SBXW-166LHGE-6 /Wireless Broadband Router

Check Point Safe@Office

Internet Security Appliance

User Guide

Version 6.0

Part No: 700797, November 2005

COPYRIGHT & TRADEMARKS

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

PREAMBLE

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started

running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among

countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

To receive the SofaWare GPL licensed code, contact info@sofaware.com.

SAFETY PRECAUTIONS

Carefully read the Safety Instructions the Installation and Operating Procedures provided in this User's Guide before attempting to install or operate the appliance. Failure to follow these instructions may result in damage to equipment and/or personal injuries.

- Before cleaning the appliance, unplug the power cord. Use only a soft cloth dampened with water for cleaning.
- When installing the appliance, ensure that the vents are not blocked.
- Do not place this product on an unstable surface or support. The product may fall, causing serious injury to a child or adult, as well as serious damage to the product.
- Do not use the appliance outdoors.
- Do not expose the appliance to liquid or moisture.
- Do not expose the appliance to extreme high or low temperatures.
- Do not disassemble or open the appliance. Failure to comply will void the warranty.
- Do not use any accessories other than those approved by Check Point. Failure to do so may result in loss of performance, damage to the product, fire, electric shock or injury, and will void the warranty.
- Route power supply cords where they are not likely to be walked on or pinched by items placed on or against them. Pay particular attention to cords where they are attached to plugs and convenience receptacles, and examine the point where they exit the unit.
- Do not connect or disconnect power supply cables and data transmission lines during thunderstorms.
- Do not overload wall outlets or extension cords, as this can result in a risk of fire or electric shock. Overloaded AC outlets, extension cords, frayed power cords, damaged or cracked wire insulation, and broken plugs are dangerous. They may result in a shock or fire hazard. Periodically examine the cord, and if its appearance indicates damage or deteriorated insulation, have it replaced by your service technician.
- If the unit or any part of it is damaged, disconnect the power plug and inform the responsible service personnel. Non-observance may result in damage to the router.

POWER ADAPTER

- Operate this product only from the type of power source indicated on the product’s marking label. If you are not sure of the type of power supplied to your home, consult your dealer or local power company.
- Use only the power supply provided with your product. Check whether the device’s set supply voltage is the same as the local supply voltage.
- To reduce risk of damage to the unit, remove it from the outlet by holding the power adapter rather than the cord.

SECURITY DISCLAIMER

The appliance provides your office network with the highest level of security. However, no single security product can provide you with absolute protection against a determined effort to break into your system. We recommend using additional security measures to secure highly valuable or sensitive information.

Contents

About This Guide

To make finding information in this manual easier, some types of information are marked with special symbols or formatting.

Boldface type is used for command and button names.

Note: Notes are denoted by indented text and preceded by the Note icon.

Warning: Warnings are denoted by indented text and preceded by the Warning icon.

Each task is marked with an icon indicating the Safe@Office product required to perform the task, as follows:

If this icon appears...	You can perform the task using these products...
500	Safe@Office 500 or Safe@Office 500W, with or without the Power Pack
500W	Safe@Office 500W *only*, with or without the Power Pack
Power Pack	Safe@Office 500 or Safe@Office 500W, with the Power Pack *only*

Chapter 1

Introduction

This chapter introduces the Check Point Safe@Office appliance and this guide.

This chapter includes the following topics:

About Your Check Point Safe@Office Appliance

The Check Point Safe@Office 500 appliance is a unified threat management (UTM) appliance that enables secure high-speed Internet access from the office. Developed and supported by SofaWare Technologies, an affiliate of Check Point Software Technologies, the worldwide leader in securing the Internet, the Safe@Office 500 product family includes both wired and wireless models. The Safe@Office firewall, based on the world-leading Check Point Embedded NGX Stateful Inspection technology, inspects and filters all incoming and outgoing traffic, blocking all unauthorized traffic.

The Safe@Office appliance also allows sharing your Internet connection among several PCs or other network devices, enabling advanced office networking and saving the cost of purchasing static IP addresses.

With the Safe@Office appliance, you can subscribe to additional security services available from select service providers, including firewall security and software updates, Antivirus, Web Filtering, reporting, VPN management, and Dynamic DNS. By supporting integrated VPN capabilities, the Safe@Office appliance allows teleworkers and road warriors to securely connect to the office network, and enables secure interconnection of branch offices.

Safe@Office 500 Product Family

The Safe@Office 500 series includes the following hardware models:

- Safe@Office 500 Internet Security Appliance
- Safe@Office 500W Wireless Security Appliance

You can upgrade your Safe@Office appliance to include additional features without replacing the hardware by installing the Safe@Office 500 Power Pack, and you can increase the number of licensed users by installing node upgrades. Contact your reseller for more details.

Safe@Office Features and Compatibility

Connectivity

The Safe@Office 500 series includes the following features:

- LAN ports: 4-ports 10/100 Mbps Fast Ethernet switch
- WAN port: 10/100 Mbps Fast Ethernet
- DMZ/WAN2 Port: 10/100 Mbps Fast Ethernet
- Serial (RS232) port for console access and dialup modem connection
- Supported Internet connection methods: Static IP, DHCP Client, Cable Modem, PPTP Client, PPPoE Client, Telstra BPA login, Dialup
- Concurrent firewall connections: 8,000
- DHCP server, client, and relay
- MAC cloning

- Static NAT
- Static routes and source routes
- Ethernet cable type recognition
- Backup Internet connection
- Dead Internet Connection Detection (DCD)
- Traffic Monitoring
- Traffic Shaping
- VLAN Support (requires Power Pack)
- Dynamic Routing (requires Power Pack)

The Safe@Office 500W includes the following additional features:

- Wireless LAN interface with dual diversity antennas supporting up to 108 Mbps (Super G) and Extended Range (XR)
- Integrated USB print server
- Wireless QoS (WMM)

Firewall

The Safe@Office 500 series includes the following features:

- Check Point Firewall-1 Embedded NGX firewall with Application Intelligence
- Intrusion Detection and Prevention using Check Point SmartDefense
- Network Address Translation (NAT)
- Three preset security policies
- Anti-spoofing
- Voice over IP (H.323) support
- Instant messenger blocking/monitoring

- P2P file sharing blocking/monitoring

VPN

The Safe@Office 500 series includes the following features:

- Remote Access VPN Server with OfficeMode and RADIUS support
- Remote Access VPN Client
- Site to Site VPN Gateway
- IPSEC VPN pass-through
- Algorithms: AES/3DES/DES, SHA1/MD5
- Hardware Based Secure RNG (Random Number Generator)
- IPSec NAT traversal (NAT-T)
- Route-based VPN
- Backup VPN gateways

Management

The Safe@Office 500 series includes the following features:

- Management via HTTP, HTTPS, SSH, SNMP, Serial CLI
- Central Management: SMP
- NTP automatic time setting
- TFTP Rapid Deployment
- Local diagnostics tools: Ping, WHOIS, Packet Sniffer, VPN Tunnel Monitor, Connection Table Monitor, Wireless Monitor, Active Computers Display, Local Logs

Optional Security Services

The following subscription security services are available to Safe@Office owners by connecting to a Service Center:

- Firewall Security and Software Updates
- Web Filtering
- Email Antivirus and Antispam Protection
- VStream Embedded Antivirus Updates
- Dynamic DNS Service
- VPN Management
- Security Reporting
- Vulnerability Scanning Service

Power Pack Features

The table below describes the differences between the standard Safe@Office 500 models and Safe@Office 500 models with the Power Pack installed.

Feature	Safe@Office 500/500W	Safe@Office 500/500W with Power Pack
High Availability	—	✓
Traffic Shaper	Basic	Advanced
DiffServ Tagging	—	✓
Dynamic Routing	—	✓
Firewall/VPN Throughput (Mbps)	100/20	150/30

Feature	Safe@Office 500/500W	Safe@Office 500/500W with Power Pack
Secure Hotspot	—	✓
VLAN (Port/Tag-based)	—	✓
VPN Throughput	20 Mbps	30 Mbps
Site-to-Site VPN	2 tunnels	15 tunnels
Site-to-Site VPN (Managed) *	10 tunnels	100 tunnels
Included VPN-1 SecuRemote client Licenses	5 users	25 users

* When managed by SofaWare Security Management Portal (SMP).

Package Contents

The Safe@Office 500 series package includes the following:

- Safe@Office Internet Security Appliance
- Power adapter
- CAT5 Straight-through Ethernet cable
- Getting Started Guide
- This Users Guide

The Safe@Office 500W also includes:

- Two antennas
- Wall mounting kit, including two plastic conical anchors and two cross-head screws
- USB extension cable

Network Requirements

- A broadband Internet connection via cable or DSL modem with Ethernet interface (RJ-45)
- 10BaseT or 100BaseT Network Interface Card installed on each computer
- TCP/IP network protocol installed on each computer
- Internet Explorer 5.0 or higher, or Netscape Navigator 4.7 and higher
- CAT 5 STP (Category 5 Shielded Twisted Pair) Straight Through Ethernet cable for each attached device

Note: The Safe@Office appliance automatically detects cable types, so you can use either a straight-through or crossed cable, when cascading an additional hub or switch to the Safe@Office appliance.

Note: For optimal results, it is highly recommended to use either Microsoft Internet Explorer 5.5 or higher, or Mozilla Firefox 1.0 or higher.

- When using Safe@Office 500W, an 802.11b, 802.11g or 802.11 Super G wireless card installed on each wireless station

Getting to Know Your Safe@Office 500 Appliance

500

Rear Panel

All physical connections (network and power) to the Safe@Office appliance are made via the rear panel of your Safe@Office appliance.

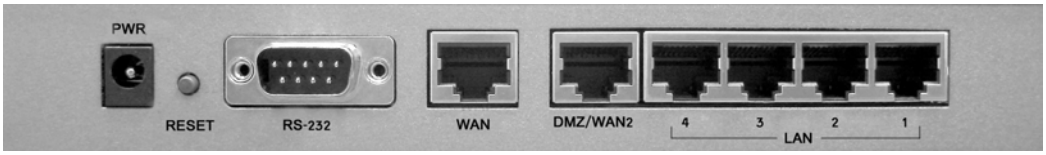


Figure 1: Safe@Office 500 SBX-166LHGE-2 Appliance Rear Panel Items

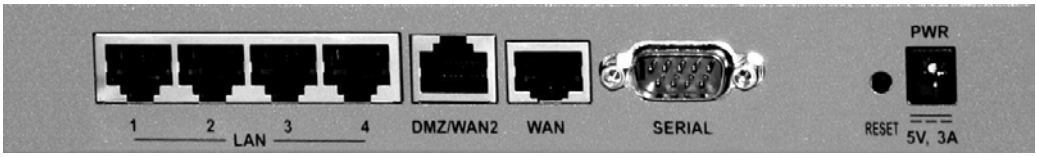


Figure 2: Safe@Office 500 SBX-166LHGE-4 Appliance Rear Panel Items

The following table lists the Safe@Office 500 appliance's rear panel elements.

Table 1: Safe@Office 500 Appliance Rear Panel Elements

Label	Description
PWR	A power jack used for supplying power to the unit. Connect the supplied power adapter to this jack.

Label	Description
RESET	A button used for rebooting the Safe@Office appliance or resetting the Safe@Office appliance to its factory defaults. You need to use a pointed object to press this button. • Short press. Reboots the Safe@Office appliance • Long press (7 seconds). Resets the Safe@Office appliance to its factory defaults, and resets your firmware to the version that shipped with the Safe@Office appliance. This results in the loss of all security services and passwords and reverting to the factory default firmware. You will have to re-configure your Safe@Office appliance. Do not reset the unit without consulting your system administrator.
RS-232 / Serial	A serial port used for connecting computers in order to access the Safe@Office CLI (Command Line Interface), or for connecting an external dialup modem
WAN	Wide Area Network: An Ethernet port (RJ-45) used for connecting your cable or xDSL modem, or for connecting a hub when setting up more than one Internet connection
DMZ/ WAN2	A dedicated Ethernet port (RJ-45) used to connect a DMZ (Demilitarized Zone) computer or network. Alternatively, can serve as a secondary WAN port , or as a VLAN trunk.
LAN 1-4	Local Area Network switch: Four Ethernet ports (RJ-45) used for connecting computers or other network devices

Front Panel

The Safe@Office 500 appliance includes several status LEDs that enable you to monitor the appliance's operation.

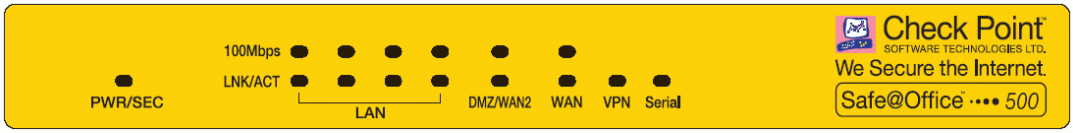


Figure 3: Safe@Office 500 Appliance Front Panel

For an explanation of the Safe@Office 500 appliance's status LEDs, see the table below.

Table 2: Safe@Office 500 Appliance Status LEDs

LED	State	Explanation
PWR/SEC	Off	Power off
	Flashing quickly (Green)	System boot-up
	Flashing slowly (Green)	Establishing Internet connection
	On (Green)	Normal operation
	Flashing (Red)	Hacker attack blocked
	On (Red)	Error
LAN 1-4/ WAN/ DMZ/WAN2	LINK/ACT Off, 100 Off	Link is down
	LINK/ACT On, 100 Off	10 Mbps link established for the corresponding port

LED	State	Explanation
	LINK/ACT On, 100 On	100 Mbps link established for the corresponding port
	LNK/ACT Flashing	Data is being transmitted/received
VPN	Flashing (Green)	VPN port in use
Serial	Flashing (Green)	Serial port in use

Getting to Know Your Safe@Office 500W Appliance

500W

Rear Panel

All physical connections (network and power) to the Safe@Office appliance are made via the rear panel of your Safe@Office appliance.

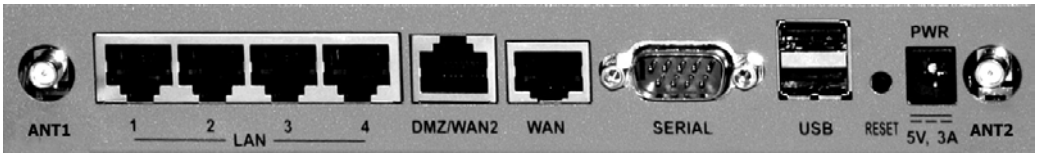


Figure 4: Safe@Office 500W Appliance Rear Panel Items

The following table lists the Safe@Office 500W appliance's rear panel elements.

Table 3: Safe@Office 500W Appliance Rear Panel Elements

Label	Description
PWR	A power jack used for supplying power to the unit. Connect the supplied power adapter to this jack.

Label	Description
RESET	A button used for rebooting the Safe@Office appliance or resetting the Safe@Office appliance to its factory defaults. You need to use a pointed object to press this button. • Short press. Reboots the Safe@Office appliance • Long press (7 seconds). Resets the Safe@Office appliance to its factory defaults, and resets your firmware to the version that shipped with the Safe@Office appliance. This results in the loss of all security services and passwords and reverting to the factory default firmware. You will have to re-configure your Safe@Office appliance. Do not reset the unit without consulting your system administrator.
USB	Two USB 2.0 ports used for connecting USB-based printers
RS232	A serial (RS-232) port used for connecting computers in order to access the Safe@Office CLI (Command Line Interface), or for connecting an external dialup modem
WAN	Wide Area Network: An Ethernet port (RJ-45) used for connecting your cable or xDSL modem, or for connecting a hub when setting up more than one Internet connection
DMZ/ WAN2	A dedicated Ethernet port (RJ-45) used to connect a DMZ (Demilitarized Zone) computer or network. Alternatively, can serve as a secondary WAN port , or as a VLAN trunk.
LAN 1-4	Local Area Network switch: Four Ethernet ports (RJ-45) used for connecting computers or other network devices
ANT 1/ ANT 2	Antenna connectors, used to connect the supplied wireless antennas

Front Panel

The Safe@Office 500W appliance includes several status LEDs that enable you to monitor the appliance's operation.

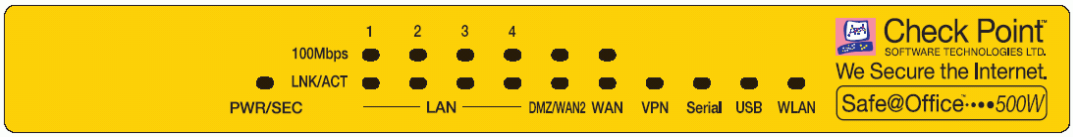


Figure 5: Safe@Office 500W Appliance Front Panel

For an explanation of the Safe@Office 500W appliance's status LEDs, see the table below.

Table 4: Safe@Office 500W Appliance Status LEDs

LED	State	Explanation
PWR/SEC	Off	Power off
	Flashing quickly (Green)	System boot-up
	Flashing slowly (Green)	Establishing Internet connection
	On (Green)	Normal operation
	Flashing (Red)	Hacker attack blocked
	On (Red)	Error
	Flashing (Orange)	Software update in progress
LAN 1-4/ WAN/ DMZ/WAN2	LINK/ACT Off, 100 Off	Link is down
	LINK/ACT On, 100 Off	10 Mbps link established for the corresponding port

LED	State	Explanation
	LINK/ACT On, 100 On	100 Mbps link established for the corresponding port
	LNK/ACT Flashing	Data is being transmitted/received
VPN	Flashing (Green)	VPN port in use
Serial	Flashing (Green)	Serial port in use
USB	Flashing (Green)	USB port in use
WLAN	Flashing (Green)	WLAN in use

Contacting Technical Support

If there is a problem with your Safe@Office appliance, see http://www.sofaware.com/support.

You can also download the latest version of this guide from the site.

Chapter 2

Installing and Setting up the Safe@Office Appliance

This chapter describes how to properly set up and install your Safe@Office appliance in your networking environment.

This chapter includes the following topics:

Before You Install the Safe@Office Appliance

Prior to connecting and setting up your Safe@Office appliance for operation, you must do the following:

- Check if TCP/IP Protocol is installed on your computer.
- Check your computer's TCP/IP settings to make sure it obtains its IP address automatically.

Refer to the relevant section in this guide in accordance with the operating system that runs on your computer. The sections below will guide you through the TCP/IP setup and installation process.

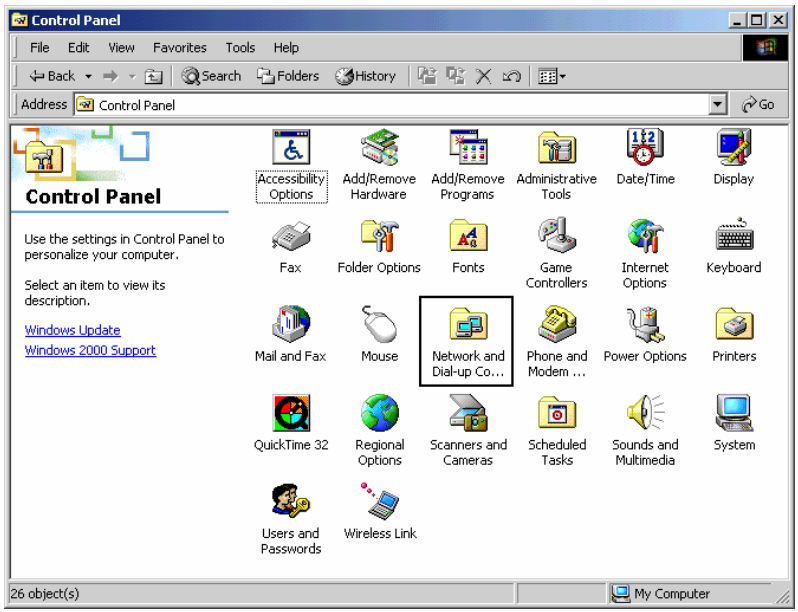
Windows 2000/XP

Note: While Windows XP has an "Internet Connection Firewall" option, it is recommended to disable it if you are using a Safe@Office appliance, since the Safe@Office appliance offers better protection.

Checking the TCP/IP Installation

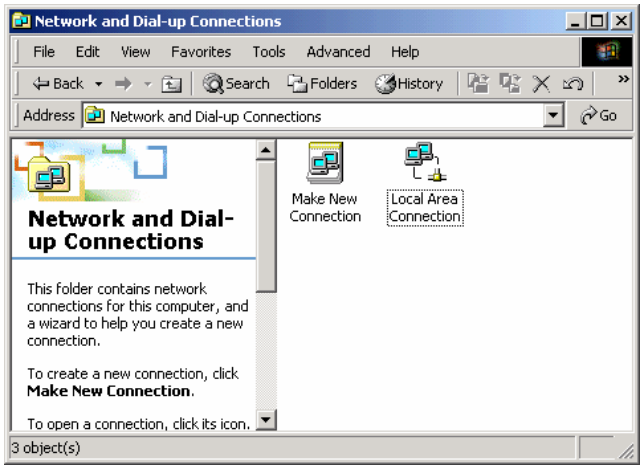
1. Click Start > Settings > Control Panel.

   The Control Panel window appears.



2. Double-click the Network and Dial-up Connections icon.

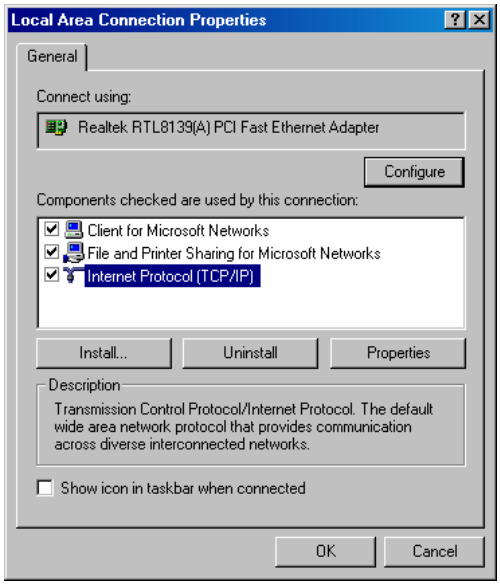
The **Network and Dial-up Connections** window appears.



3. Right-click the 

icon and select **Properties** from the pop-up menu that opens.

The Local Area Connection Properties window appears.

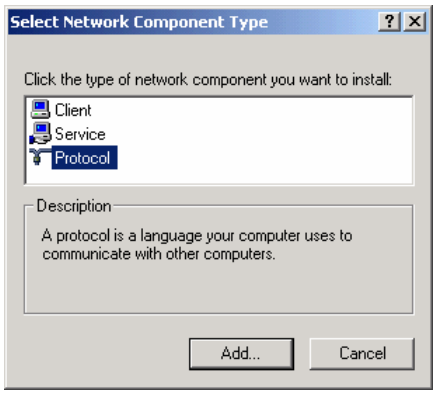


4. In the above window, check if TCP/IP appears in the components list and if it is properly configured with the Ethernet card, installed on your computer. If TCP/IP does not appear in the Components list, you must install it as described in the next section.

Installing TCP/IP Protocol

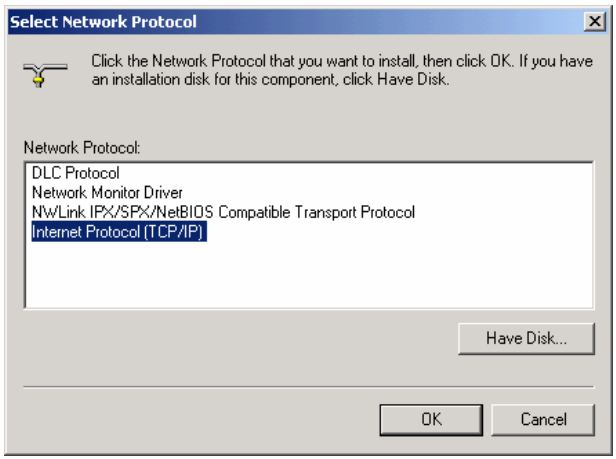
1. In the Local Area Connection Properties window click Install....

