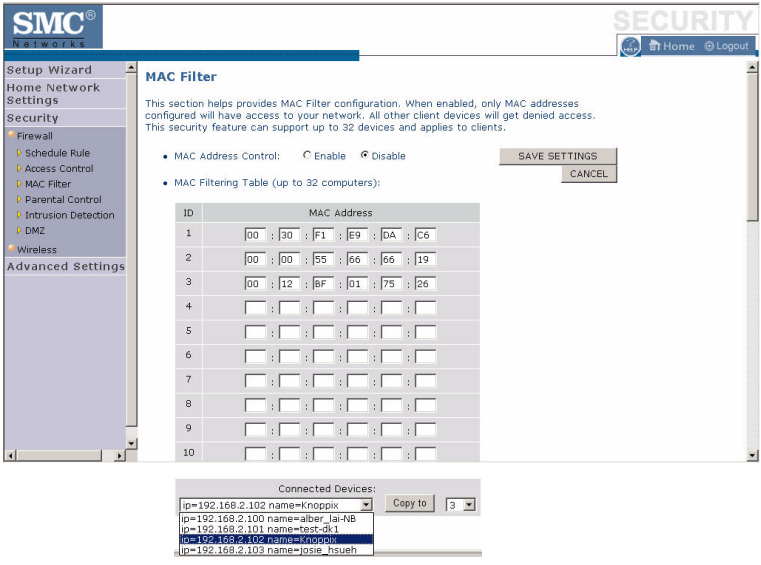
Define the appropriate settings for client PC services (as shown above). At the bottom of this screen, you can set the scheduling function. You can set this function to **Always Blocking** or to whatever schedule you have defined in the Schedule Rule screen. Click **OK** to save your settings. The added PC will now appear in the Access Control page.

For the URL/keyword blocking function, you will need to configure the URL address or blocked keyword on the Parental Control page first. Click **Parental Control** to add to the list of disallowed URL's and keywords.

To enable scheduling, you also need to configure the schedule rule first. Click **Schedule Rule** in the left-hand menu to set the times for which you wish to enforce the rule.

MAC Filter

Use this page to block access to your network using MAC addresses.

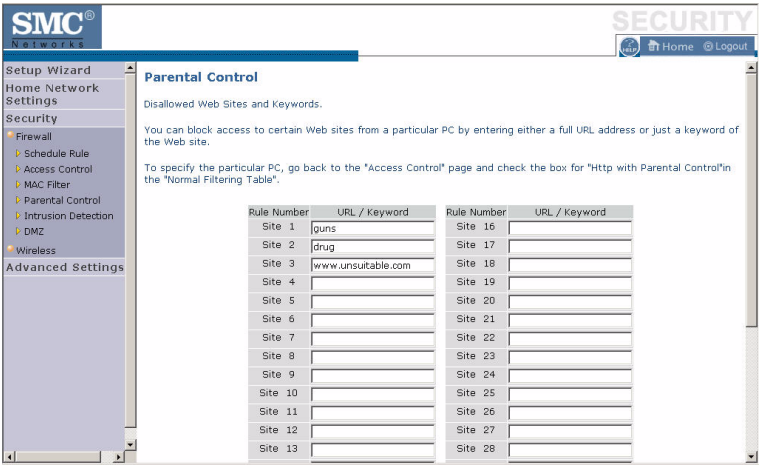


The Barricade can also limit the access of hosts within the local area network (LAN). The MAC Filtering Table allows the Barricade to enter up to 32 MAC addresses that are allowed access to the WAN port. All other devices will be denied access. By default, this feature is disabled.

Click **Save Settings** to proceed, or **Cancel** to change your settings.

Parental Control

The Barricade allows the user to block access to web sites from a particular PC by entering either a full URL address or just a keyword. This feature can be used to protect children from accessing violent or pornographic web sites.



You can define up to 30 sites or keywords here. To configure the Parental Control feature, use the table to specify the web sites (www.somesite.com) and/or keywords you want to block on your network.