   The Select Network Component Type window appears.



2. Choose Protocol and click Add.

   The Select Network Protocol window appears.



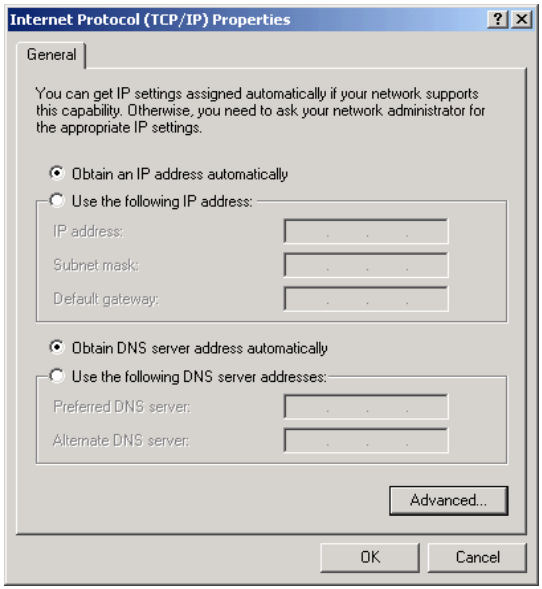
3. Choose Internet Protocol (TCP/IP) and click OK.

   TCP/IP protocol is installed on your computer.

TCP/IP Settings

1. In the Local Area Connection Properties window double-click the Internet Protocol (TCP/IP) component, or select it and click Properties.

   The Internet Protocol (TCP/IP) Properties window opens.



2. Click the Obtain an IP address automatically radio button.

   Note: Normally, it is not recommended to assign a static IP address to your PC but rather to obtain an IP address automatically. If for some reason you need to assign a static IP address, select Specify an IP address, type in an IP address in the range of 192.168.10.129-254, enter 255.255.255.0 in the Subnet Mask field, and click OK to save the new settings.

   (Note that 192.168.10 is the default value, and it may vary if you changed it in the My Network page.)

3. Click the Obtain DNS server address automatically radio button.
4. Click OK to save the new settings.

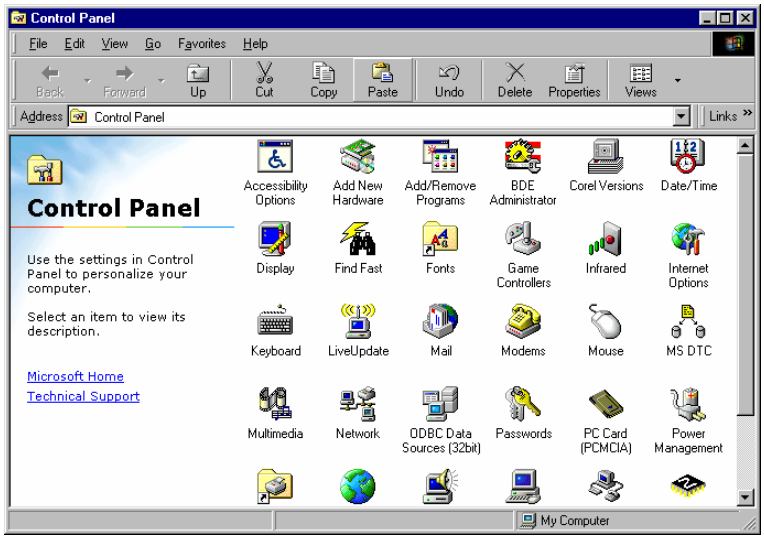
   Your computer is now ready to access your Safe@Office appliance.

Windows 98/Millennium

Checking the TCP/IP Installation

1. Click Start > Settings > Control Panel.

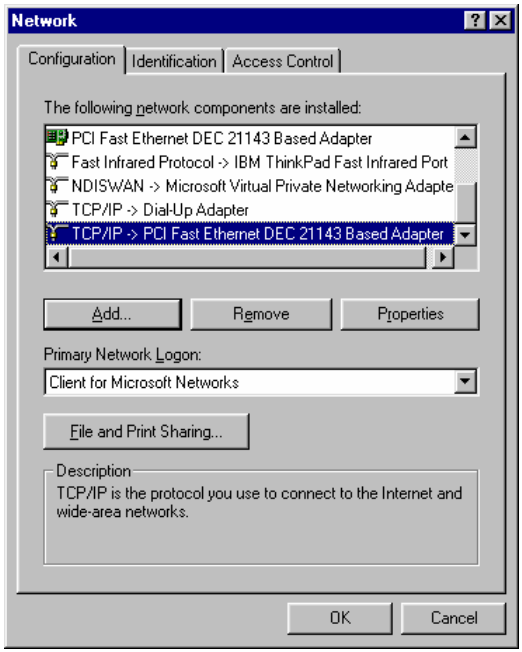
   The Control Panel window appears.



2. Double-click the 

icon.

The Network window appears.



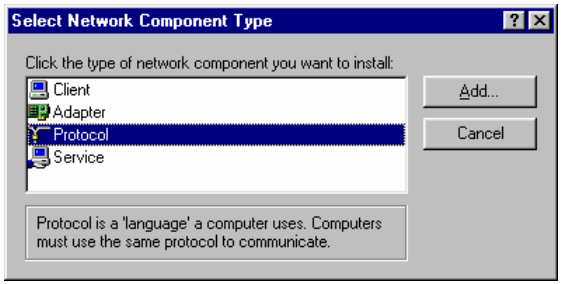
3. In the Network window, check if TCP/IP appears in the network components list and if it is already configured with the Ethernet card, installed on your computer.

Installing TCP/IP Protocol

Note: If TCP/IP is already installed and configured on your computer skip this section and move directly to TCP/IP Settings.

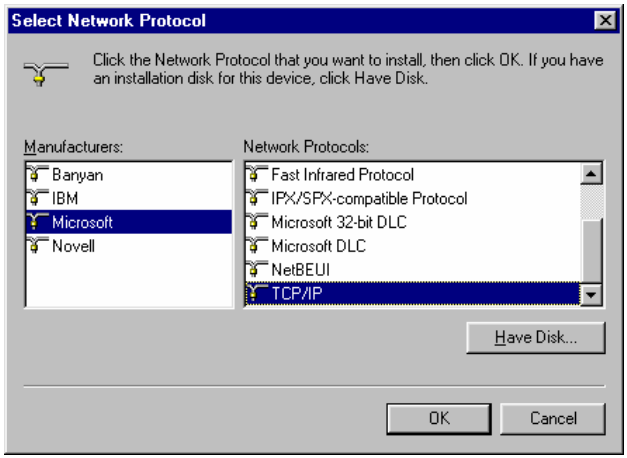
1. In the Network window, click Add.

The Select Network Component Type window appears.



2. Choose Protocol and click Add.

   The Select Network Protocol window appears.



3. In the Manufacturers list choose Microsoft, and in the Network Protocols list choose TCP/IP.
4. Click OK.

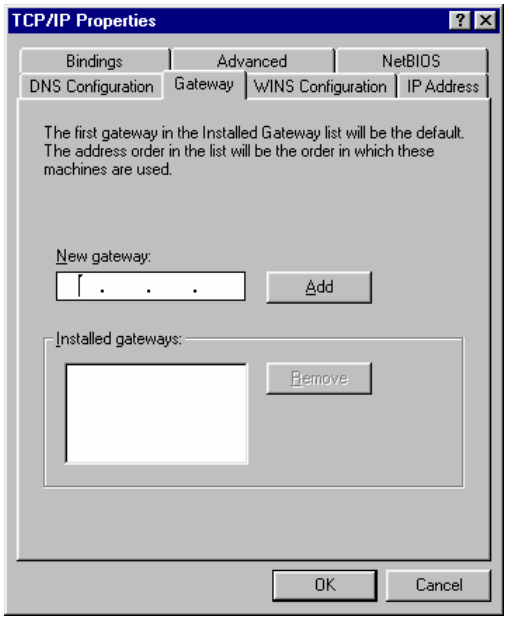
   If Windows asks for original Windows installation files, provide the installation CD and relevant path when required (e.g. D:\win98)

5. Restart your computer if prompted.

TCP/IP Settings

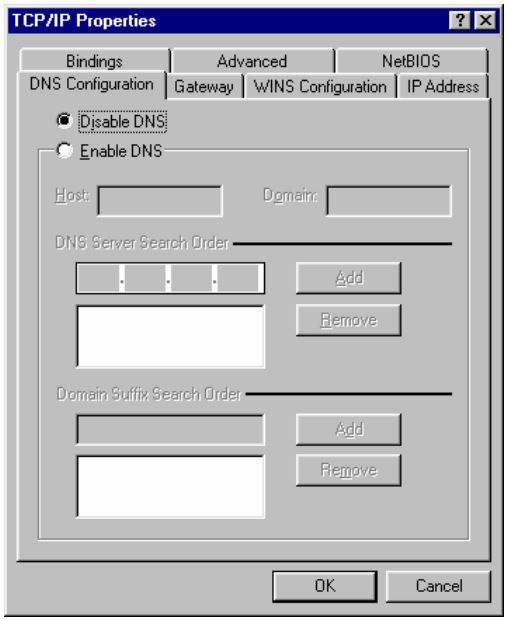
Note: If you are connecting your Safe@Office appliance to an existing LAN, consult your network manager for the correct configurations.

1. In the Network window, double-click the TCP/IP service for the Ethernet card, which has been installed on your computer (e.g. TCP/IP -> PCI Fast Ethernet DEC 21143 Based Adapter).
   The TCP/IP Properties window opens.

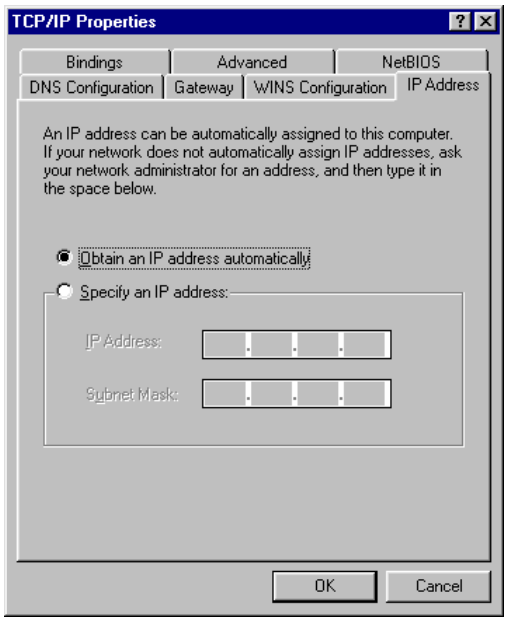


2. Click the Gateway tab, and remove any installed gateways.

3. Click the **DNS Configuration** tab, and click the **Disable DNS** radio button.



4. Click the IP Address tab, and click the Obtain an IP address automatically radio button.



Note: Normally, it is not recommended to assign a static IP address to your PC but rather to obtain an IP address automatically. If for some reason you need to assign a static IP address, select Specify an IP address, type in an IP address in the range of 192.168.10.129-254, enter 255.255.255.0 in the Subnet Mask field, and click OK to save the new settings.

(Note that 192.168.10 is the default value, and it may vary if you changed it in the My Network page.)

5. Click Yes when prompted for "Do you want to restart your computer?".

   Your computer restarts, and the new settings to take effect.

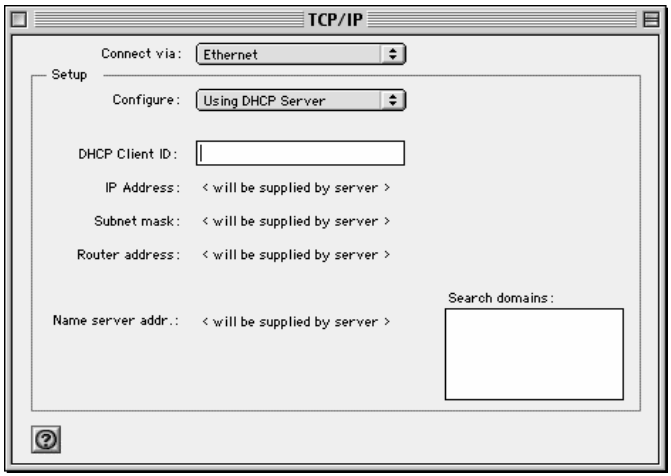
   Your computer is now ready to access your Safe@Office appliance.

Mac OS

Use the following procedure for setting up the TCP/IP Protocol.

1. Choose **Apple Menus -> Control Panels -> TCP/IP**.

   The **TCP/IP window** appears.



2. Click the **Connect via** drop-down list, and select **Ethernet**.
3. Click the **Configure** drop-down list, and select **Using DHCP Server**.
4. Close the window and save the setup.

Mac OS-X

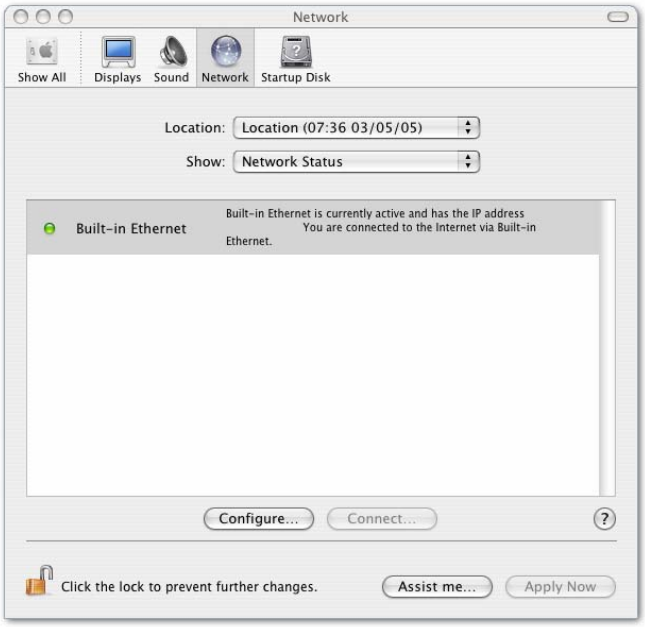
Use the following procedure for setting up the TCP/IP Protocol.

1. Choose Apple -> System Preferences.

   The System Preferences window appears.

2. Click Network.

   The Network window appears.



3. Click **Configure.**

TCP/IP configuration fields appear.

4. Click the Configure IPv4 drop-down list, and select Using DHCP.
5. Click Apply Now.

Wall Mounting the Appliance

500W

If desired, you can mount your Safe@Office 500W appliance on the wall.

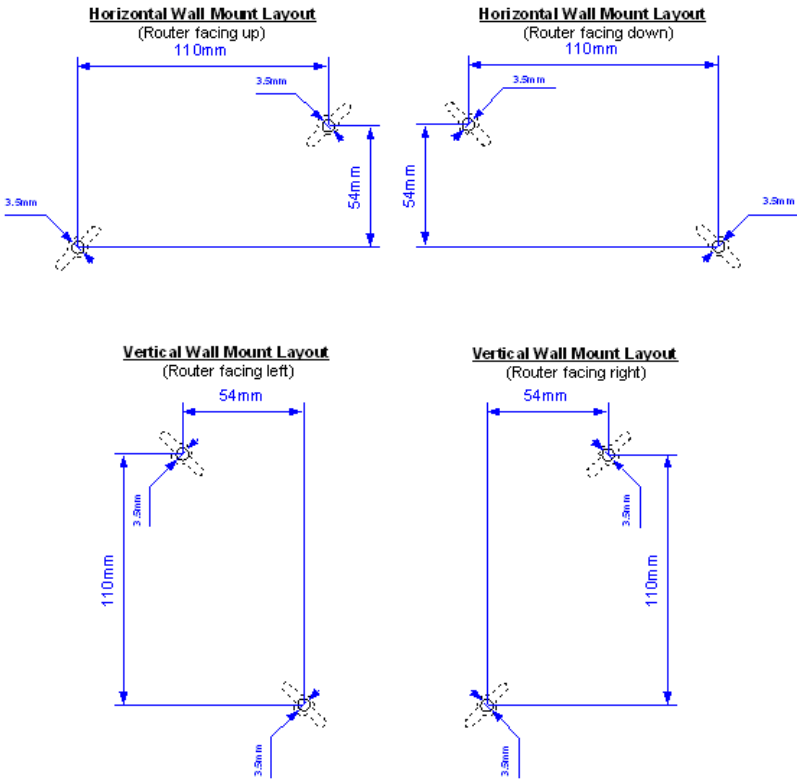
To mount the Safe@Office appliance on the wall

1. Decide where you want to mount your Safe@Office appliance.
2. Decide on the mounting orientation.

   You can mount the appliance on the wall facing up, down, left, or right.

Note: Mounting the appliance facing downwards is not recommended, as dust might accumulate in unused ports.

3. Mark two drill holes on the wall, in accordance with the following sketch:



4. Drill two 3.5 mm diameter holes, approximately 25 mm deep.
5. Insert two plastic conical anchors into the holes.

Note: The conical anchors you received with your Safe@Office appliance are suitable for concrete walls. If you want to mount the appliance on a plaster wall, you must use anchors that are suitable for plaster walls.

6. Insert the two screws you received with your Safe@Office appliance into the plastic conical anchors, and turn them until they protrude approximately 5 mm from the wall.

7. Align the holes on the Safe@Office appliance's underside with the screws on the wall, then push the appliance in and down.

   Your Safe@Office appliance is wall mounted. You can now connect it to your computer. See ***Network Installation*** on page 35.

Securing the Appliance against Theft

500W

The Safe@Office 500W features a security slot to the rear of the right panel, which enables you to secure your appliance against theft, using an anti-theft security device.

Note: Anti-theft security devices are available at most computer hardware stores.

This procedure explains how to install a looped security cable on your appliance. A looped security cable typically includes the parts shown in the diagram below.

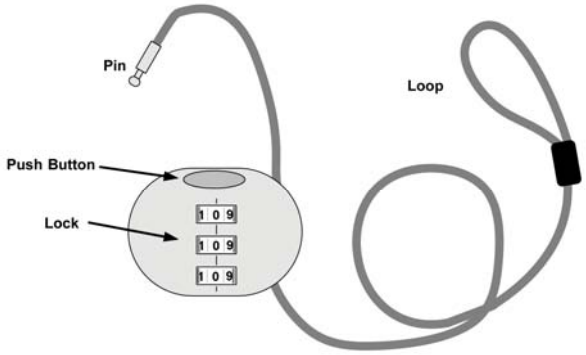


Figure 6: Looped Security Cable

While these parts may differ between devices, all looped security cables include a bolt with knobs, as shown in the diagram below:

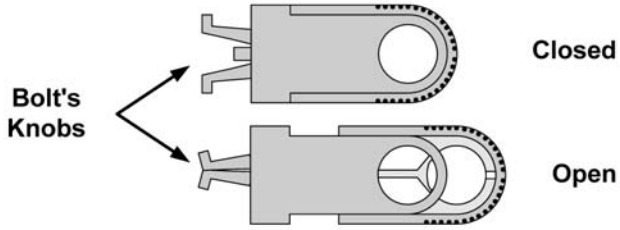


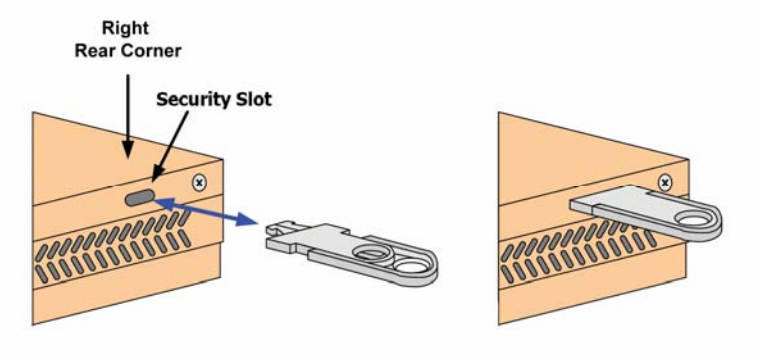
Figure 7: Looped Security Cable Bolt

The bolt has two states, Open and Closed, and is used to connect the looped security cable to the appliance's security slot.

To install an anti-theft device on the Safe@Office appliance

1. If your anti-theft device has a combination lock, set the desired code, as described in the documentation that came with your device.
2. Connect the anti-theft device's loop to any sturdy mounting point, as described in the documentation that came with your device.
3. Slide the anti-theft device's bolt to the Open position.

4. Insert the bolt into the Safe@Office appliance's security slot, then slide the bolt to the Closed position until the the bolts holes are aligned.



5. Thread the anti-theft device's pin through the bolt’s holes, and insert the pin into the main body of the anti-theft device, as described in the documentation that came with your device.

Network Installation

1. Verify that you have the correct cable type.

   For information, see Network Requirements.

2. Connect the LAN cable:

   - Connect one end of the Ethernet cable to one of the LAN ports at the back of the unit.
   - Connect the other end to PCs, hubs, or other network devices.

3. Connect the WAN cable:

   - Connect one end of the Ethernet cable to the WAN port at the back of the unit.
   - Connect the other end of the cable to a Cable Modem, xDSL modem or office network.

4. Connect the power adapter to the power socket, labeled PWR, at the back of the Safe@Office appliance.
5. Plug the power adapter into the wall electrical outlet.

Warning: The Safe@Office appliance power adapter is compatible with either 100, 120 or 230 VAC input power. Verify that the wall outlet voltage is compatible with the voltage specified on your power adapter. Failure to observe this warning may result in injuries or damage to equipment.

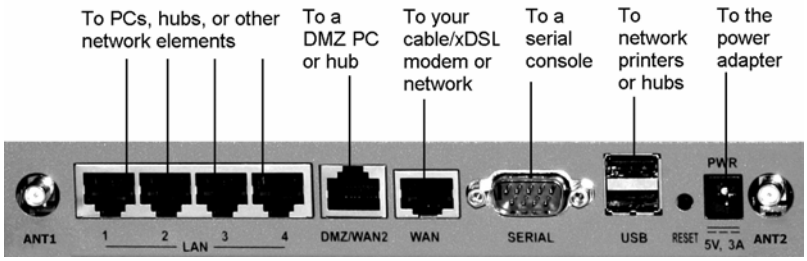


Figure 8: Typical Connection Diagram

6. In wireless models, prepare the Safe@Office appliance for a wireless connection:

   a. Connect the antennas that came with your Safe@Office appliance to the ANT1 and ANT2 antenna connectors in the appliance's rear panel.

   b. Bend the antennas at the hinges, so that they point upwards.

7. In models with a print server, you can connect network printers as follows:

   a. Connect one end of a USB cable to a USB port at the back of the unit.

      If needed, you can use the provided USB extension cord.

   b. Connect the other end to a printer or a USB 2.0 hub.

Warning: Verify that the USB devices' power requirement does not exceed the appliance's USB power supply capabilities. Failure to observe this warning may cause damage to the appliance and void the warranty.

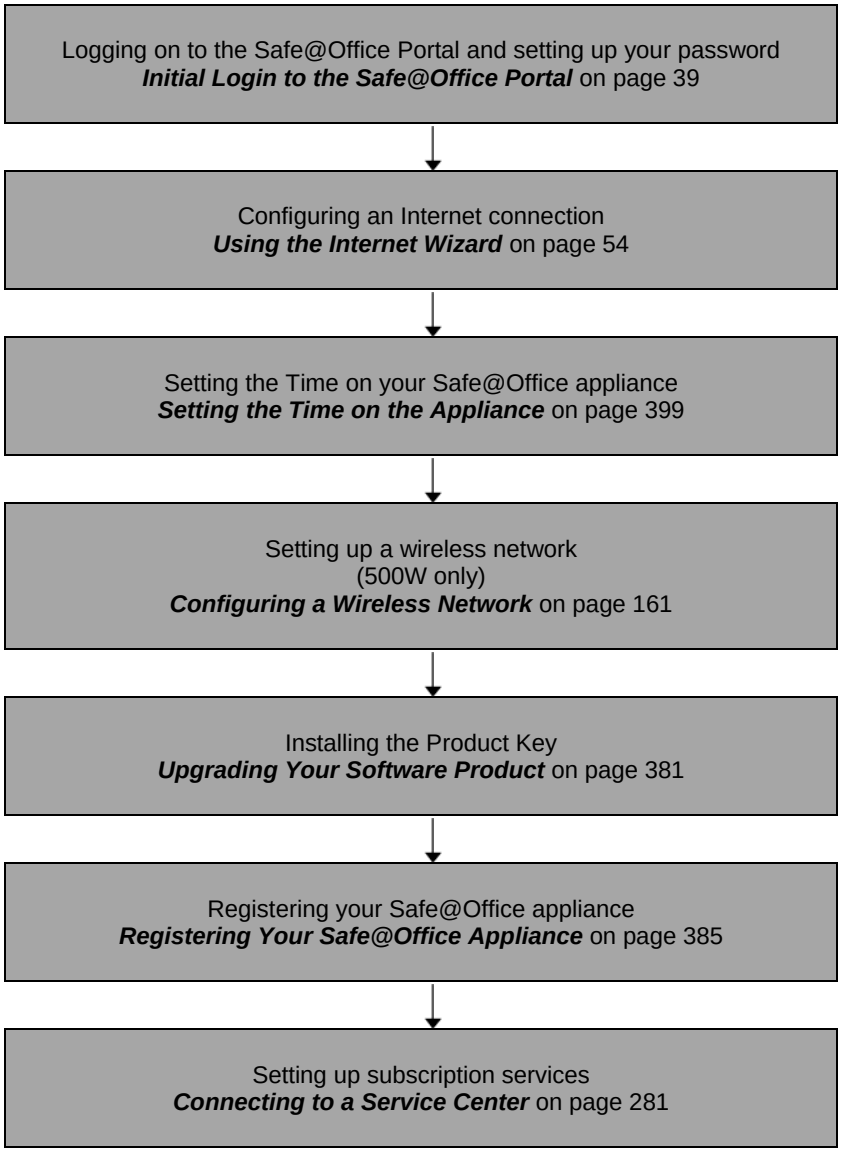
For information on setting up network printers, see ***Setting up Network Printers*** on page 426.

Setting Up the Safe@Office Appliance

500

After you have installed the Safe@Office appliance, you must set it up using the steps shown below.

When setting up your Safe@Office appliance for the first time after installation, these steps follow each other automatically. After you have logged on and set up your password, the Safe@Office Setup Wizard automatically opens and displays the dialog boxes for configuring your Internet connection. After you have configured your Internet connection, the Setup Wizard automatically displays the dialog boxes for registering your Safe@Office appliance. If desired, you can exit the Setup Wizard and perform each of these steps separately.

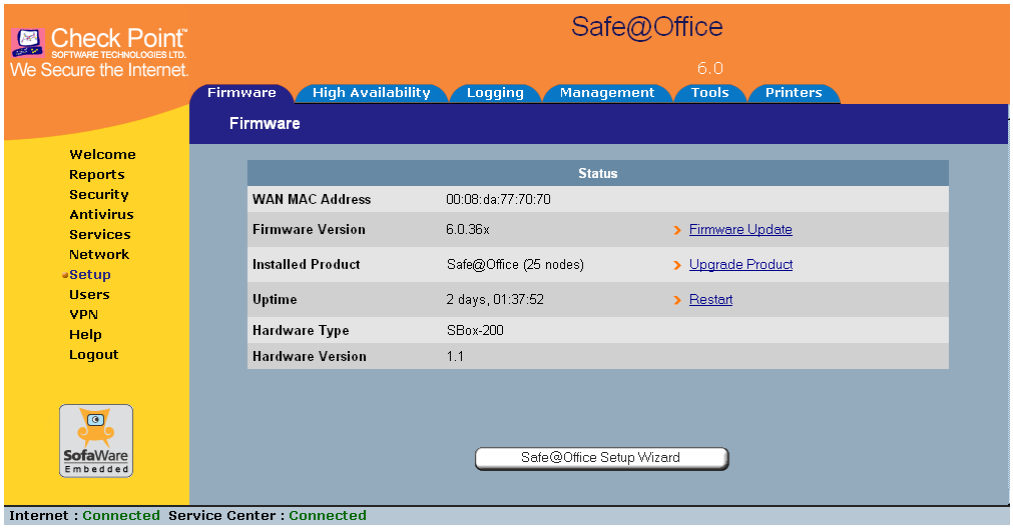


You can access the Setup Wizard at any time after initial setup, using the procedure below.

To access the Setup Wizard

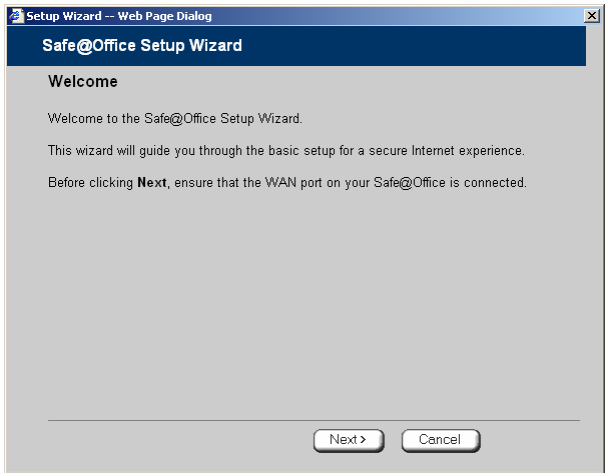
1. Click **Setup** in the main menu, and click the **Firmware** tab.

   The **Firmware** page appears.



2. Click **Safe@Office Setup Wizard**.

   The **Safe@Office Setup Wizard** opens with the **Welcome** page displayed.



Chapter 3

Getting Started

This chapter contains all the information you need in order to get started using your Safe@Office appliance.

This chapter includes the following topics:

Initial Login to the Safe@Office Portal

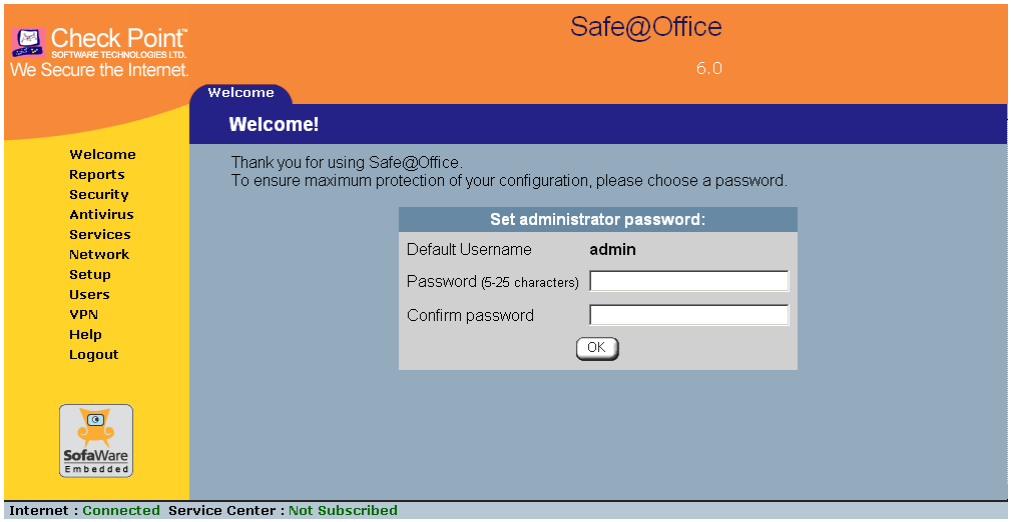
500

The first time you log on to the Safe@Office Portal, you must set up your password.

To log on to the Safe@Office Portal for the first time

1. Browse to http://my.firewall.

The initial login page appears.



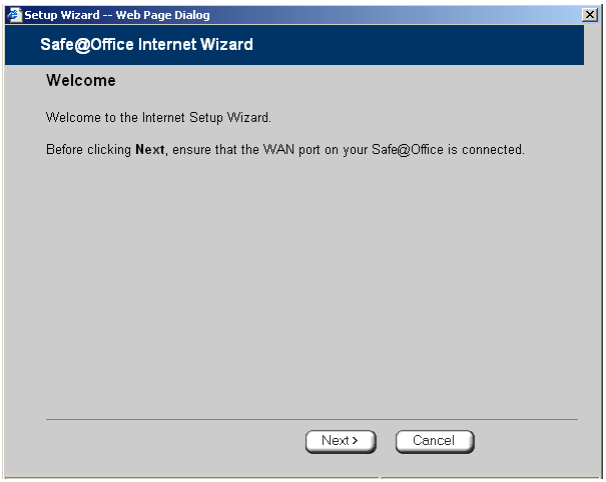
2. Type a password both in the **Password** and the **Confirm Password** fields.

Note: The password must be five to 25 characters (letters or numbers).

Note: You can change your password at any time. For further information, see Changing Your Password.

3. Click **OK**.

The Safe@Office Setup Wizard opens, with the Welcome page displayed.



4. Configure your Internet connection using one of the following ways:

   - Internet Wizard

     The Internet Wizard is the first part of the Setup Wizard, and it takes you through basic Internet connection setup, step by step. For information on using the Internet Wizard, see ***Using the Internet Wizard*** on page 54.

     After you have completed the Internet Wizard, the Setup Wizard continues to guide you through appliance setup. For more information, see Setting Up the Safe@Office Appliance.

   - Internet Setup

     Internet Setup offers advanced setup options, such as configuring two Internet connections. To use Internet Setup, click Cancel and refer to ***Using Internet Setup*** on page 63.

Logging on to the Safe@Office Portal

500

Note: By default, HTTP and HTTPS access to the Safe@Office Portal is not allowed from the WLAN, unless you do one of the following:

- Configure a specific firewall rule to allow access from the WLAN. See ***Using Rules*** on page 209.

  Or

- Enable HTTPS access from the Internet. See ***Configuring HTTPS*** on page 392.

To log on to the Safe@Office Portal

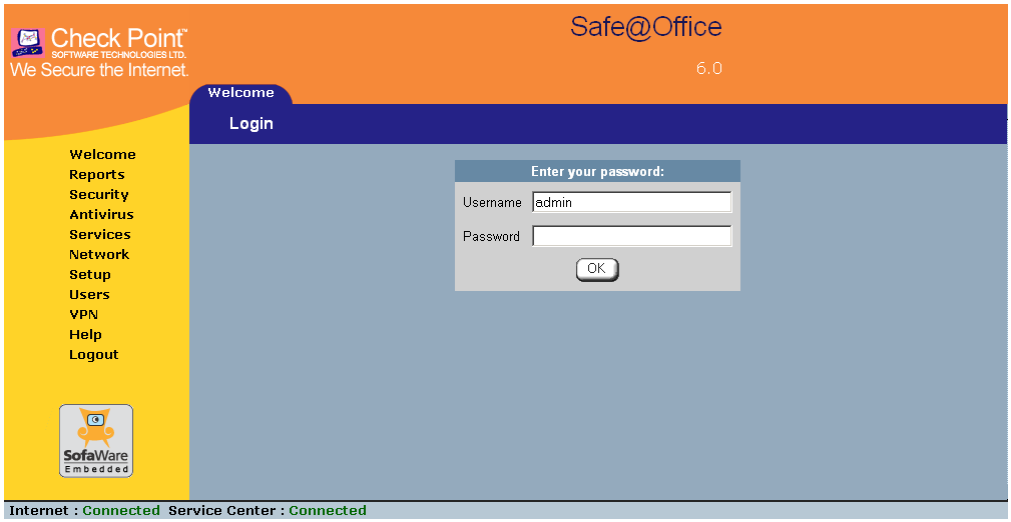
1. Do one of the following:

   - Browse to http://my.firewall.

     Or

   - To log on through HTTPS (locally or remotely), follow the procedure ***Accessing the Safe@Office Portal Remotely*** on page 44.

The login page appears.



2. Type your username and password.
3. Click OK.

The Welcome page appears.

Accessing the Safe@Office Portal Remotely Using HTTPS

500

You can access the Safe@Office Portal remotely (from the Internet) through HTTPS. HTTPS is a protocol for accessing a secure Web server. It is used to transfer confidential user information. If desired, you can also use HTTPS to access the Safe@Office Portal from your internal network.

Note: In order to access the Safe@Office Portal remotely using HTTPS, you must first do both of the following:

- Configure your password, using HTTP. See ***Initial Login to the Safe@Office Portal*** on page 39.
- Configure HTTPS Remote Access. See ***Configuring HTTPS*** on page 392.

Note: Your browser must support 128-bit cipher strength. To check your browser's cipher strength, open Internet Explorer and click Help > About Internet Explorer.

To access the Safe@Office Portal from your internal network

- Browse to https://my.firewall.

  (Note that the URL starts with “https”, not “http”.)

  The Safe@Office Portal appears.

To access the Safe@Office Portal from the Internet

- Browse to https://<firewall_IP_address>:981.

  (Note that the URL starts with “https”, not “http”.)

  The following things happen in the order below:

  If this is your first attempt to access the Safe@Office Portal through HTTPS, the certificate in the Safe@Office appliance is not yet known to the browser, so the Security Alert dialog box appears.

  To avoid seeing this dialog box again, install the certificate of the destination Safe@Office appliance. If you are using Internet Explorer 5, do the following:

  a. Click View Certificate.

     The Certificate dialog box appears, with the General tab displayed.

  b. Click Install Certificate.

     The Certificate Import Wizard opens.

  c. Click Next.

  d. Click Next.

  e. Click Finish.

  f. Click Yes.

  g. Click OK.

The Security Alert dialog box reappears.

h. Click Yes.

The Safe@Office Portal appears.

Using the Safe@Office Portal

The Safe@Office Portal is a Web-based management interface, which enables you to manage and configure the Safe@Office appliance operation and options.

The Safe@Office Portal consists of three major elements.

Table 5: Safe@Office Portal Elements

Element	Description
Main menu	Used for navigating between the various topics (such as Reports, Security, and Setup).
Main frame	Displays information and controls related to the selected topic. The main frame may also contain tabs that allow you to view different pages related to the selected topic.
Status bar	Shows your Internet connection and managed services status.

Figure 9: Safe@Office Portal

Main Menu

The main menu includes the following submenus.

Table 6: Main Menu Submenus

This submenu…	Does this…
Welcome	Displays general welcome information.
Reports	Provides reporting capabilities in terms of event logging, traffic monitoring, active computers, and established connections.
Security	Provides controls and options for setting the security of any computer in the network.
Antivirus	Allows you to configure VStream Antivirus settings.
Services	Allows you to control your subscription to subscription services.

This submenu…	Does this…
Network	Allows you to manage and configure your network settings and Internet connections.
Setup	Provides a set of tools for managing your Safe@Office appliance. Allows you to upgrade your license and firmware and to configure HTTPS access to your Safe@Office appliance.
Users	Allows you to manage Safe@Office appliance users.
VPN	Allows you to manage, configure, and log on to VPN sites.
Help	Provides context-sensitive help.
Logout	Allows you to log off of the Safe@Office Portal.

Main Frame

The main frame displays the relevant data and controls pertaining to the menu and tab you select. These elements sometimes differ depending on what model you are using. The differences are described throughout this guide.

Status Bar

The status bar is located at the bottom of each page. It displays the fields below, as well as the date and time.

Table 7: Status Bar Fields

This field…	Displays this…
Internet	Your Internet connection status. The connection status may be one of the following: • Connected. The Safe@Office appliance is connected to the Internet. • Connected – Probing OK. Connection probing is enabled and has detected that the Internet connectivity is OK. • Connected – Probing Failed. Connection probing is enabled and has detected problems with the Internet connectivity. • Not Connected. The Internet connection is down. • Establishing Connection. The Safe@Office appliance is connecting to the Internet. • Contacting Gateway. The Safe@Office appliance is trying to contact the Internet default gateway. • Disabled. The Internet connection has been manually disabled. Note: You can configure both a primary and a secondary Internet connection. When both connections are configured, the Status bar displays both statuses. For example “Internet [Primary]: Connected”. For information on configuring a secondary Internet connection, see ***Configuring the Internet Connection*** on page 53.

This field…	Displays this…
Service Center	Displays your subscription services status. Your Service Center may offer various subscription services. These include the firewall service and optional services such as Web Filtering and Email Antivirus. Your subscription services status may be one of the following: • **Not Subscribed**. You are not subscribed to security services. • **Connection Failed**. The Safe@Office appliance failed to connect to the Service Center. • **Connecting**. The Safe@Office appliance is connecting to the Service Center. • **Connected**. You are connected to the Service Center, and security services are active.

Logging off

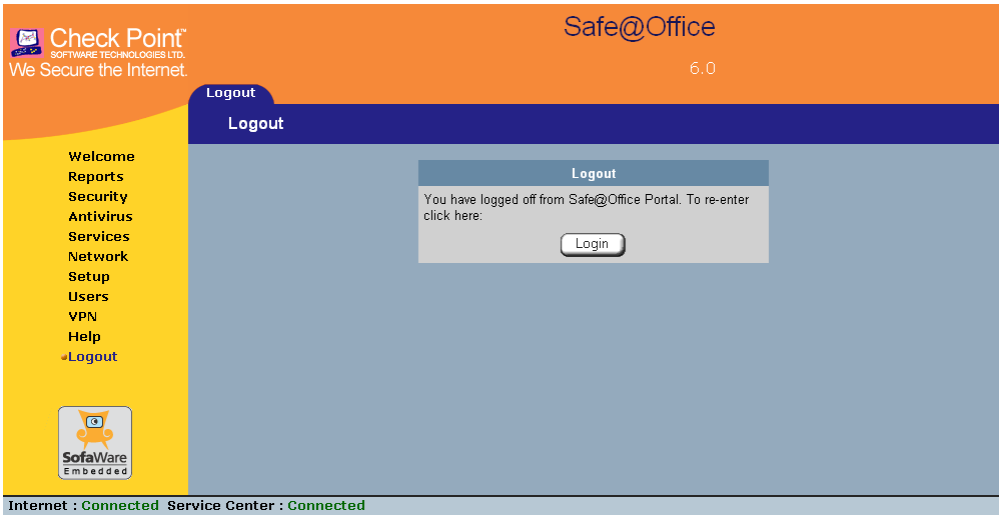
500

Logging off terminates your administration session. Any subsequent attempt to connect to the Safe@Office Portal will require re-entering of the administration password.

To log off of the Safe@Office Portal

- Do one of the following:
  - If you are connected through HTTP, click Logout in the main menu.

    The Logout page appears.



  - If you are connected through HTTPS, the Logout option does not appear in the main menu. Close the browser window.

Chapter 4

Configuring the Internet Connection

This chapter describes how to configure and work with an Safe@Office Internet connection.

This chapter includes the following topics:

Overview

You must configure your Internet connection before you can access the Internet through the Safe@Office appliance. You can configure your Internet connection using any of the following setup tools:

- Setup Wizard. Guides you through the Safe@Office appliance setup step by step. The first part of the Setup Wizard is the Internet Wizard. For further information on the Setup Wizard, see Setting Up the Safe@Office Appliance.
- Internet Wizard. Guides you through the Internet connection configuration process step by step.
- Internet Setup. Offers the following advanced setup options:
  - Configure two Internet connections.

    For information, see ***Configuring a Backup Internet Connection*** on page 90.

- Enable Traffic Shaper for traffic flowing through the connection.

  For information on Traffic Shaper, see ***Using Traffic Shaper*** on page 151.

- Configure a dialup Internet connection.

  Before configuring the connection, you must first set up the modem. For information, see ***Setting Up a Dialup Modem*** on page 84.

Using the Internet Wizard

500

The Internet Wizard allows you to configure your Safe@Office appliance for Internet connection quickly and easily through its user-friendly interface. It lets you to choose between the following three types of broadband connection methods:

- Direct LAN Connection
- Cable Modem
- PPTP or PPPoE dialer

Note: The first time you log on to the Safe@Office Portal, the Internet Wizard starts automatically as part of the Setup Wizard. In this case, you should skip to step 3 in the procedure below.

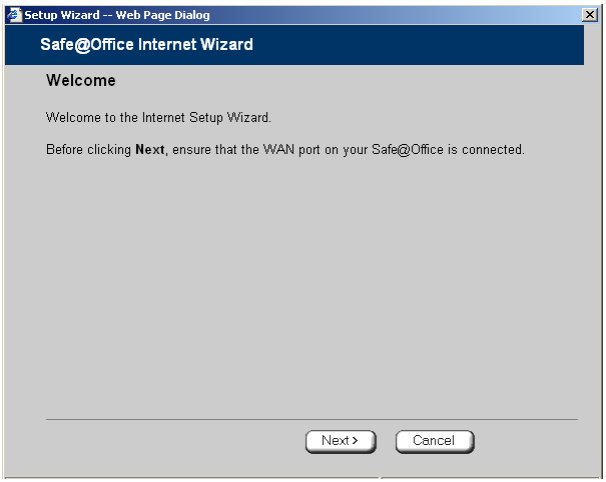
To set up the Internet connection using the Internet Wizard

1. Click Network in the main menu, and click the Internet tab.

   The Internet page appears.

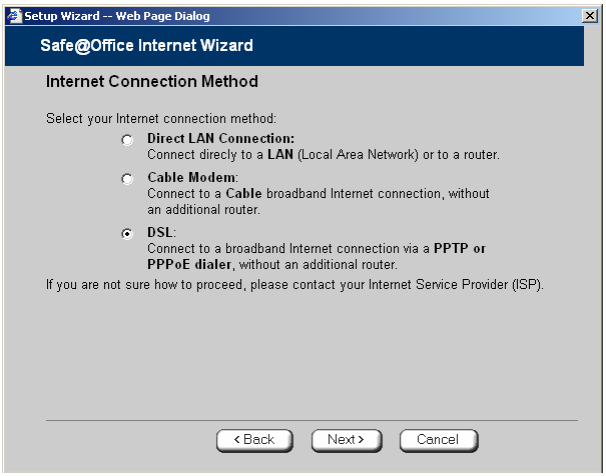
2. Click Internet Wizard.

The Internet Wizard opens with the **Welcome** page displayed.



3. Click **Next.**

   The **Internet Connection Method** dialog box appears.



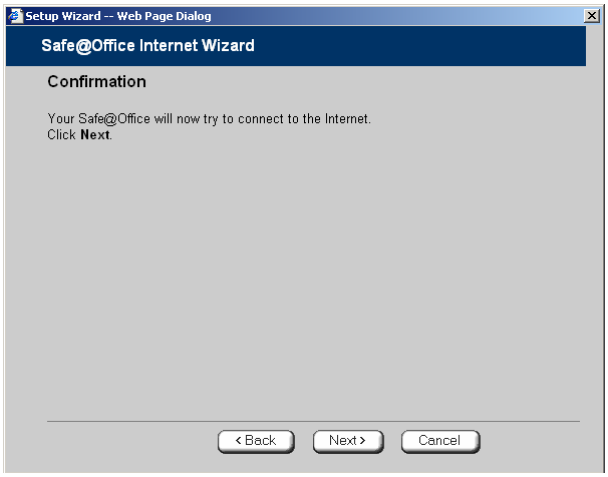
4. Select the Internet connection method you want to use for connecting to the Internet.

Note: If you selected PPTP or PPPoE dialer, do not use your dial-up software to connect to the Internet.