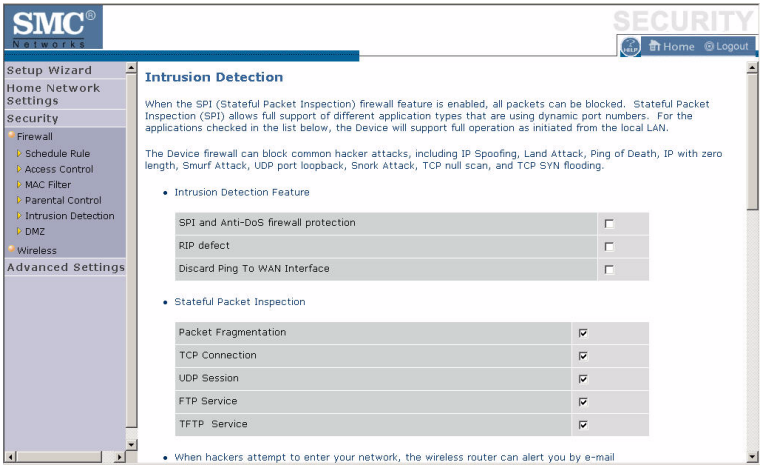
To complete this configuration, you will need to create or modify an access rule in "Access Control Add PC" on page 4-32. To modify an existing rule, click the **Edit** option next to the rule you want to modify. To create a new rule, click on the **Add PC** option.

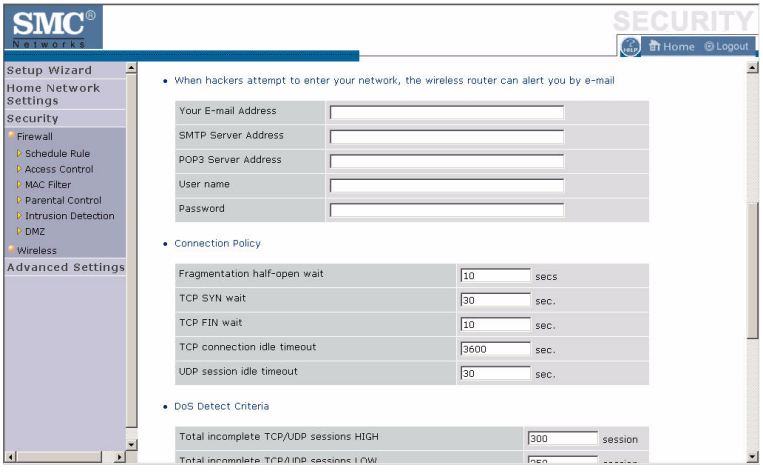
From the Access Control, Add PC section, check the option for **WWW with Parental Control** in the Client PC Service table to filter out the web sites and keywords selected below, on a specific PC.

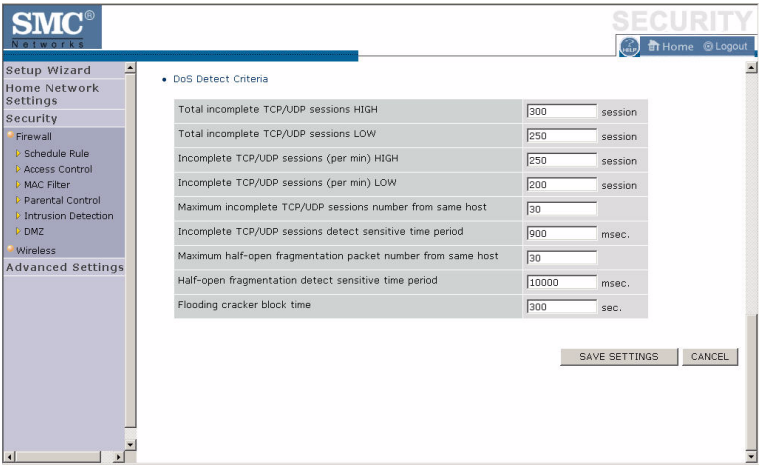
Click **Save Settings** to proceed, or **Cancel** to change your settings.

Intrusion Detection

The Barricade's firewall inspects packets at the application layer, 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 Denial-of-Service (DoS) attacks.







Network attacks that deny access to a network device are called DoS attacks. 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 resources.

The Barricade protects against DoS attacks including: 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.

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

The table below lists the Intrusion Detection parameters and their descriptions.

Parameter	Defaults	Description
Intrusion Detection Feature		
SPI and Anti-DoS firewall protection	No	The Intrusion Detection feature of the Barricade limits the access of incoming traffic at the WAN port. When the Stateful Packet Inspection (SPI) feature is turned on, all incoming packets are blocked except those types marked with a check in the SPI section at the top of the screen.
RIP Defect	Disabled	If the router does not reply to an IPX RIP request packet, it will stay in the input queue and not be released. Accumulated packets could cause the input queue to fill, causing severe problems for all protocols. Enabling this feature prevents the packets accumulating.
Discard Ping to WAN	Don't discard	Prevents a ping on the router's WAN port from being routed to the network.