5. Click **Next**.

Using a Direct LAN Connection

No further settings are required for a direct LAN (Local Area Network) connection. The **Confirmation** screen appears.



1. Click **Next**.

   The system attempts to connect to the Internet via the selected connection.

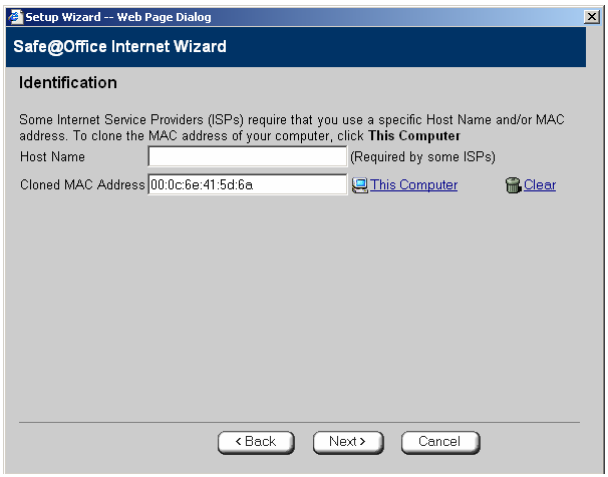
   The **Connecting**... screen appears.

At the end of the connection process the **Connected** screen appears.

2. Click **Finish**.

Using a Cable Modem Connection

If you selected the Cable Modem connection method, the Identification dialog box appears.



1. If your ISP requires a specific hostname for authentication, type it in the Host Name field.

   The ISP will supply you with the proper hostname, if required. Most ISPs do not require a specific hostname.

2. A MAC address is a 12-digit identifier assigned to every network device. If your ISP restricts connections to specific, recognized MAC addresses, they will instruct you to enter the MAC address. Otherwise, you may leave this field blank.

   If your ISP requires the MAC address, do either of the following:

   - Click This Computer to automatically "clone" the MAC address of your computer to the Safe@Office appliance.

     Or

   - If the ISP requires authentication using the MAC address of a different computer, enter the MAC address in the MAC cloning field.

3. Click **Next**.

   The **Confirmation** screen appears.

4. Click **Next**.

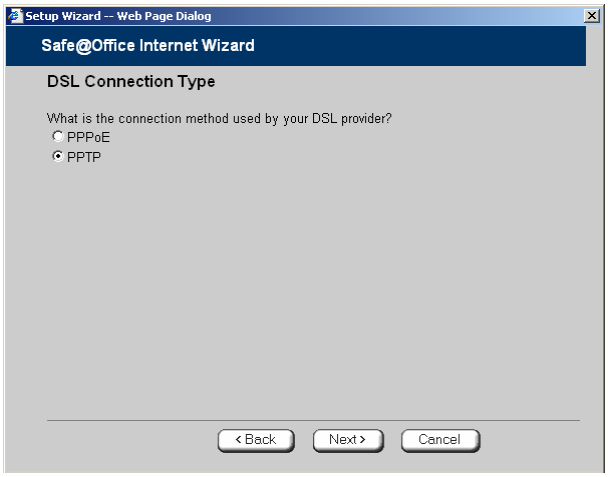
   The system attempts to connect to the Internet.

   The **Connecting**... screen appears. At the end of the connection process the **Connected** screen appears.

5. Click **Finish**.

Using a PPTP or PPPoE Dialer Connection

If you selected the PPTP or PPPoE dialer connection method, the **DSL Connection Type** dialog box appears.



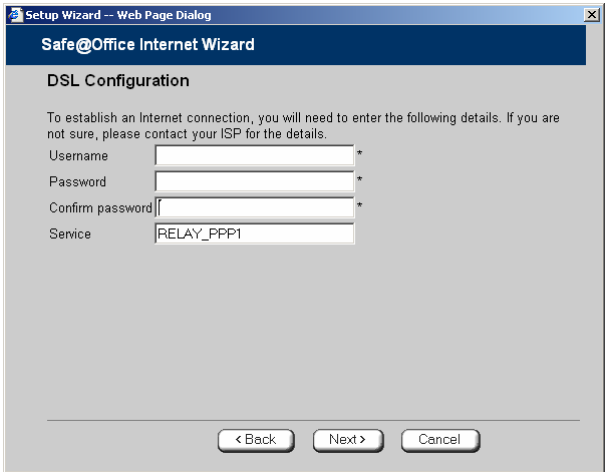
1. Select the connection method used by your DSL provider.

Note: Most xDSL providers use PPPoE. If you are uncertain regarding which connection method to use contact your xDSL provider.

2. Click **Next**.

Using PPPoE

If you selected the PPPoE connection method, the DSL Configuration dialog box appears.



1. Complete the fields using the information in the table below.
2. Click Next.

   The Confirmation screen appears.
3. Click Next.

   The system attempts to connect to the Internet via the DSL connection.

   The Connecting... screen appears.

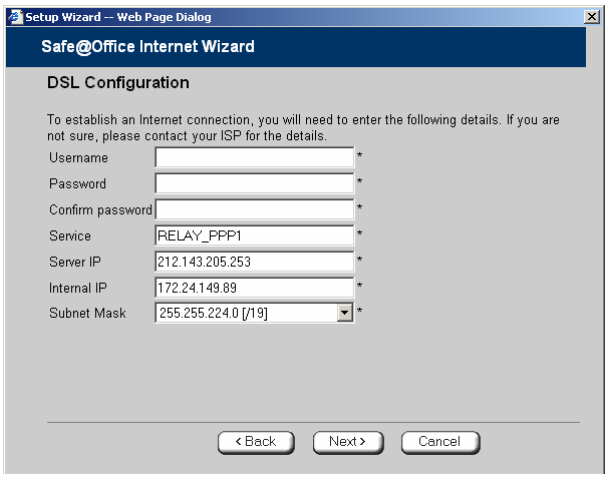
   At the end of the connection process the Connected screen appears.
4. Click Finish.

Table 8: PPPoE Connection Fields

In this field…	Do this…
Username	Type your user name.
Password	Type your password.
Confirm password	Type your password again.
Service	Type your service name. This field can be left blank.

Using PPTP

If you selected the PPTP connection method, the DSL Configuration dialog box appears.



1. Complete the fields using the information in the table below.
2. Click Next.

   The Confirmation screen appears.

3. Click Next.

   The system attempts to connect to the Internet via the DSL connection.

   The Connecting... screen appears.

   At the end of the connection process the Connected screen appears.

4. Click Finish.

Table 9: PPTP Connection Fields

In this field...	Do this...
Username	Type your user name.
Password	Type your password.
Confirm password	Type your password again.
Service	Type your service name.
Server IP	Type the IP address of the PPTP modem.
Internal IP	Type the local IP address required for accessing the PPTP modem.
Subnet Mask	Type the subnet mask of the PPTP modem.

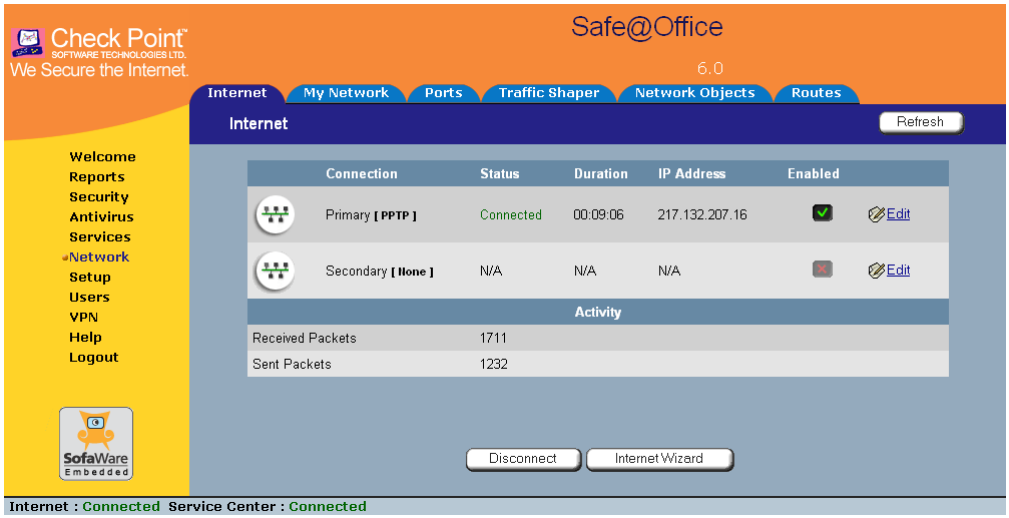
Using Internet Setup

500

Internet Setup allows you to manually configure your Internet connection.

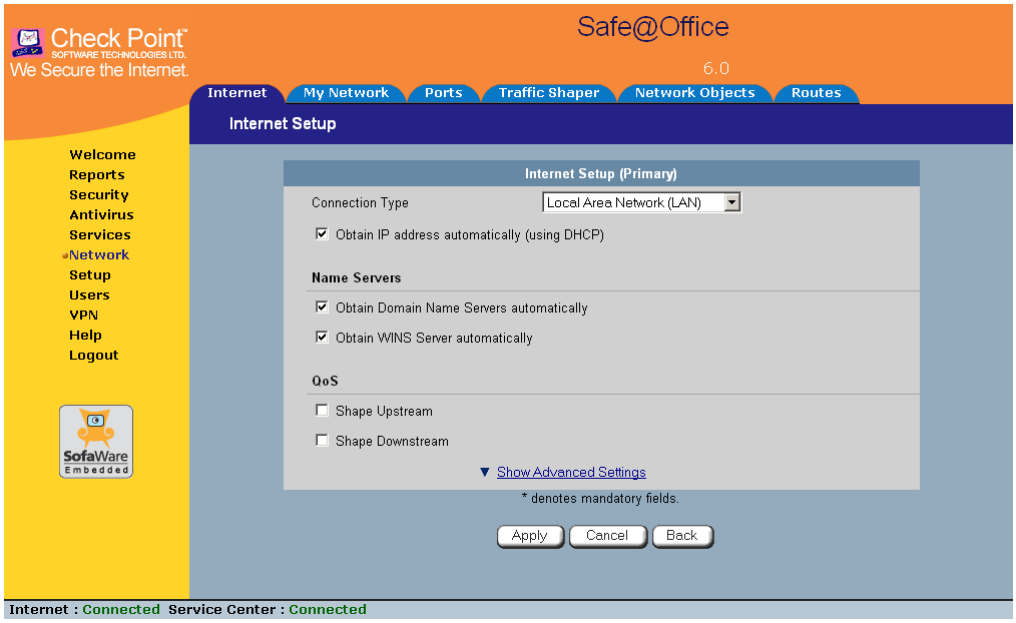
To configure the Internet connection using Internet Setup

1. Click **Network** in the main menu, and click the **Internet** tab.



2. Next to the desired Internet connection, click **Edit**.

The **Internet Setup** page appears.

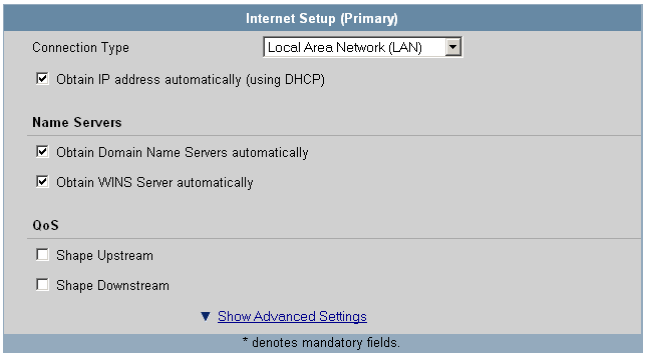


3. From the **Connection Type** drop-down list, select the Internet connection type you are using/intend to use.

   The display changes according to the connection type you selected.

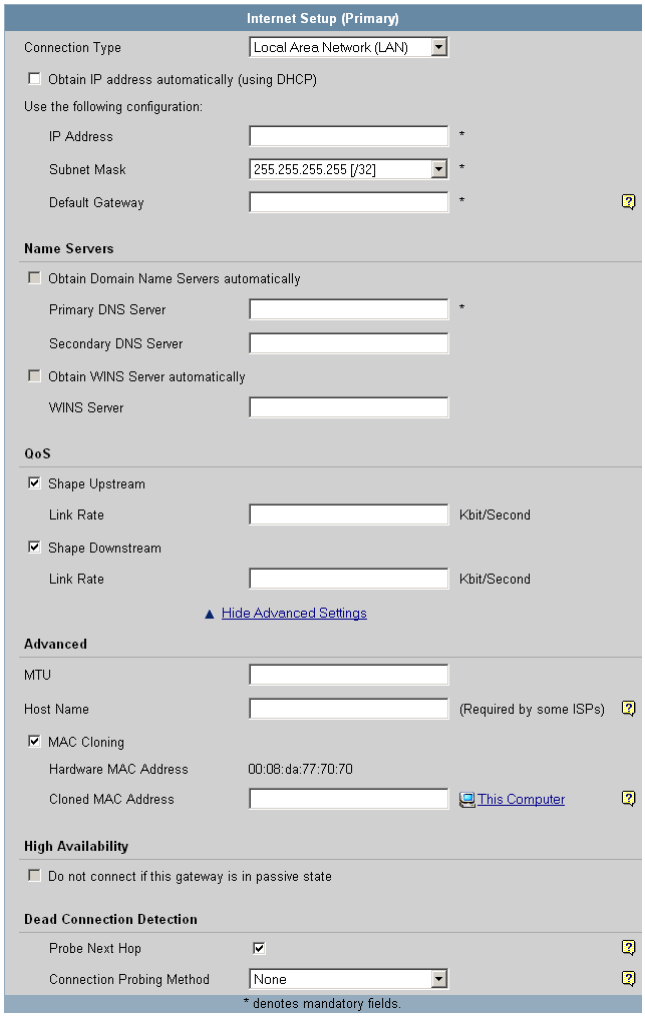
The following steps should be performed in accordance with the connection type you have chosen.

Using a LAN Connection



1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 77.

New fields appear, depending on the check boxes you selected.

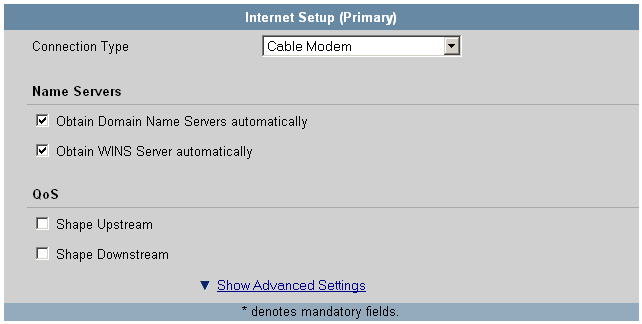


2. Click **Apply**.

   The Safe@Office appliance attempts to connect to the Internet, and the Status Bar displays the Internet status “Connecting”. This may take several seconds.

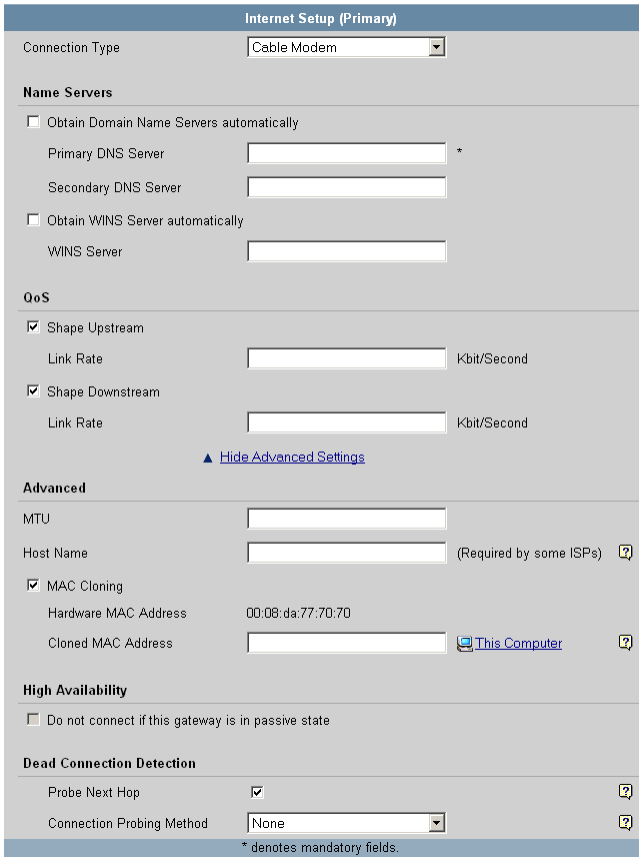
   Once the connection is made, the Status Bar displays the Internet status “Connected”.

Using a Cable Modem Connection



1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 77.

New fields appear, depending on the check boxes you selected.

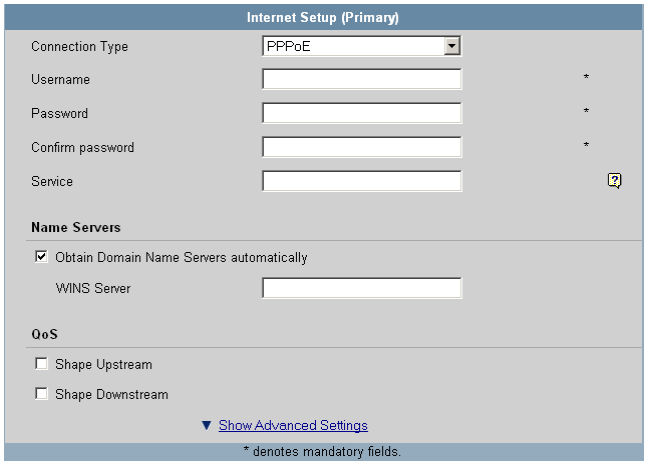


2. Click **Apply**.

   The Safe@Office appliance attempts to connect to the Internet, and the Status Bar displays the Internet status “Connecting”. This may take several seconds.

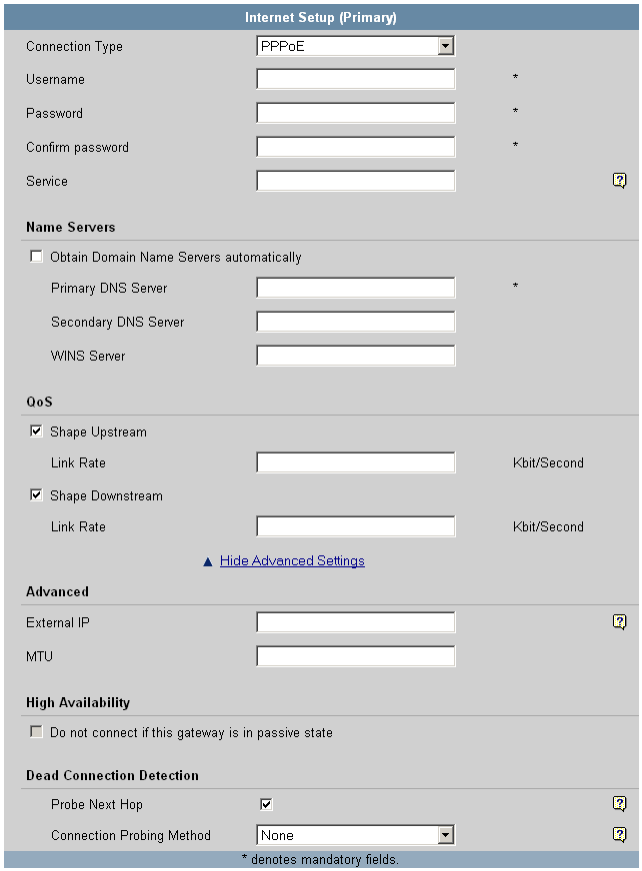
   Once the connection is made, the Status Bar displays the Internet status “Connected”.

Using a PPPoE Connection



1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 77.

New fields appear, depending on the check boxes you selected.

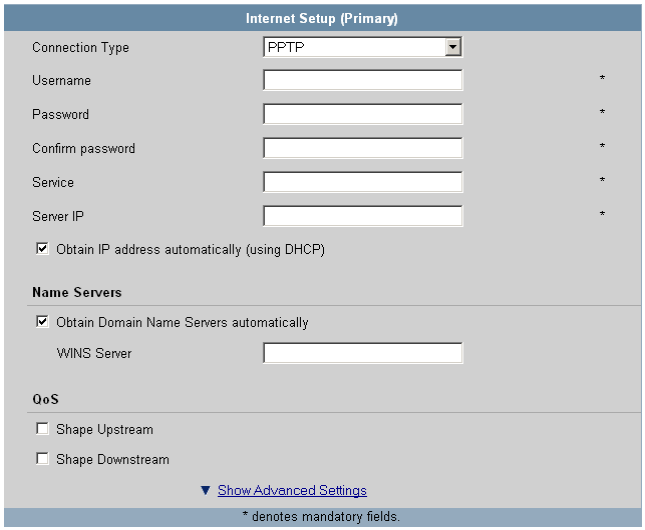


2. Click **Apply**.

   The Safe@Office appliance attempts to connect to the Internet, and the Status Bar displays the Internet status “Connecting”. This may take several seconds.

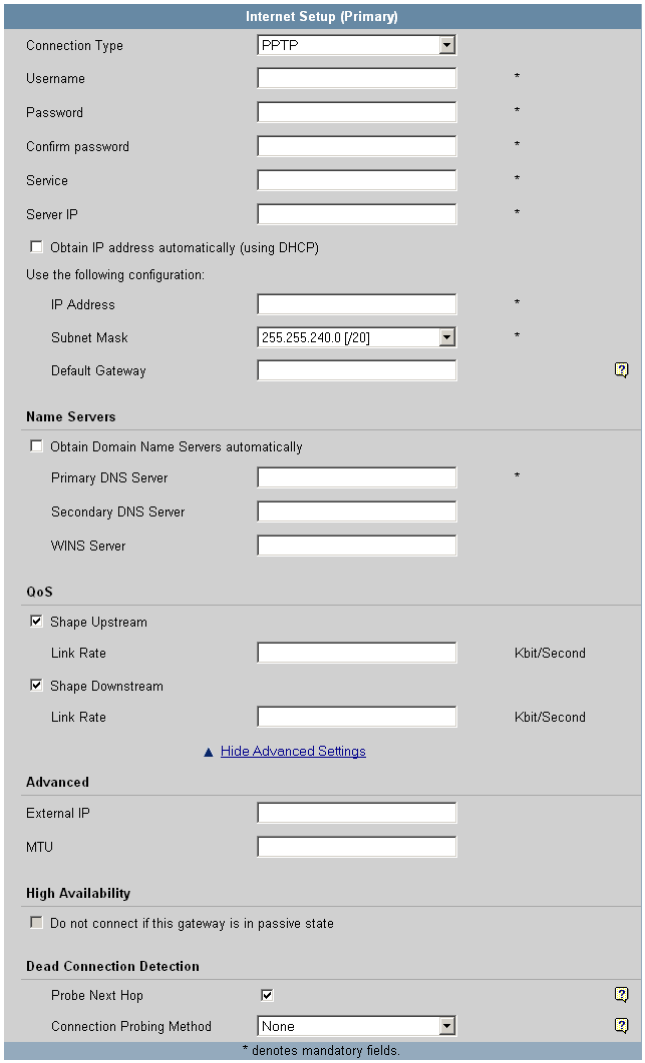
   Once the connection is made, the Status Bar displays the Internet status “Connected”.

Using a PPTP Connection



1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 77.

New fields appear, depending on the check boxes you selected.



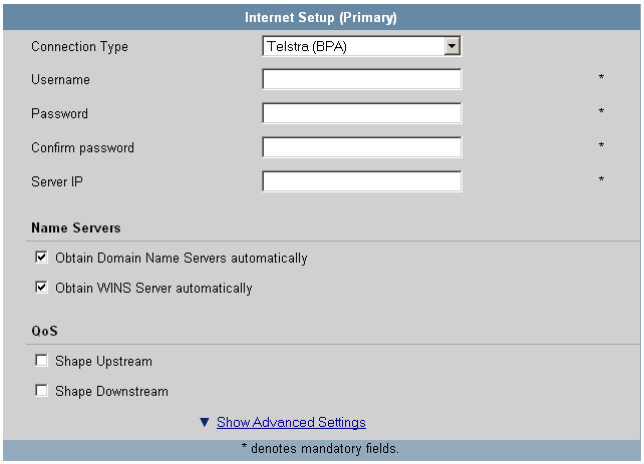
2. Click **Apply**.

   The Safe@Office appliance attempts to connect to the Internet, and the Status Bar displays the Internet status “Connecting”. This may take several seconds.

Once the connection is made, the Status Bar displays the Internet status “Connected”.

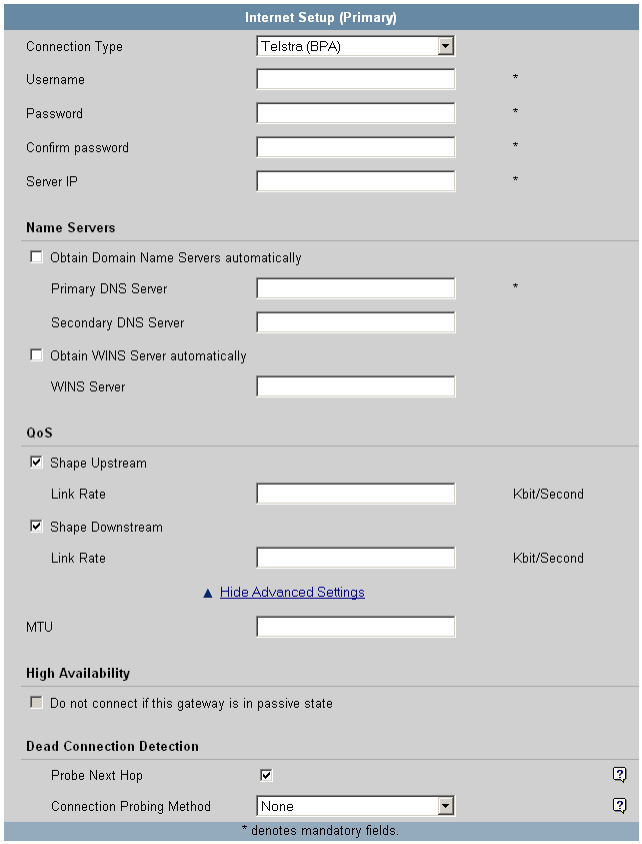
Using a Telstra (BPA) Connection

Use this Internet connection type only if you are subscribed to Telstra® BigPond™ Internet. Telstra BigPond is a trademark of Telstra Corporation Limited.



1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 77.

New fields appear, depending on the check boxes you selected.



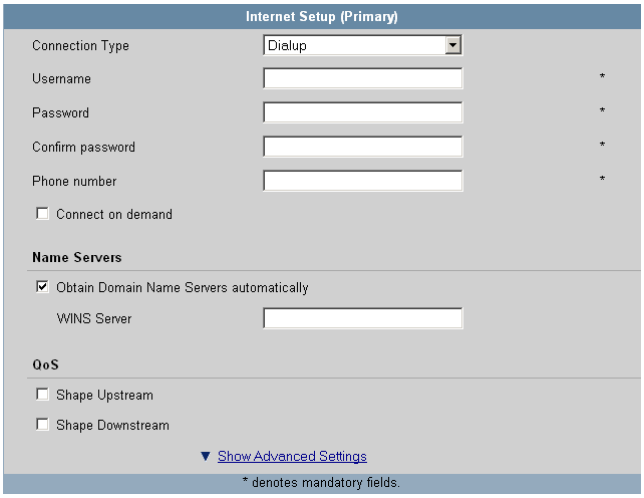
2. Click **Apply**.

   The Safe@Office appliance attempts to connect to the Internet, and the Status Bar displays the Internet status “Connecting”. This may take several seconds.

   Once the connection is made, the Status Bar displays the Internet status “Connected”.

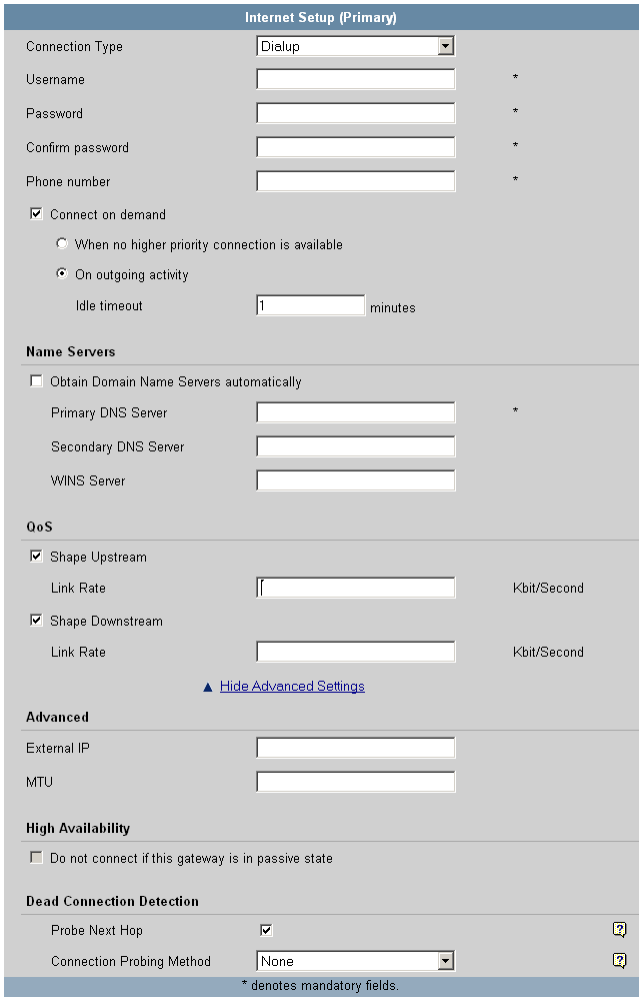
Using a Dialup Connection

To use this connection type, you must first set up the dialup modem. For information, see ***Setting Up a Dialup Modem*** on page 84.



1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 77.

New fields appear, depending on the check boxes you selected.



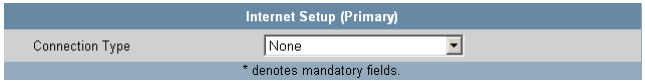
2. Click **Apply**.

   The Safe@Office appliance attempts to connect to the Internet, and the Status Bar displays the Internet status “Connecting”. This may take several seconds.

Once the connection is made, the Status Bar displays the Internet status “Connected”.

Using No Connection

If you do not have an Internet connection, set the connection type to None.



- Click Apply.

Table 10: Internet Setup Fields

In this field…	Do this…
Username	Type your user name.
Password	Type your password.
Confirm password	Type your password.
Service	Type your service name. If your ISP has not provided you with a service name, leave this field empty.
Server IP	If you selected PPTP, type the IP address of the PPTP server as given by your ISP. If you selected Telstra (BPA), type the IP address of the Telstra authentication server as given by Telstra.
Phone Number	If you selected Dialup, type the phone number that the modem should dial, as given by your ISP.

In this field…	Do this…
Connect on demand	Select this option if you do not want the dialup modem to be constantly connected to the Internet. The modem will dial a connection only under certain conditions. This option is useful when configuring a dialup backup connection. For information, see ***Setting Up a Dialup Backup Connection*** on page 92.
When no higher priority connection is available	Select this option to specify that the dialup modem should only dial a connection if no other connection exists, and the Safe@Office appliance is not acting as a Backup appliance. If another connection opens, the dialup modem will disconnect. For information on configuring the appliance as a Backup or Master, see ***Configuring High Availability*** on page 119.
On outgoing activity	Select this option to specify that the dialup modem should only dial a connection if no other connection exists, and there is outgoing activity (that is, packets need to be transmitted to the Internet). If another connection opens, or if the connection times out, the dialup modem will disconnect.
Idle timeout	Type the amount of time (in minutes) that the connection can remain idle. Once this period of time has elapsed, the dialup modem will disconnect.
Obtain IP address automatically (using DHCP)	Clear this option if you do not want the Safe@Office appliance to obtain an IP address automatically using DHCP.
IP Address	Type the static IP address of your Safe@Office appliance.
Subnet Mask	Select the subnet mask that applies to the static IP address of your Safe@Office appliance.

In this field…	Do this…
Default Gateway	Type the IP address of your ISP's default gateway.
Name Servers	
Obtain Domain Name Servers automatically	Clear this option if you want the Safe@Office appliance to obtain an IP address automatically using DHCP, but not to automatically configure DNS servers.
Obtain WINS Server automatically	Clear this option if you want the Safe@Office appliance to obtain an IP address automatically using DHCP, but not to automatically configure the WINS server.
Primary DNS Server	Type the Primary DNS server IP address.
Secondary DNS Server	Type the Secondary DNS server IP address.
WINS Server	Type the WINS server IP address.
QoS	
Shape Upstream: Link Rate	Select this option to enable Traffic Shaper for outgoing traffic. Then type a rate (in kilobits/second) slightly lower than your Internet connection's maximum measured upstream speed in the field provided. It is recommended to try different rates in order to determine which one provides the best results. For information on using Traffic Shaper, see ***Using Traffic Shaper*** on page 151.

In this field…	Do this…
Shape Downstream: Link Rate	Select this option to enable Traffic Shaper for incoming traffic. Then type a rate (in kilobits/second) slightly lower than your Internet connection's maximum measured downstream speed in the field provided. It is recommended to try different rates in order to determine which one provides the best results. Note: Traffic Shaper cannot control the number or type of packets it receives from the Internet; it can only affect the rate of incoming traffic by dropping received packets. This makes the shaping of inbound traffic less accurate than the shaping of outbound traffic. It is therefore recommended to enable traffic shaping for incoming traffic only if necessary. For information on using Traffic Shaper, see ***Using Traffic Shaper*** on page 151.
Advanced	
External IP	If you selected PPTP, type the IP address of the PPTP client as given by your ISP. If you selected PPPoE, this field is optional, and you do not have to fill it in unless your ISP has instructed you to do so.
MTU	This field allows you to control the maximum transmission unit size. As a general recommendation you should leave this field empty. If however you wish to modify the default MTU, it is recommended that you consult with your ISP first and use MTU values between 1300 and 1500.

In this field…	Do this…
MAC Cloning	A MAC address is a 12-digit identifier assigned to every network device. If your ISP restricts connections to specific, recognized MAC addresses, you must select this option to clone a MAC address. Note: When configuring MAC cloning for the secondary Internet connection, the DMZ/WAN2 port must be configured as WAN2; otherwise this field is disabled. For information on configuring ports, see ***Managing Ports*** on page 145.
Hardware MAC Address	This field displays the Safe@Office appliance's MAC address. This field is read-only.
Cloned MAC Address	Do one of the following: • Click This Computer to automatically "clone" the MAC address of your computer to the Safe@Office appliance. • If the ISP requires authentication using the MAC address of a different computer, type the MAC address in this field. Note: In the secondary Internet connection, this field is enabled only if the DMZ/WAN2 port is set to WAN2.
High Availability	The High Availability area only appears in Safe@Office 500 with Power Pack.
Do not connect if this gateway is in passive state	If you are using High Availability (HA), select this option to specify that the gateway should connect to the Internet only if it is the Active Gateway in the HA cluster. This field is only enabled if HA is configured. For information on HA, see ***Configuring High Availability*** on page 119.
Dead Connection Detection	

In this field…	Do this…
Probe Next Hop	Select this option to automatically detect loss of connectivity to the default gateway. If you selected LAN, this is done by sending ARP requests to the default gateway. If you selected PPTP, PPPoE, or Dialup, this is done by sending PPP echo reply (LCP) messages to the PPP peer. By default, if the default gateway does not respond, the Internet connection is considered to be down. If it is determined that the Internet connection is down, and two Internet connections are defined, a failover will be performed to the second Internet connection, ensuring continuous Internet connectivity. This option is selected by default.

In this field...	Do this...
Connection Probing Method	While the Probe Next Hop option checks the availability of the next hop router, which is usually at your ISP, connectivity to the next hop router does not always indicate that the Internet is accessible. For example, if there is a problem with a different router at the ISP, the next hop will be reachable, but the Internet might be inaccessible. Connection probing is a way to detect Internet failures that are more than one hop away. Specify what method to use for probing the connection, by selecting one of the following: • None. Do not perform Internet connection probing. Next hop probing will still be used, if the Probe Next Hop check box is selected. This is the default value. • Ping Addresses. Ping anywhere from one to three servers specified by IP address or DNS name in the 1, 2, and 3 fields. If for 45 seconds none of the defined servers respond to pinging, the Internet connection is considered to be down. Use this method if you have reliable servers that can be pinged, that are a good indicator of Internet connectivity, and that are not likely to fail simultaneously (that is, they are not at the same location). • Probe DNS Servers. Probe the primary and secondary DNS servers. If for 45 seconds neither gateway responds, the Internet connection is considered to be down. Use this method if the availability of your DNS servers is a good indicator for the availability of Internet connectivity. • Probe VPN Gateway (RDP). Send RDP echo requests to up to three Check Point VPN gateways specified by IP address or DNS name in the 1, 2, and 3 fields. If for 45 seconds none of the defined gateways respond, the Internet connection is considered to be down. Use this option if you have Check Point VPN gateways, and you want loss of connectivity to these gateways to trigger ISP failover to an Internet connection from which these gateways are reachable.

In this field…	Do this…
1, 2, 3	If you chose the Ping Addresses connection probing method, type the IP addresses or DNS names of the desired servers. If you chose the Probe VPN Gateway (RDP) connection probing method, type the IP addresses or DNS names of the desired VPN gateways. You can clear a field by clicking Clear.

Setting Up a Dialup Modem

500

You can use a dialup modem as a primary or secondary Internet connection method. This is useful in locations where broadband Internet access is unavailable.

When used as a backup Internet connection, the modem can be automatically disconnected when not in use. For information on setting up a dialup backup connection, see ***Setting Up a Dialup Backup Connection*** on page 92.

To set up a dialup modem

1. Connect a regular or ISDN dialup modem to your Safe@Office appliance's serial port.

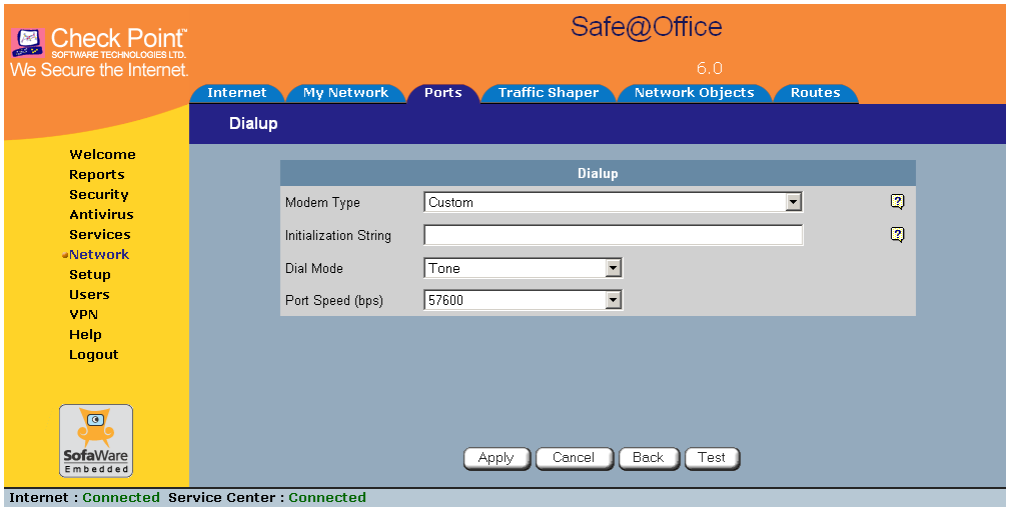
   For information on locating the serial port, see Rear Panel.

2. Click Network in the main menu, and click the Ports tab.

The Ports page appears.

3. In the RS232 drop-down list, select Dialup.
4. Click Apply.
5. Next to the RS232 drop-down list, click Setup.

The Dialup page appears.



6. Complete the fields using the information in the table below.
7. Click Apply.
8. To check that that the values you entered are correct, click Test.

   The Dialup page displays a message indicating whether the test succeeded.
9. Configure a Dialup Internet connection using the information in ***Using Internet Setup*** on page 63.

Table 11: Dialup Fields

In this field…	Do this…
Modem Type	Select the modem type. If you selected Custom, the Installation String field is enabled. Otherwise, it is filled in with the correct installation string for the modem type.
Initialization String	Type the installation string for the custom modem type. If you selected a standard modem type, this field is read-only.

In this field...	Do this...
Dial Mode	Select the dial mode the modem uses.
Port Speed	Select the modem's port speed (in bits per second).

Viewing Internet Connection Information

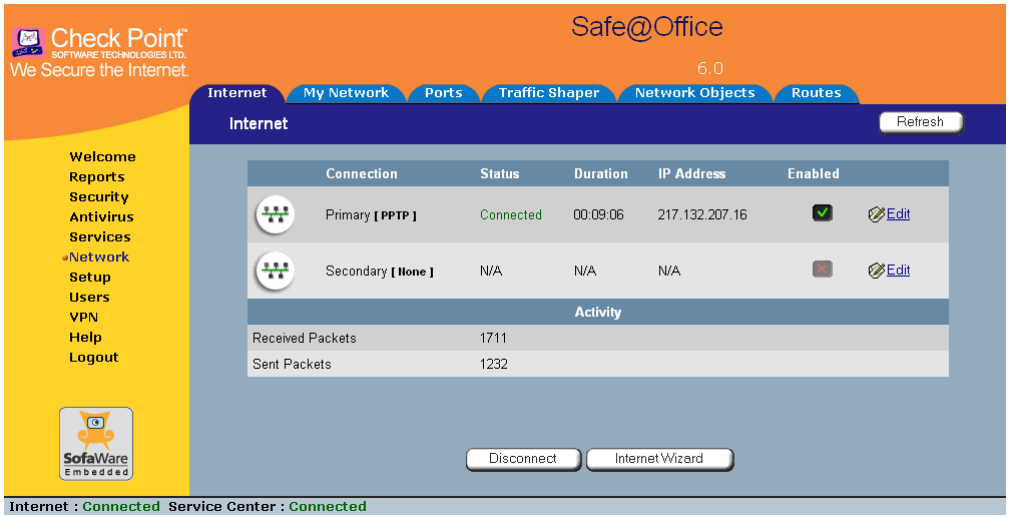
500

You can view information on your Internet connection(s) in terms of status, duration, and activity.

To view Internet connection information

1. Click Network in the main menu, and click the Internet tab.

   The Internet page appears.



   For an explanation of the fields on this page, see the table below.

2. To refresh the information on this page, click Refresh.

Table 12: Internet Page Fields

Field	Description
Status	Indicates the connection's status.
Duration	Indicates the connection duration, if active. The duration is given in the format hh:mm:ss, where: hh=hours mm=minutes ss=seconds
IP Address	Your IP address.
Enabled	Indicates whether or not the connection is enabled. For further information, see ***Enabling/Disabling the Internet Connection*** on page 88
Received Packets	The number of data packets received in the active connection.
Sent Packets	The number of data packets sent in the active connection.

Enabling/Disabling the Internet Connection

500

You can temporarily disable an Internet connection. This is useful if, for example, you are going on vacation and do not want to leave your computer connected to the Internet. If you have two Internet connections, you can force the Safe@Office appliance to use a particular connection, by disabling the other connection.

The Internet connection's Enabled/Disabled status is persistent through Safe@Office appliance reboots.

To enable/disable an Internet connection

1. Click Network in the main menu, and click the Internet tab.

   The Internet page appears.

2. Next to the Internet connection, do one of the following:

   - To enable the connection, click .

     The button changes to and the connection is enabled.

   - To disable the connection, click .

     The button changes to and the connection is disabled.

Using Quick Internet Connection/Disconnection

500

By clicking the Connect or Disconnect button (depending on the connection status) on the Internet page, you can establish a quick Internet connection using the currently-selected connection type. In the same manner, you can terminate the active connection.

The Internet connection retains its Connected/Not Connected status until the Safe@Office appliance is rebooted. The Safe@Office appliance then connects to the Internet if the connection is enabled. For information on enabling an Internet connection, see ***Enabling/Disabling the Internet Connection*** on page 88.

Configuring a Backup Internet Connection

You can configure both a primary and a secondary Internet connection. The secondary connection acts as a backup, so that if the primary connection fails, the Safe@Office appliance remains connected to the Internet.

Note: You can configure different DNS servers for the primary and secondary connections. The Safe@Office appliance acts as a DNS relay and routes requests from computers within the network to the appropriate DNS server for the active Internet connection.

Setting Up a LAN or Broadband Backup Connection

Using the Safe@Office Appliance's WAN Port

500

To set up a LAN or broadband backup Internet connection

1. Connect a hub or switch to the WAN port on your appliance's rear panel.
2. Connect your two modems or routers to the hub/switch.
3. Configure two Internet connections.

   For instructions, see ***Using Internet Setup*** on page 63.

Important: The two connections can be of different types. However, they cannot both be LAN DHCP connections.

Using the Safe@Office Appliance's DMZ/WAN2 Port

500

To set up a LAN or broadband backup Internet connection

1. Connect a modem to the DMZ/WAN2 port on your appliance's rear panel.
2. Click Network in the main menu, and click the Ports tab.

   The Ports page appears.
3. In the DMZ/WAN2 drop-down list, select WAN2.
4. Click Apply.
5. Configure two Internet connections.

   For instructions, see ***Using Internet Setup*** on page 63.

Setting Up a Dialup Backup Connection

500

If desired, you can use a dialup modem as the secondary Internet connection method. The Safe@Office appliance automatically dials the modem if the primary Internet connection fails.

To set up a dialup backup Internet connection

1. Setup a dialup modem.

   For instructions, see ***Setting Up a Dialup Modem*** on page 84.

2. Configure a LAN or broadband primary Internet connection.

   For instructions, see ***Using Internet Setup*** on page 63.

3. Configure a Dialup secondary Internet connection.

   For instructions, see ***Using Internet Setup*** on page 63.

Chapter 5

Managing Your Network

This chapter describes how to manage and configure your network connection and settings.

This chapter includes the following topics:

Configuring Network Settings

Warning: These are advanced settings. Do not change them unless it is necessary and you are qualified to do so.

Note: If you change the network settings to incorrect values and are unable to correct the error, you can reset the Safe@Office appliance to its default settings. See ***Resetting the Safe@Office appliance to Defaults*** on page 420.

Configuring a DHCP Server

500

By default, the Safe@Office appliance operates as a DHCP (Dynamic Host Configuration Protocol) server. This allows the Safe@Office appliance to automatically configure all the devices on your network with their network configuration details.

Note: The DHCP server only serves computers that are configured to obtain an IP address automatically. If a computer is not configured to obtain an IP address automatically, it is recommended to assign it an IP address outside of the DHCP address range. If you do assign it an IP address within the DHCP address range, the DHCP server will not assign this IP address to another computer.

If you already have a DHCP server in your internal network, and you want to use it instead of the Safe@Office DHCP server, you must disable the Safe@Office DHCP server, since you cannot have two DHCP servers or relays on the same network segment.

If you want to use a DHCP server on the Internet or via a VPN, instead of the Safe@Office DHCP server, you can configure DHCP relay. When in DHCP relay mode, the Safe@Office appliance relays information from the desired DHCP server to the devices on your network.

Note: You can perform DHCP reservation using network objects. For information, see ***Using Network Objects*** on page 129.

Enabling/Disabling the Safe@Office DHCP Server

500

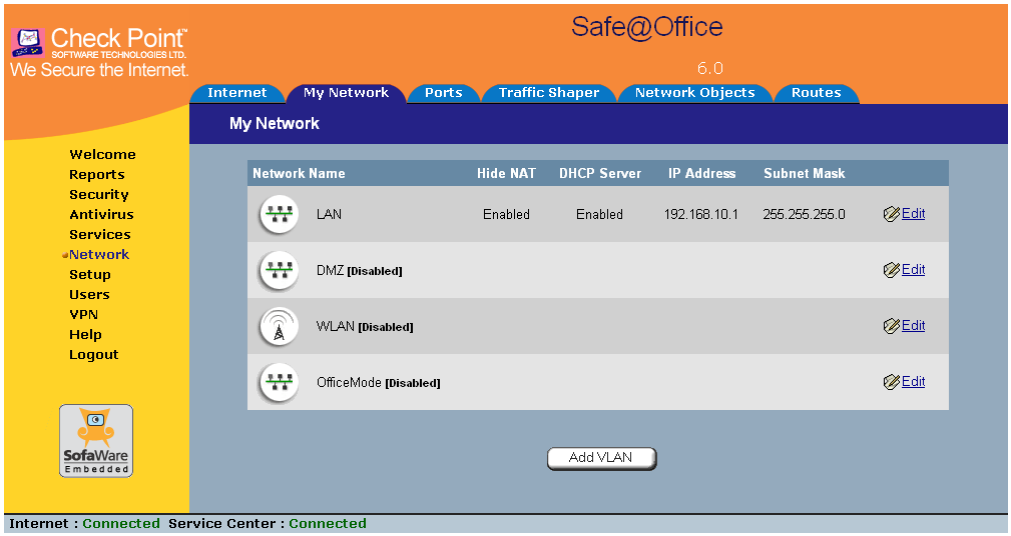
You can enable and disable the Safe@Office DHCP Server for internal networks.

Note: Enabling and disabling the DHCP Server is not available for the OfficeMode network.

To enable/disable the Safe@Office DHCP server

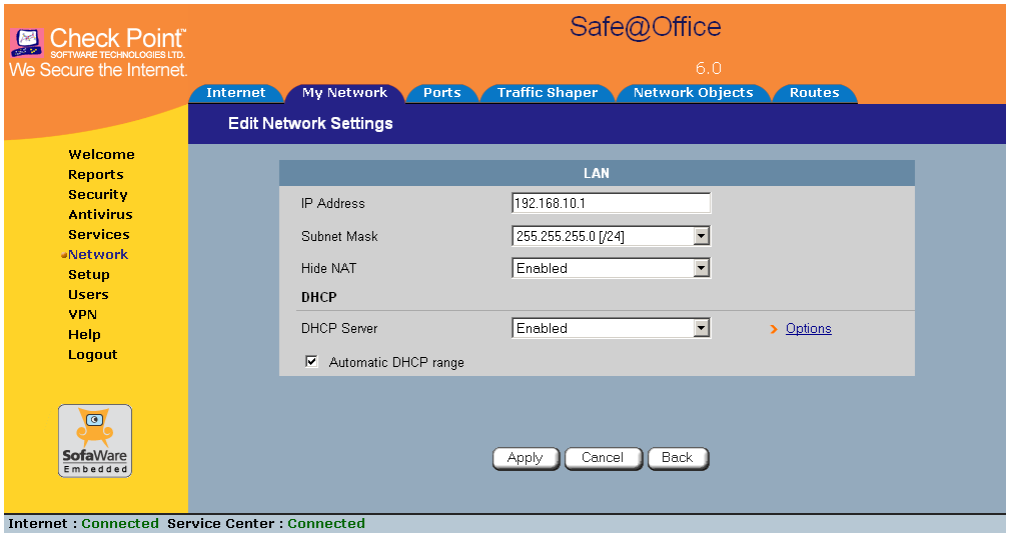
1. Click Network in the main menu, and click the My Network tab.

   The My Network page appears.



2. In the desired network's row, click Edit.

The **Edit Network Settings** page appears.



3. From the **DHCP Server** list, select **Enabled** or **Disabled**.
4. Click **Apply**.

   A warning message appears.
5. Click **OK**.

   A success message appears
6. If your computer is configured to obtain its IP address automatically (using DHCP), and either the Safe@Office DHCP server or another DHCP server is enabled, restart your computer.

   If you enabled the DHCP server, your computer obtains an IP address in the DHCP address range.

Configuring the DHCP Address Range

500

By default, the Safe@Office DHCP server automatically sets the DHCP address range. The DHCP address range is the range of IP addresses that the DHCP server can assign to network devices. IP addresses outside of the DHCP address range are reserved for statically addressed computers.

If desired, you can set the Safe@Office DHCP range manually.

Note: Setting the DHCP range manually is not available for the OfficeMode network.

To configure the DHCP address range

1. Click Network in the main menu, and click the My Network tab.

   The My Network page appears.

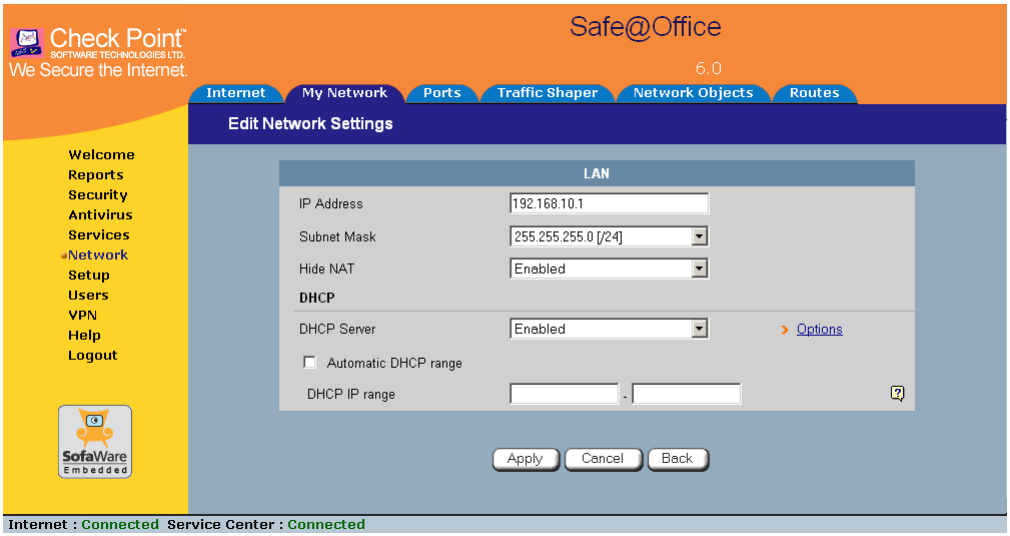
2. In the desired network's row, click Edit.

   The Edit Network Settings page appears.

3. To set the DHCP range manually:

   a. Clear the Automatic DHCP range check box.

The DHCP IP range fields appear.



b. In the DHCP IP range fields, type the desired DHCP range.

4. To allow the DHCP server to set the IP address range, select the Automatic DHCP range check box.

5. Click Apply.

   A warning message appears.

6. Click OK.

   A success message appears

7. If your computer is configured to obtain its IP address automatically (using DHCP), and either the Safe@Office DHCP server or another DHCP server is enabled, restart your computer.

   Your computer obtains an IP address in the new DHCP address range.

Configuring DHCP Relay

500

You can configure DHCP relay for internal networks.

Note: DHCP relay will not work if the appliance is located behind a NAT device.

Note: Configuring DHCP options is not available for the OfficeMode network.

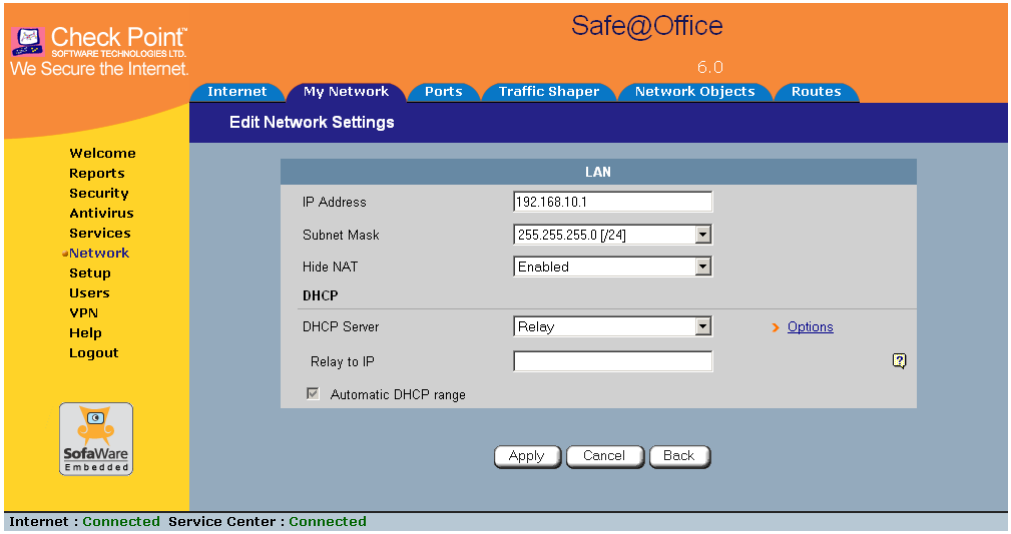
To configure DHCP relay

1. Click Network in the main menu, and click the My Network tab.

   The My Network page appears.
2. In the desired network's row, click Edit.

   The Edit Network Settings page appears.
3. In the DHCP Server list, select Relay.

The Automatic DHCP range check box is disabled, and the Relay to IP field appears.



4. In the Relay to IP field, type the IP address of the desired DHCP server.
5. Click Apply.

   A warning message appears.
6. Click OK.

   A success message appears
7. If your computer is configured to obtain its IP address automatically (using DHCP), and either the Safe@Office DHCP server or another DHCP server is enabled, restart your computer.

   Your computer obtains an IP address in the DHCP address range.

Configuring DHCP Server Options

500

If desired, you can configure the following custom DHCP options for an internal network:

- Domain suffix
- DNS servers
- WINS servers
- NTP servers
- VoIP call managers
- TFTP server and boot filename

Note: Configuring DHCP options is not available for the DMZ or VLANs.

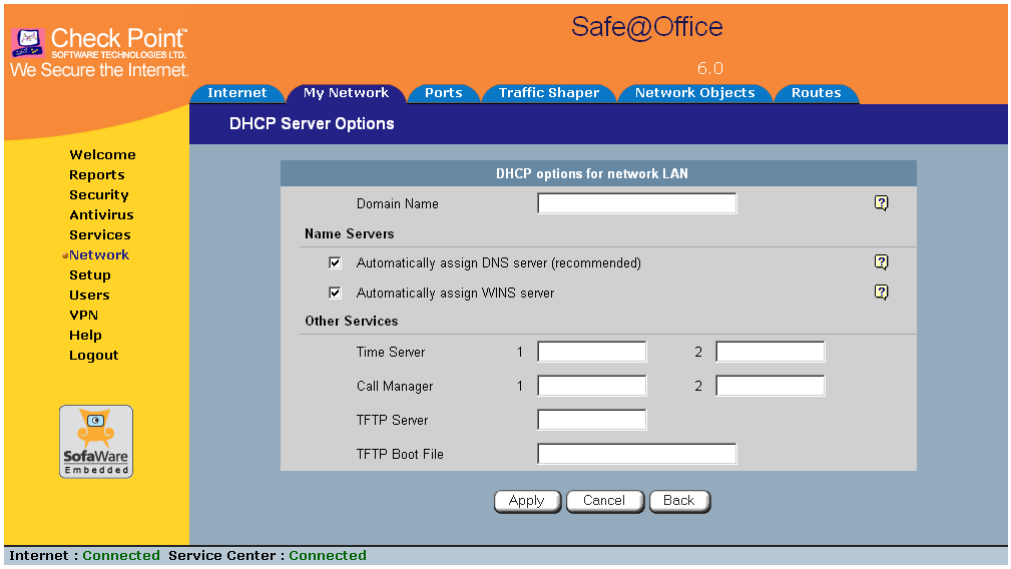
To configure DHCP options

1. Click Network in the main menu, and click the My Network tab.

   The My Network page appears.
2. In the desired network's row, click Edit.

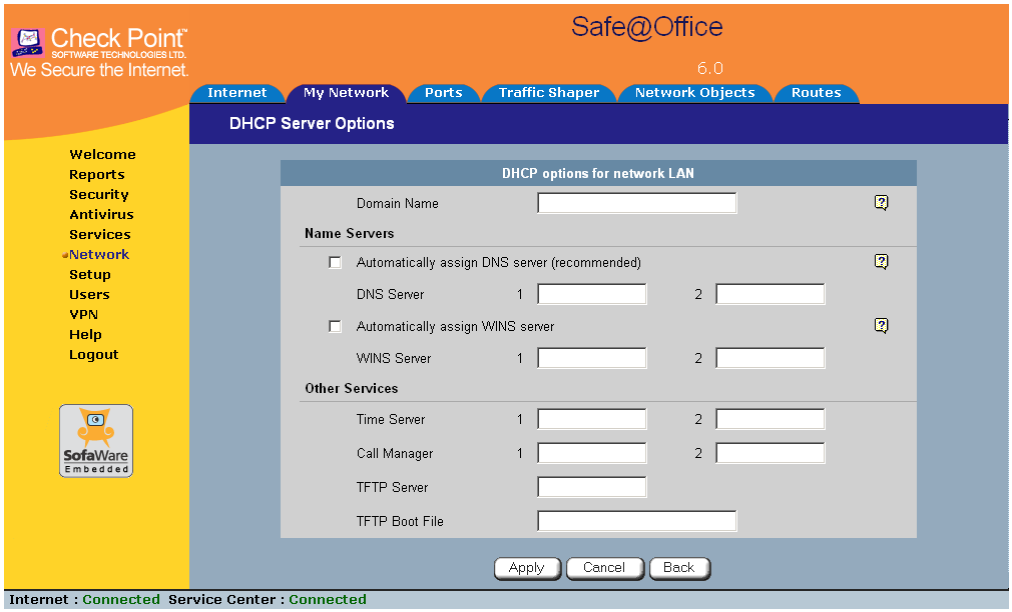
   The Edit Network Settings page appears.
3. In the DHCP area, click Options.

The DHCP Server Options page appears.



4. Complete the fields using the relevant information in the table below.

New fields appear, depending on the check boxes you selected.



5. Click **Apply**.
6. If your computer is configured to obtain its IP address automatically (using DHCP), restart your computer.

   Your computer obtains an IP address in the DHCP address range.

Table 13: DHCP Server Options Fields

In this field...	Do this...
Domain Name	Type a default domain suffix that should be passed to DHCP clients. The DHCP client will automatically append the domain suffix for the resolving of non-fully qualified names. For example, if the domain suffix is set to "mydomain.com", and the client tries to resolve the name “mail”, the suffix will be automatically appended to the name, resulting in “mail.mydomain.com”.

In this field…	Do this…
Name Servers	
Automatically assign DNS server (recommended)	Clear this option if you do not want the gateway to act as a DNS relay server and pass its own IP address to DHCP clients. Normally, it is recommended to leave this option selected. The DNS Server 1 and DNS Server 2 fields appear.
DNS Server 1, 2	Type the IP addresses of the Primary and Secondary DNS servers to pass to DHCP clients instead of the gateway.
Automatically assign WINS server	Clear this option if you do not want DHCP clients to be assigned the same WINS servers as specified by the Internet connection configuration (in the Internet Setup page). The WINS Server 1 and WINS Server 2 fields appear.
WINS Server 1, 2	Type the IP addresses of the Primary and Secondary WINS servers to use instead of the gateway.
Other Services	These fields are not available for the OfficeMode network.
Time Server 1, 2	To use Network Time Protocol (NTP) servers to synchronize the time on the DHCP clients, type the IP address of the Primary and Secondary NTP servers.
Call Manager 1, 2	To assign Voice over Internet Protocol (VoIP) call managers to the DHCP clients, type the IP address of the Primary and Secondary VoIP servers.

In this field…	Do this…
TFTP Server	Trivial File Transfer Protocol (TFTP) enables booting diskless computers over the network. To assign a TFTP server to the DHCP clients, type the IP address of the TFTP server.
TFTP Boot File	Type the boot file to use for booting DHCP clients via TFTP.

Changing IP Addresses

500

If desired, you can change your Safe@Office appliance's internal IP address, or the entire range of IP addresses in your internal network. You may want to perform these tasks if, for example, you are adding the Safe@Office appliance to a large existing network and don't want to change that network's IP address range, or if you are using a DHCP server other than the Safe@Office appliance, that assigns addresses within a different range.

To change IP addresses

1. Click Network in the main menu, and click the My Network tab.

   The My Network page appears.

2. In the LAN network's row, click Edit.

   The Edit Network Settings page appears.

3. To change the Safe@Office appliance's internal IP address, enter the new IP address in the IP Address field.

4. To change the internal network range, enter a new value in the Subnet Mask field.

Note: The internal network range is defined both by the Safe@Office appliance's internal IP address and by the subnet mask.

For example, if the Safe@Office appliance's internal IP address is 192.168.100.7, and you set the subnet mask to 255.255.255.0, the network's IP address range will be 192.168.100.1 – 192.168.100.254.

The default internal network range is 192.168.10.*.

5. Click Apply.

   A warning message appears.

6. Click OK.

   - The Safe@Office appliance's internal IP address and/or the internal network range are changed.
   - A success message appears.

7. Do one of the following:

   - If your computer is configured to obtain its IP address automatically (using DHCP), and the Safe@Office DHCP server is enabled, restart your computer.

     Your computer obtains an IP address in the new range.

   - Otherwise, manually reconfigure your computer to use the new address range using the TCP/IP settings. For information on configuring TCP/IP, see ***TCP/IP Settings*** on page 24, on page 20.

Enabling/Disabling Hide NAT

500

Hide Network Address Translation (Hide NAT) enables you to share a single public Internet IP address among several computers, by “hiding” the private IP addresses of the internal computers behind the Safe@Office appliance’s single Internet IP address.

Note: If Hide NAT is disabled, you must obtain a range of Internet IP addresses from your ISP. Hide NAT is enabled by default.

Note: Static NAT and Hide NAT can be used together.

To enable/disable Hide NAT

1. Click Network in the main menu, and click the My Network tab.

   The My Network page appears.
2. In the desired network's row, click Edit.

   The Edit Network Settings page appears.
3. From the Hide NAT list, select Enabled or Disabled.
4. Click Apply.

   A warning message appears.
5. Click OK.

   - If you chose to disable Hide NAT, it is disabled.
   - If you chose to enable Hide NAT, it is enabled.

Configuring a DMZ Network

500

In addition to the LAN network, you can define a second internal network called a DMZ (demilitarized zone) network.

For information on default security policy rules controlling traffic to and from the DMZ, see ***Default Security Policy*** on page 203.

To configure a DMZ network

1. Connect the DMZ computer to the DMZ port.

   If you have more than one computer in the DMZ network, connect a hub or switch to the DMZ port, and connect the DMZ computers to the hub.

2. Click Network in the main menu, and click the Ports tab.

   The Ports page appears.

3. In the DMZ drop-down list, select DMZ.
4. Click Apply.
5. Click Network in the main menu, and click the My Network tab.

   The My Network page appears.
6. In the DMZ network's row, click Edit.

   The Edit Network Settings page appears.
7. In the Mode drop-down list, select Enabled.

   The fields are enabled.
8. If desired, enable or disable Hide NAT.

   See ***Enabling/Disabling Hide NAT*** on page 107.
9. If desired, configure a DHCP server.

   See ***Configuring a DHCP Server*** on page 94.
10. In the IP Address field, type the IP address of the DMZ network's default gateway.

Note: The DMZ network must not overlap other networks.

11. In the Subnet Mask text box, type the DMZ’s internal network range.
12. Click Apply.

    A warning message appears.
13. Click OK.

    A success message appears.

Configuring the OfficeMode Network

500

By default, VPN Clients connect to the VPN Server using an Internet IP address locally assigned by an ISP. This may lead to the following problems:

- VPN Clients on the same network will be unable to communicate with each other via the Safe@Office Internal VPN Server. This is because their IP addresses are on the same subnet, and they therefore attempt to communicate directly over the local network, instead of through the secure VPN link.
- Some networking protocols or resources may require the client's IP address to be an internal one.

OfficeMode solves these problems by enabling the Safe@Office DHCP Server to automatically assign a unique local IP address to the VPN client, when the client connects and authenticates. The IP addresses are allocated from a pool called the *OfficeMode network*.

Note: OfficeMode requires Check Point SecureClient to be installed on the VPN clients. It is not supported by Check Point SecuRemote.

When OfficeMode is not supported by the VPN client, traditional mode will be selected used instead.

To configure the OfficeMode network

1. Click Network in the main menu, and click the My Network tab.

   The My Network page appears.

2. In the OfficeMode network's row, click Edit.

   The Edit Network Settings page appears.

3. In the Mode drop-down list, select Enabled.

   The fields are enabled.

4. In the IP Address field, type the IP address to use as the OfficeMode network's default gateway.

Note: The OfficeMode network must not overlap other networks.

5. In the Subnet Mask text box, type the OfficeMode internal network range.
6. If desired, enable or disable Hide NAT.

   See ***Enabling/Disabling Hide NAT*** on page 107.
7. If desired, configure DHCP options.

   See ***Configuring DHCP Server Options*** on page 101.
8. Click Apply.

   A warning message appears.
9. Click OK.

   A success message appears.

Configuring VLANs

Power Pack

Your Safe@Office appliance allows you partition your network into several virtual LAN networks (VLANs). A VLAN is a logical network behind the Safe@Office appliance. Computers in the same VLAN behave as if they were on the same physical network: traffic flows freely between them, without passing through a firewall. In contrast, traffic between a VLAN and other networks passes through the firewall and is subject to the security policy. By default, traffic from a VLAN to any other internal network (including other VLANs) is blocked. In this way, defining VLANs can increase security and reduce network congestion.

For example, you can assign each division within your organization to a different VLAN, regardless of their physical location. The members of a division will be able to communicate with each other and share resources, and only members who need to communicate with other divisions will be allowed to do so. Furthermore,

you can easily transfer a member of one division to another division without rewiring your network, by simply reassigning them to the desired VLAN.

The Safe@Office appliance supports the following VLAN types:

- Tag-based

  In tag-based VLAN you use one of the gateway's ports as a 802.1Q VLAN trunk, connecting the appliance to a VLAN-aware switch. Each VLAN behind the trunk is assigned an identifying number called a "VLAN ID", also referred to as a "VLAN tag". All outgoing traffic from a tag-based VLAN contains the VLAN's tag in the packet headers. Incoming traffic to the VLAN must contain the VLAN's tag as well, or the packets are dropped. Tagging ensures that traffic is directed to the correct VLAN.

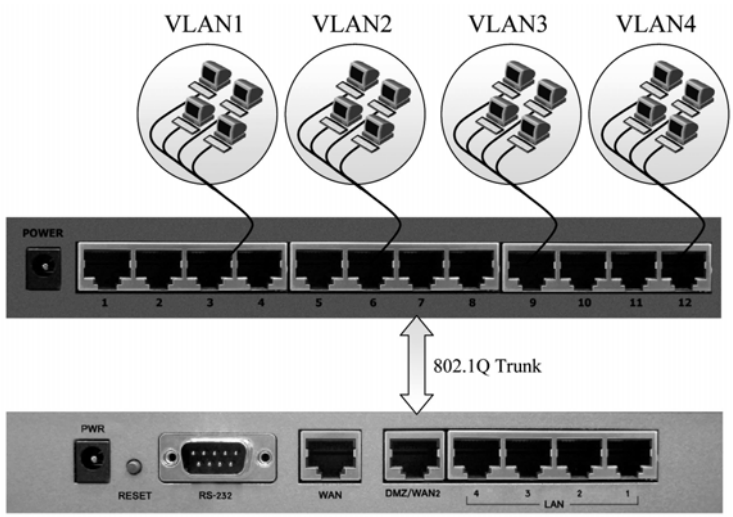


Figure 10: Tag-based VLAN

- Port-based

  Port-based VLAN allows assigning the appliance's LAN ports to VLANs, effectively transforming the appliance's four-port switch into up to four firewall-isolated security zones. You can assign multiple ports to the same VLAN, or each port to a separate VLAN.

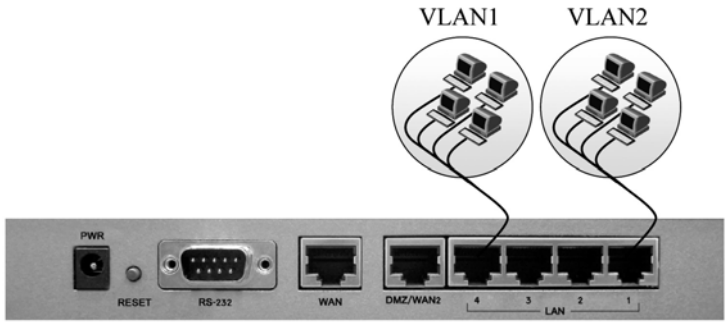


Figure 11: Port-based VLAN

Port-based VLAN does not require an external VLAN-capable switch, and is therefore simpler to use than tag-based VLAN. However, port-based VLAN is limited, because the appliance's internal switch has only four ports.

You can define up to ten VLAN networks (port-based and tag-based combined).

For information on the default security policy for VLANs, see ***Default Security Policy*** on page 203.

Adding and Editing Port-Based VLANs

Power Pack

To add or edit a port-based VLAN

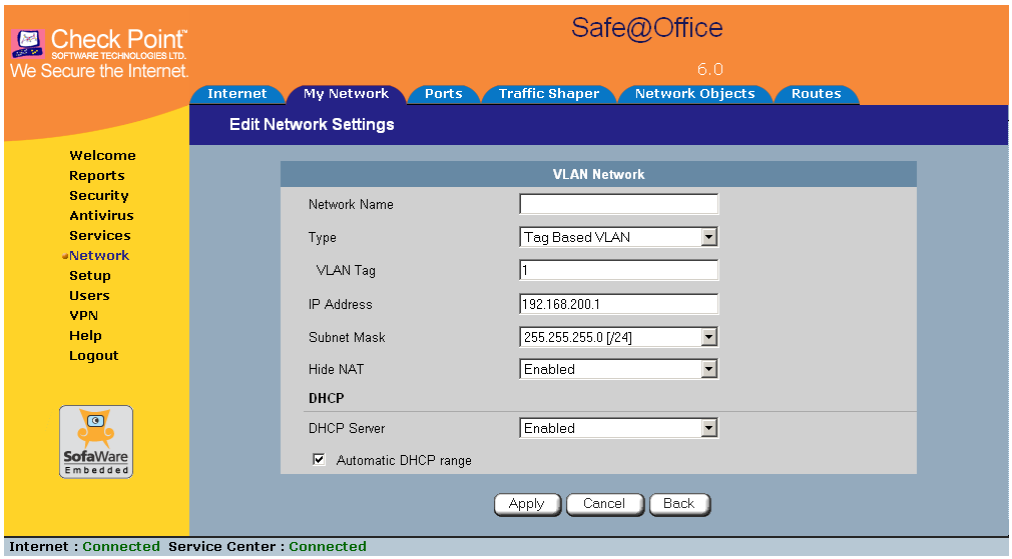
1. Click Network in the main menu, and click the My Network tab.

   The My Network page appears.

2. Do one of the following:

   - To add a VLAN site, click Add VLAN.
   - To edit a VLAN site, click Edit in the desired VLAN's row.

   The Edit Network Settings page for VLAN networks appears.



3. In the Network Name field, type a name for the VLAN.
4. In the Type drop-down list, select Port Based VLAN.

   The VLAN Tag field disappears.

5. In the IP Address field, type the IP address of the VLAN network's default gateway.

Note: The VLAN network must not overlap other networks.

6. In the Subnet Mask field, type the VLAN's internal network range.
7. If desired, enable or disable Hide NAT.

   See ***Enabling/Disabling Hide NAT*** on page 107.

8. If desired, configure a DHCP server.

   See ***Configuring a DHCP Server*** on page 94.

9. Click Apply.

   A warning message appears.

10. Click OK.

    A success message appears.

11. Click Network in the main menu, and click the Ports tab.

    The Ports page appears.

12. In the drop-down list next to the LAN port you want to assign, select the VLAN network's name.

    You can assign more than one port to the VLAN.

13. Click Apply.

Adding and Editing Tag-Based VLANs

Power Pack

To add or edit a tag-based VLAN

1. Click Network in the main menu, and click the My Network tab.

   The My Network page appears.

2. Do one of the following:

   - To add a VLAN site, click Add VLAN.
   - To edit a VLAN site, click Edit in the desired VLAN's row.

   The Edit Network Settings page for VLAN networks appears.

3. In the Network Name field, type a name for the VLAN.
4. In the Type drop-down list, select Tag Based VLAN.

   The VLAN Tag field appears.

5. In the VLAN Tag field, type a tag for the VLAN.

   This must be an integer between 1 and 4095.

6. In the IP Address field, type the IP address of the VLAN network's default gateway.

Note: The VLAN network must not overlap other networks.

7. In the Subnet Mask field, type the VLAN's internal network range.
8. If desired, enable or disable Hide NAT.

   See ***Enabling/Disabling Hide NAT*** on page 107.

9. If desired, configure a DHCP server.

   See ***Configuring a DHCP Server*** on page 94.

10. Click Apply.

    A warning message appears.

11. Click OK.

    A success message appears.

12. Click Network in the main menu, and click the Ports tab.

    The Ports page appears.

13. In the DMZ/WAN2 drop-down list, select VLAN Trunk.

14. Click Apply.

    The DMZ/WAN2 port now operates as a VLAN Trunk port. In this mode, it will not accept untagged packets.

15. Configure a VLAN trunk (802.1Q) port on the VLAN-aware switch, according to the vendor instructions. Define the same VLAN IDs on the switch.

16. Connect the Safe@Office appliance's DMZ/WAN2 port to the VLAN-aware switch's VLAN trunk port.

Deleting VLANs

Power Pack

To delete a VLAN

1. If the VLAN is port-based, do the following:
   a. Click Network in the main menu, and click the Ports tab.

      The Ports page appears.
   b. Remove all port assignments to the VLAN, by selecting other networks in the drop-down lists.
   c. Click Apply.
2. Click Network in the main menu, and click the My Network tab.

   The My Network page appears.
3. In the desired VLAN's row, click the Erase icon.

   A confirmation message appears.
4. Click OK.

   The VLAN is deleted.

Configuring High Availability

Power Pack

You can create a High Availability (HA) cluster consisting of two or more Safe@Office appliances. For example, you can install two Safe@Office appliances on your network, one acting as the “Master”, the default gateway through which all network traffic is routed, and one acting as the “Backup”. If the Master fails, the Backup automatically and transparently takes over all the roles of the Master. This ensures that your network is consistently protected by a Safe@Office appliance and connected to the Internet.

The gateways in a HA cluster each have a separate IP address within the local network. In addition, the gateways share a single virtual IP address, which is the default gateway address for the local network. Control of the virtual IP address is passed as follows:

1. Each gateway is assigned a priority, which determines the gateway's role: the gateway with the highest priority is the Active Gateway and uses the virtual IP address, and the rest of the gateways are Passive Gateways.
2. The Active Gateway sends periodic signals, or “heartbeats”, to the network via a synchronization interface.

   The synchronization interface can be any internal network existing on both gateways except the WLAN.
3. If the heartbeat from the Active Gateway stops (indicating that the Active gateway has failed), the gateway with the highest priority becomes the new Active Gateway and takes over the virtual IP address.
4. When a gateway that was offline comes back online, or a gateway's priority changes, the gateway sends a heartbeat notifying the other gateways in the cluster.

   If the gateway's priority is now the highest, it becomes the Active Gateway.

The Safe@Office appliance supports Internet connection tracking, which means that each appliance tracks its Internet connection's status and reduces its own

priority by a user-specified amount, if its Internet connection goes down. If the Active Gateway's priority drops below another gateway's priority, then the other gateway becomes the Active Gateway.

Note: You can force a fail-over to a passive Safe@Office appliance. You may want to do this in order to verify that HA is working properly, or if the active Safe@Office appliance needs repairs. To force a fail-over, switch off the primary box or disconnect it from the LAN network.

The Safe@Office appliance supports configuring multiple HA clusters on the same network segment. To this end, each cluster must be assigned a unique ID number.

When HA is configured, you can specify that only the Active Gateway in the cluster should connect to the Internet. This is called WAN HA, and it is useful in the following situations:

- Your Internet subscription cost is based is on connection time, and therefore having the Passive appliance needlessly connected to the Internet costs you money.
- You want multiple appliances to share the same static IP address without creating an IP address conflict.

WAN HA avoids an IP address change, and thereby ensures virtually uninterrupted access from the Internet to internal servers at your network.

Before configuring HA, the following requirements must be met:

- You must have at least two identical Safe@Office appliances.
- The appliances must have identical firmware versions and firewall rules.
- The appliances' internal networks must be the same.
- The appliances must have *different* real internal IP addresses, but share *the same* virtual IP address.
- The appliances' synchronization interface ports must be connected either directly, or via a hub or a switch. For example, if the DMZ is the synchronization interface, then the DMZ/WAN2 ports on the appliances must be connected to each other.

  The synchronization interface need not be dedicated for synchronization only. It may be shared with an active internal network.

You can configure HA for any internal network, except the OfficeMode network.

Note: You can enable the DHCP server in all Safe@Office appliances. A Passive Gateway's DHCP server will start answering DHCP requests only if the Active Gateway fails.

Note: If you configure HA for the WLAN network:

- A passive appliance's wireless transmitter will be disabled until the gateway becomes active.
- The two WLAN networks can share the same SSID and wireless frequency.
- The WLAN interface cannot serve as the synchronization interface.

Configuring High Availability on a Gateway

Power Pack

The following procedure explains how to configure HA on a single gateway. You must perform this procedure on each Safe@Office appliance that you want to include in the HA cluster.

To configure HA on a Safe@Office appliance

1. Set the appliance's internal IP addresses and network range.

   Each appliance must have a different internal IP address.

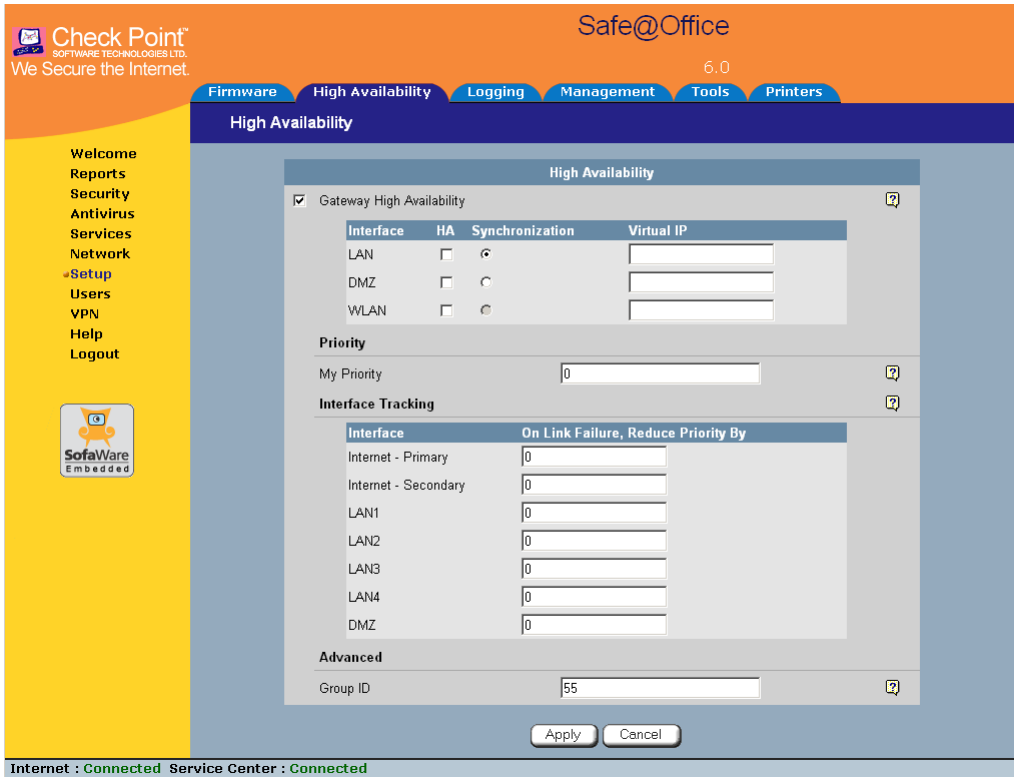
   See ***Changing IP Addresses*** on page 105.

2. Click Setup in the main menu, and click the High Availability tab.

   The High Availability page appears.

3. Select the Gateway High Availability check box.

The fields are enabled.



4. Next to each network for which you want to enable HA, select the HA check box.
5. In the Virtual IP field, type the default gateway IP address.

   This can be any unused IP address in the network, and must be the same for all gateways.
6. Click the Synchronization radio button next to the network you want to use as the synchronization interface.

   You can choose any network listed except the WLAN.

Note: The synchronization interface must be the same for all gateways, and must always be connected and enabled on all gateways. Otherwise, multiple appliances may become active, causing unpredictable problems.

7. Complete the fields using the information the table below.
8. Click Apply.

   A success message appears.
9. If desired, configure WAN HA for both the primary and secondary Internet connection.

   This setting should be the same for all gateways. For further information, see ***Using Internet Setup*** on page 63.

Table 14: High Availability Page Fields

In this field…	Do this…
Priority	
My Priority	Type the gateway's priority. This must be an integer between 1 and 255.
Interface Tracking	
Internet - Primary	Type the amount to reduce the gateway's priority if the primary Internet connection goes down. This must be an integer between 0 and 255.

In this field…	Do this…
Internet - Secondary	Type the amount to reduce the gateway's priority if the secondary Internet connection goes down. This must be an integer between 0 and 255. Note: This value is only relevant if you configured a backup connection. For information on configuring a backup connection, see ***Configuring a Backup Internet Connection*** on page 90.
LAN1/2/3/4	Type the amount to reduce the gateway's priority if the LAN port's Ethernet link is lost.
DMZ	Type the amount to reduce the gateway's priority if the DMZ / WAN2 port's Ethernet link is lost.
Advanced	
Group ID	If multiple HA clusters exist on the same network segment, type the ID number of the cluster to which the gateway should belong. This must be an integer between 1 and 255. The default value is 55. If only one HA cluster exists, there is no need to change this value.

Sample Implementation on Two Gateways

Power Pack

The following procedure illustrates how to configure HA for the following two Safe@Office gateways, Gateway A and Gateway B:

Table 15: Gateway Details

	Gateway A	Gateway B
Internal Networks	LAN, DMZ	LAN, DMZ
Internet Connections	Primary and secondary	Primary only
LAN Network IP Address	192.169.100.1	192.169.100.2
LAN Network Subnet Mask	255.255.255.0	255.255.255.0
DMZ Network IP Address	192.169.101.1	192.169.101.2
DMZ Network Subnet Mask	255.255.255.0	255.255.255.0

The gateways have two internal networks in common, LAN and DMZ. This means that you can configure HA for the LAN network, the DMZ network, or both. You can use either of the networks as the synchronization interface.

The procedure below shows how to configure HA for both the LAN and DMZ networks. The synchronization interface is the DMZ network, the LAN virtual IP address is 192.168.100.3, and the DMZ virtual IP address is 192.168.101.3. Gateway A is the Active Gateway.

To configure HA for Gateway A and Gateway B

1. Connect the LAN port of Gateways A and B to hub 1.

2. Connect the DMZ port of Gateways A and B to hub 2.
3. Connect the LAN network computers of Gateways A and B to hub 1.
4. Connect the DMZ network computers of Gateways A and B to hub 2.
5. Do the following on Gateway A:
   a. Set the gateway's internal IP addresses and network range to the values specified in the table above.

      See ***Changing IP Addresses*** on page 105.
   b. Click Setup in the main menu, and click the High Availability tab.

      The High Availability page appears.
   c. Select the Gateway High Availability check box.

      The Gateway High Availability area is enabled. The LAN and DMZ networks are listed.
   d. Next to LAN, select the HA check box.
   e. In the LAN network's Virtual IP field, type the default gateway IP address 192.168.100.3.
   f. Next to DMZ, select the HA check box.
   g. In the DMZ network's Virtual IP field, type the default gateway IP address 192.168.101.3.
   h. Click the Synchronization radio button next to DMZ.
   i. In the My Priority field, type "100".

      The high priority means that Gateway A will be the Active Gateway.
   j. In the Internet - Primary field, type "20".

      Gateway A will reduce its priority by 20, if its primary Internet connection goes down.
   k. In the Internet - Secondary field, type "30".

Gateway A will reduce its priority by 30, if its secondary Internet connection goes down.

l. Click Apply.

A success message appears.

6. Do the following on Gateway B:

a. Set the gateway's internal IP addresses and network range to the values specified in the table above.

See ***Changing IP Addresses*** on page 105.

b. Click Setup in the main menu, and click the High Availability tab.

The High Availability page appears.

c. Select the Gateway High Availability check box.

The Gateway High Availability area is enabled. The LAN and DMZ networks are listed.

d. Next to LAN, select the HA check box.

e. In the LAN network's Virtual IP field, type the default gateway IP address 192.168.100.3.

f. Next to DMZ, select the HA check box.

g. In the DMZ network's Virtual IP field, type the default gateway IP address 192.168.101.3.

h. Click the Synchronization radio button next to DMZ.

i. In the My Priority field, type "60".

The low priority means that Gateway B will be the Passive Gateway.

j. In the Internet - Primary field, type "20".

Gateway B will reduce its priority by 20, if its Internet connection goes down.

k. Click Apply.

A success message appears.

Gateway A's priority is 100, and Gateway B's priority is 60. So long as one of Gateway A's Internet connections is up, Gateway A is the Active Gateway, because its priority is higher than that of Gateway B.

If both of Gateway A's Internet connections are down, it deducts from its priority 20 (for the primary connection) and 30 (for the secondary connection), reducing its priority to 50. In this case, Gateway B's priority is the higher priority, and it becomes the Active Gateway.

500

You can add individual computers or networks as network objects. This enables you to configure various settings for the computer or network represented by the network object.

You can configure the following settings for a network object:

- Static NAT (or One-to-One NAT)

  Static NAT allows the mapping of Internet IP addresses or address ranges to hosts inside the internal network. This is useful if you want a computer in your private network to have its own Internet IP address. For example, if you have both a mail server and a Web server in your network, you can map each one to a separate Internet IP address.

  Static NAT rules do not imply any security rules. To allow incoming traffic to a host for which you defined Static NAT, you must create an Allow rule. When specifying firewall rules for such hosts, use the host’s internal IP address, and not the Internet IP address to which the internal IP address is mapped. For further information, see ***Using Rules*** on page 209.

Note: Static NAT and Hide NAT can be used together.

Note: The Safe@Office appliance supports Proxy ARP (Address Resolution Protocol). When an external source attempts to communicate with such a computer, the Safe@Office appliance automatically replies to ARP queries with its own MAC address, thereby enabling communication. As a result, the Static NAT Internet IP addresses appear to external sources to be real computers connected to the WAN interface.

- Assign the network object's IP address to a MAC address

  Normally, the Safe@Office DHCP server consistently assigns the same IP address to a specific computer. However, if the Safe@Office DHCP server runs out of IP addresses and the computer is down, then the DHCP server may reassign the IP address to a different computer.

  If you want to guarantee that a particular computer's IP address remains constant, you can reserve the IP address for use by the computer's MAC address only. This is called *DHCP reservation*, and it is useful if you are hosting a public Internet server on your network.

- Secure HotSpot enforcement

  In Safe@Office 500 with Power Pack, you can specify whether or not to exclude the network object from HotSpot enforcement. Excluded network objects will be able to access the network without viewing the My HotSpot page. For further information on Secure HotSpot, see ***Configuring Secure HotSpot*** on page 256.

Adding and Editing Network Objects

500

You can add or edit network objects via:

- The Network Objects page

  This page enables you to add both individual computers and networks.

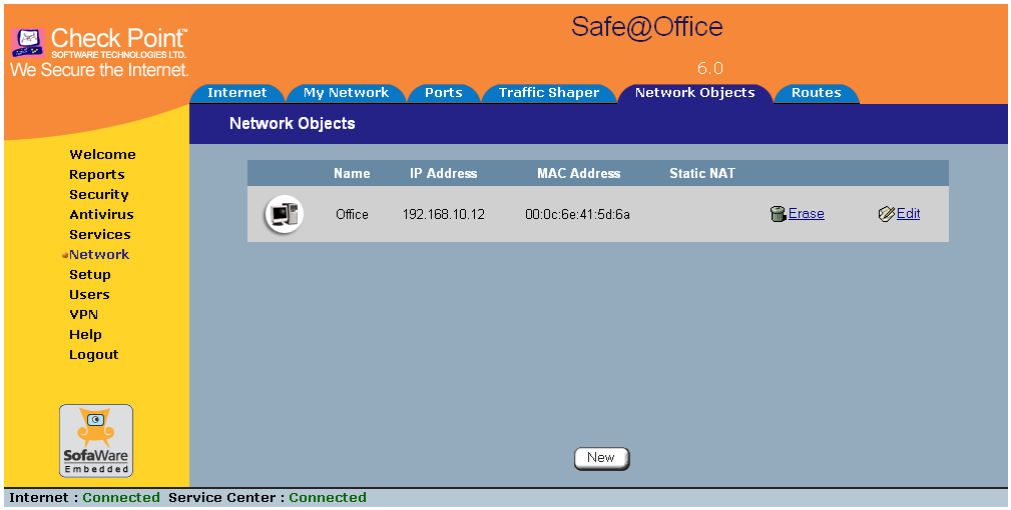
- The Active Computers page

  This page enables you to add only individual computers as network objects. The computer's details are filled in automatically in the wizard.

To add or edit a network object via the Network Objects page

1. Click Network in the main menu, and click the Network Objects tab.

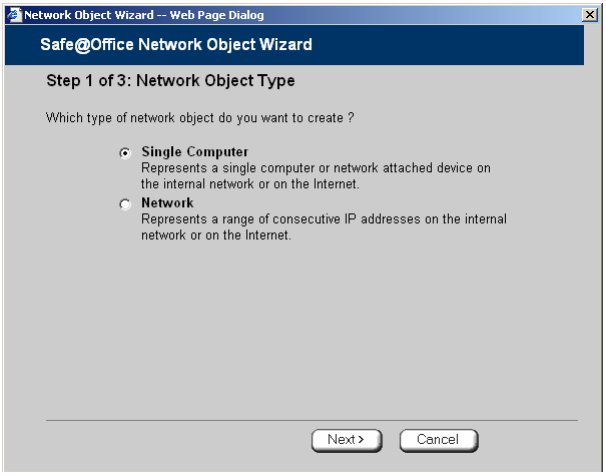
   The Network Objects page appears with a list of network objects.



2. Do one of the following:

   - To add a network object, click New.
   - To edit an existing network object, click Edit next to the desired computer in the list.

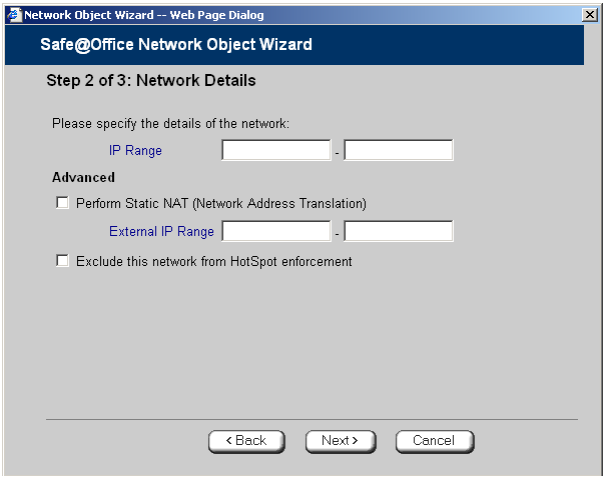
The Safe@Office Network Object Wizard opens, with the Step 1: Network Object Type dialog box displayed.



3. Do one of the following:
   - To specify that the network object should represent a single computer or device, click Single Computer.
   - To specify that the network object should represent a network, click Network.
4. Click Next.

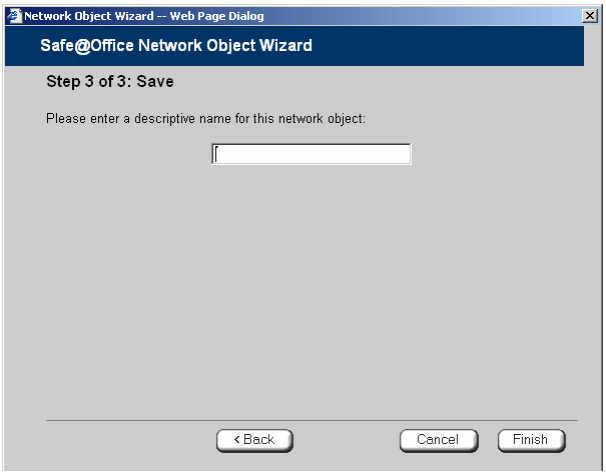
The **Step 2: Computer Details** dialog box appears. If you chose **Single Computer**, the dialog box includes the **Perform Static NAT** option.

If you chose **Network**, the dialog box does not include this option.



5. Complete the fields using the information in the tables below.
6. Click **Next**.

The Step 3: Save dialog box appears.



7. Type a name for the network object in the field.
8. Click Finish.

To add or edit a network object via the Active Computers page

1. Click Reports in the main menu, and click the Active Computers tab.

The Active Computers page appears.

If a computer has not yet been added as a network object, the Add button appears next to it. If a computer has already been added as a network object, the Edit button appears next to it.

2. Do one of the following:

   - To add a network object, click Add next to the desired computer.
   - To edit a network object, click Edit next to the desired computer.

   The Safe@Office Network Object Wizard opens, with the Step 1: Network Object Type dialog box displayed.

3. Do one of the following:

   - To specify that the network object should represent a single computer or device, click Single Computer.

- To specify that the network object should represent a network, click Network.

4. Click Next.

   The Step 2: Computer Details dialog box appears.

   The computer's IP address and MAC address are automatically filled in.

5. Complete the fields using the information in the tables below.
6. Click Next.

   The Step 3: Save dialog box appears with the network object's name. If you are adding a new network object, this name is the computer's name.

7. To change the network object name, type the desired name in the field.
8. Click Finish.

   The new object appears in the Network Objects page.

Table 16: Network Object Fields for a Single Computer

In this field…	Do this…
IP Address	Type the IP address of the local computer, or click This Computer to specify your computer.
Reserve a fixed IP address for this computer	Select this option to assign the network object's IP address to a MAC address, and to allow the network object to connect to the WLAN when MAC Filtering is used. For information about MAC Filtering, see ***Configuring a Wireless Network*** on page 161.
MAC Address	Type the MAC address you want to assign to the network object's IP address, or click This Computer to specify your computer's MAC address.
Perform Static NAT (Network Address Translation)	Select this option to map the local computer's IP address to an Internet IP address. You must then fill in the External IP field.
External IP	Type the Internet IP address to which you want to map the local computer's IP address.
Exclude this computer from HotSpot enforcement	Select this option to exclude the network object from HotSpot enforcement.

Table 17: Network Object Fields for a Network

In this field…	Do this…
IP Range	Type the range of local computer IP addresses in the network.
Perform Static NAT (Network Address Translation)	Select this option to map the network's IP address range to a range of Internet IP addresses of the same size. You must then fill in the External IP Range field.
External IP Range	Type the Internet IP address range to which you want to map the network's IP address range.
Exclude this network from HotSpot enforcement	Select this option to exclude this network from HotSpot enforcement.

Viewing and Deleting Network Objects

500

To view or delete a network object

1. Click Network in the main menu, and click the Network Objects tab.

   The Network Objects page appears with a list of network objects.
2. To delete a network object, do the following:

   a. In the desired network object's row, click the Erase icon.

      A confirmation message appears.

   b. Click OK.

      The network object is deleted.

Using Static Routes

500

A static route is a setting that explicitly specifies the route for packets originating in a certain subnet and/or destined for a certain subnet. Packets with a source and destination that does not match any defined static route will be routed to the default gateway. To modify the default gateway, see ***Using a LAN Connection*** on page 65.

A static route can be based on the packet's destination IP address, or based on the source IP address, in which case it is a source route.

Source routing can be used, for example, for load balancing between two Internet connections. For example, if you have an Accounting department and a Marketing department, and you want each to use a different Internet connection for outgoing traffic, you can add a static route specifying that traffic originating from the Accounting department should be sent via WAN1, and another static route specifying that traffic originating from the Marketing department should be sent via WAN2.

The Static Routes page lists all existing routes, including the default, and indicates whether each route is currently "Up" (reachable) or not.

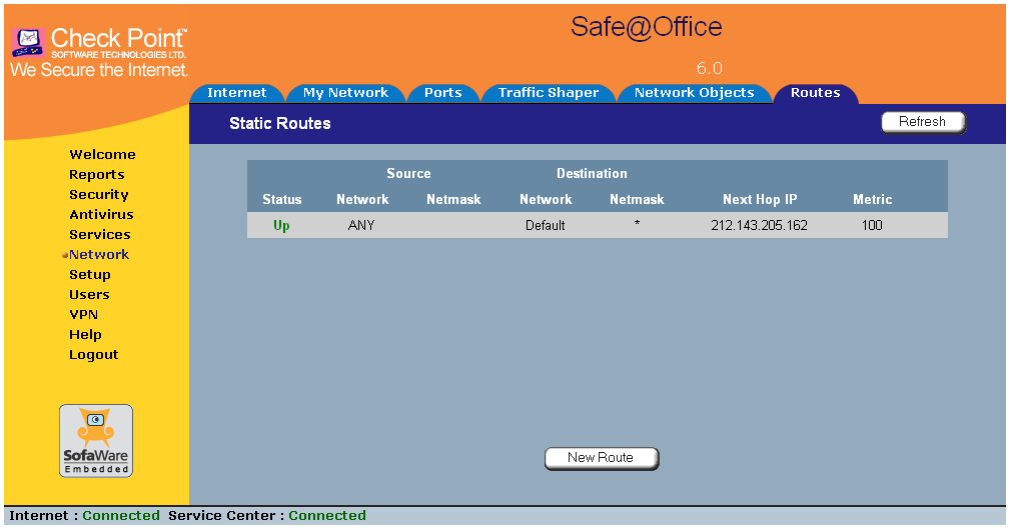
Adding and Editing Static Routes

500

To add a static route

1. Click Network in the main menu, and click the Routes tab.

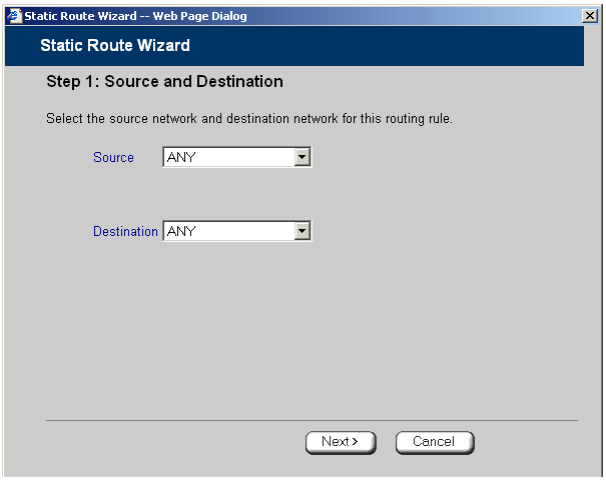
The **Static Routes** page appears, with a list of existing static routes.



2. Do one of the following:

   - To add a static route, click **New Route**.
   - To edit an existing static route, click **Edit** next to the desired route in the list.

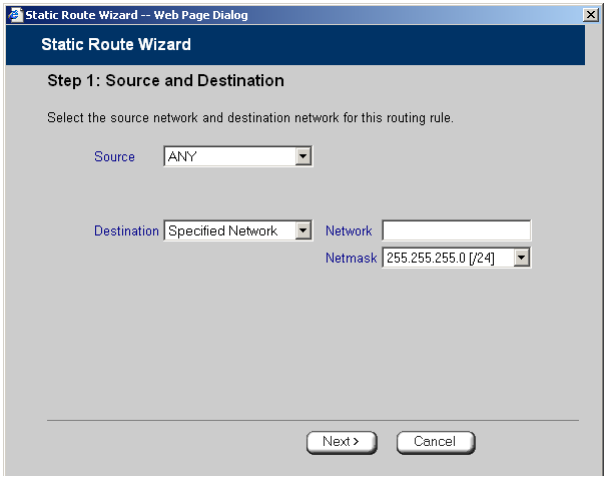
The **Static Route Wizard** opens displaying the **Step 1: Source and Destination** dialog box.



3. To select a specific source network (source routing), do the following:

   a) In the **Source** drop-down list, select **Specified Network**.

   New fields appear.



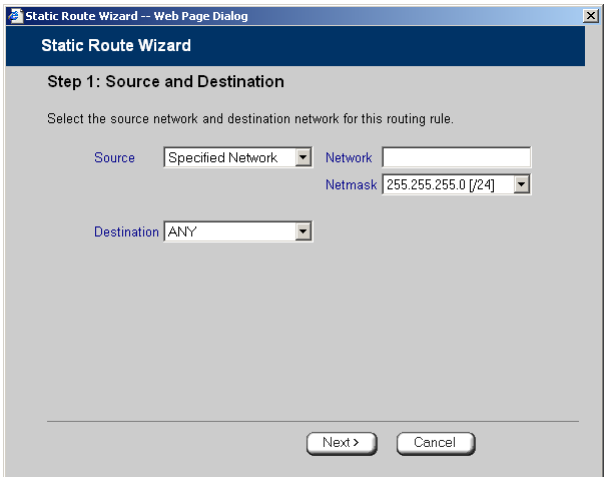
   b) In the **Network** field, type the IP address of the source network.

c) In the **Netmask** drop-down list, select the subnet mask.

4. To select a specific destination network, do the following:

a) In the **Destination** drop-down list, select **Specified Network**.

New fields appear.

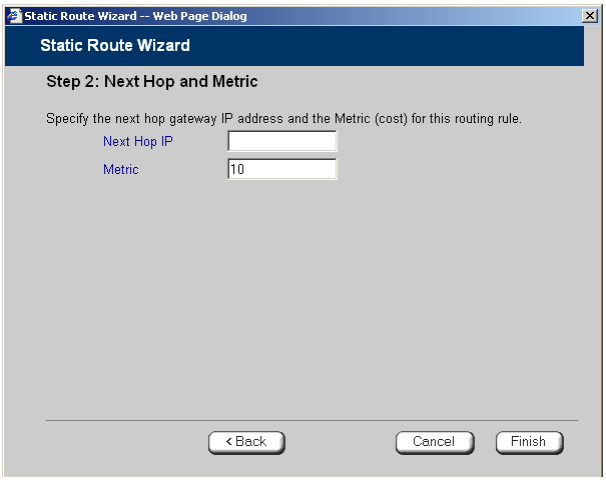


b) In the **Network** field, type the IP address of the destination network.

c) In the **Netmask** drop-down list, select the subnet mask.

5. Click **Next**.

The **Step 2: Next Hop and Metric** dialog box appears.

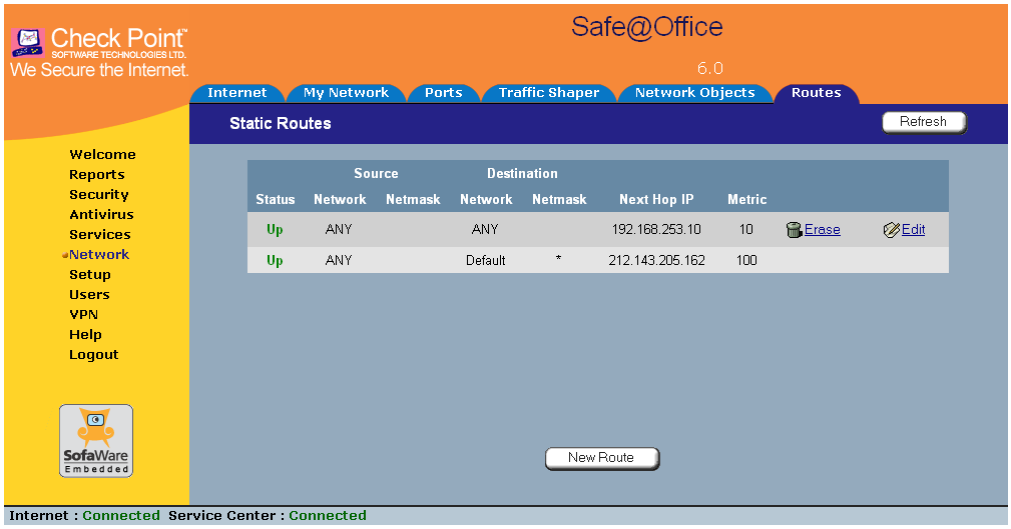


6. In the **Next Hop IP** field, type the IP address of the gateway (next hop router) to which to route the packets destined for this network.
7. In the **Metric** field, type the static route's metric.

   The gateway sends a packet to the route that matches the packet's destination and has the lowest metric.

   The default value is 10.
8. Click **Next**.

The new static route is saved.



Viewing and Deleting Static Routes

500

Note: The “default” route cannot be deleted.

To delete a static route

1. Click Network in the main menu, and click the Routes tab.

   The Static Routes page appears, with a list of existing static routes.

2. In the desired route row, click the Erase icon.

   A confirmation message appears.

3. Click OK.

   The route is deleted.

Managing Ports

500

The Safe@Office appliance enables you to quickly and easily assign its ports to different uses, as shown in the table below. Furthermore, you can restrict each port to a specific link speed and duplex setting.

Table 18: Ports and Assignments

You can assign this port...	To these uses...
LAN	LAN network
	VLAN network
DMZ/WAN2	DMZ network
	Second WAN connection
	VLAN trunk
RS232	Dialup modem
	Serial console

Viewing Port Statuses

500

You can view the status of the Safe@Office appliance's ports on the Ports page, including each Ethernet connection's duplex state. This is useful if you need to check whether the appliance's physical connections are working, and you can't see the LEDs on front of the appliance.

Note: In the Safe@Office 500 model SBX-166LHG-2, status information is only available for the WAN and DMZ ports, and not for LAN ports 1-4.

To view port statuses

1. Click Network in the main menu, and click the Ports tab.

   The Ports page appears.

   The following information is displayed for each enabled port:

- Assign To. The port's current assignment. For example, if the DMZ/WAN2 port is currently used for the DMZ, the drop-down list displays "DMZ".
- Link Configuration. The configured link speed (10 Mbps or 100 Mbps) and duplex (Full Duplex or Half Duplex) configured for the port.

  Automatic Detection indicates that the port is configured to automatically detect the link speed and duplex.
- Status. The detected link speed and duplex.

  No Link indicates that the appliance does not detect anything connected to the port.

  Disabled indicates that the port is disabled. For example, if the DMZ/WAN2 port is currently assigned to the DMZ, but the DMZ is disabled, the port is marked as such.

2. To refresh the display, click Refresh.

Modifying Port Assignments

500

You can assign ports to different networks or purposes. Since modifying port assignments often requires additional configurations, use the table below to determine which procedure you should use:

Table 19: Modifying Port Assignments

To assign a port to...	See...
LAN	The procedure below
VLAN or VLAN Trunk	***Configuring VLANs*** on page 111

To assign a port to...	See...
WAN2	***Setting Up a LAN or Broadband Backup Connection*** on page 91
DMZ	Configuring a DMZ Network
Console	***Using a Console*** on page 390
Modem	***Setting Up a Dialup Modem*** on page 84

To modify a port assignment

1. Click Network in the main menu, and click the Ports tab.

   The Ports page appears.

   In the Assigned To drop-down list to the right of the port, select the desired port assignment.

2. Click Apply.

   The port is reassigned to the specified network or purpose.

Modifying Link Configurations

500

By default, the Safe@Office automatically detects the link speed and duplex. If desired, you can manually restrict the Safe@Office appliance's ports to a specific link speed and duplex.

Note: In the Safe@Office 500 model SBX-166LHG-2, restricting the link speed and duplex is available for the WAN and DMZ ports, and not for LAN ports 1-4.

To modify a port's link configuration

1. Click Network in the main menu, and click the Ports tab.

   The Ports page appears.

2. In the Link Configuration drop-down list to the right of the port, do one of the following:

   - Select the desired link speed and duplex.
   - Select Automatic Detection to configure the port to automatically detect the link speed and duplex.

     This is the default.

3. Click Apply.

   The port uses the specified link speed and duplex.

Resetting Ports to Defaults

500

You can reset the Safe@Office appliance's ports to their default link configurations ("Automatic Detection") and default assignments (shown in the table below).

Table 20: Default Port Assignments

Port	Default Assignment
1-4	LAN
DMZ / WAN2	DMZ
WAN	This port is always assigned to the WAN.
RS232	Modem

To reset ports to defaults

1. Click Network in the main menu, and click the Ports tab.

   The Ports page appears.

2. Click Default.

   A confirmation message appears.

3. Click OK.

   The ports are reset to their default assignments and to "Automatic Detection" link configuration.

   All currently-established connections that are not supported by the default settings may be broken. For example, if you were using the DMZ/WAN2 port as WAN2, the port reverts to its DMZ assignment, and the secondary Internet connection moves to the WAN port.

Chapter 6

Using Traffic Shaper

This chapter describes how to use Traffic Shaper to control the flow of communication to and from your network.

This chapter includes the following topics:

Overview

Traffic Shaper is a bandwidth management solution that allows you to set bandwidth policies to control the flow of communication. Traffic Shaper ensures that important traffic takes precedence over less important traffic, so that your business can continue to function with minimum disruption, despite network congestion.

Traffic Shaper uses Stateful Inspection technology to access and analyze data derived from all communication layers. This data is used to classify traffic in Quality of Service (QoS) classes. Traffic Shaper divides available bandwidth among the classes according to weight. For example, suppose Web traffic is deemed three times as important as FTP traffic, and these services are assigned weights of 30 and 10 respectively. If the lines are congested, Traffic Shaper will maintain the ratio of bandwidth allocated to Web traffic and FTP traffic at 3:1.

If a specific class is not using all of its bandwidth, the leftover bandwidth is divided among the remaining classes, in accordance with their relative weights. In the example above, if only one Web and one FTP connection are active and they are competing, the Web connection will receive 75% (30/40) of the leftover

bandwidth, and the FTP connection will receive 25% (10/40) of the leftover bandwidth. If the Web connection closes, the FTP connection will receive 100% of the bandwidth.

Each class has a bandwidth limit, which is the maximum amount of bandwidth that connections belonging to that class may use together. Once a class has reached its bandwidth limit, connections belonging to that class will not be allocated further bandwidth, even if there is unused bandwidth available. For example, traffic used by Peer-To-Peer file-sharing applications may be limited to a specific rate, such as 512 kilobit per second. Each class also has a "Delay Sensitivity" value, indicating whether connections belonging to the class should be given precedence over connections belonging to other classes.

Your Safe@Office appliance offers different degrees of traffic shaping, depending on its model:

- Simplified Traffic Shaper. Includes a fixed set of four predefined classes. You can assign network traffic to each class, but you cannot modify the classes, delete them, or create new classes. Available in Safe@Office 500.
- Advanced Traffic Shaper. Includes a set of four predefined classes, but enables you to modify the classes, delete them, and create new classes. You can define up to eight classes, including weight, bandwidth limits, and DiffServ (Differentiated Services) Packet Marking parameters. DiffServ marks packets as belonging to a certain Quality of Service class. These packets are then granted priority on the public network according to their class. Available in Safe@Office 500 with Power Pack.

Note: You can prioritize wireless traffic from WMM-compliant multimedia applications, by enabling Wireless Multimedia (WMM) for the WLAN network. See ***Manually Configuring a WLAN*** on page 165.

Setting Up Traffic Shaper

500

To set up Traffic Shaper

1. Enable Traffic Shaper for the Internet connection, using the procedure ***Using Internet Setup*** on page 63.

   You can enable Traffic Shaper for incoming or outgoing connections.

   - When enabling Traffic Shaper for outgoing traffic:

     Specify a rate (in kilobits/second) slightly lower than your Internet connection's maximum measured upstream speed.

   - When enabling Traffic Shaper for incoming traffic:

     Specify a rate (in kilobits/second) slightly lower than your Internet connection's maximum measured downstream speed.

   It is recommended to try different rates in order to determine which ones provide the best results.

   Note: Traffic Shaper cannot control the number or type of packets it receives from the Internet; it can only affect the rate of incoming traffic by dropping received packets. This makes the shaping of inbound traffic less accurate than the shaping of outbound traffic. It is therefore recommended to enable traffic shaping for incoming traffic only if necessary.

2. If you are using Safe@Office 500 with Power Pack, you can add QoS classes that reflect your communication needs, or modify the four predefined QoS classes.

   See ***Adding and Editing Classes*** on page 155.

   Note: If you are using Safe@Office 500, you have Simplified Traffic Shaper, and you cannot add or modify the classes. To add or modify classes, upgrade to Safe@Office 500 with Power Pack, which supports Advanced Traffic Shaper.

3. Use Allow or Allow and Forward rules to assign different types of connections to QoS classes.

   For example, if Traffic Shaper is enabled for outgoing traffic, and you create an Allow rule associating all outgoing VPN traffic with the Urgent QoS class, then Traffic Shaper will handle outgoing VPN traffic as specified in the bandwidth policy for the Urgent class.

   See ***Adding and Editing Rules*** on page 213.

Note: Traffic Shaper must be enabled for the direction of traffic specified in the rule.

Note: If you do not assign a connection type to a class, Traffic Shaper automatically assigns the connection type to the predefined "Default" class.

Predefined QoS Classes

500

Traffic Shaper provides the following predefined QoS classes.

To assign traffic to these classes, define firewall rules as described in ***Using Rules*** on page 209.

Table 21: Predefined QoS Classes

Class	Weight	Delay Sensitivity	Useful for
Default	10	Medium (Normal Traffic)	Normal traffic. All traffic is assigned to this class by default.
Urgent	15	High (Interactive Traffic)	Traffic that is highly sensitive to delay. For example, IP telephony, videoconferencing, and interactive protocols that require quick user response, such as telnet.

Class	Weight	Delay Sensitivity	Useful for
Important	20	Medium (Normal Traffic)	Normal traffic
Low Priority	5	Low (Bulk Traffic)	Traffic that is not sensitive to long delays. For example, SMTP traffic (outgoing email).

In Simplified Traffic Shaper, these classes cannot be changed.

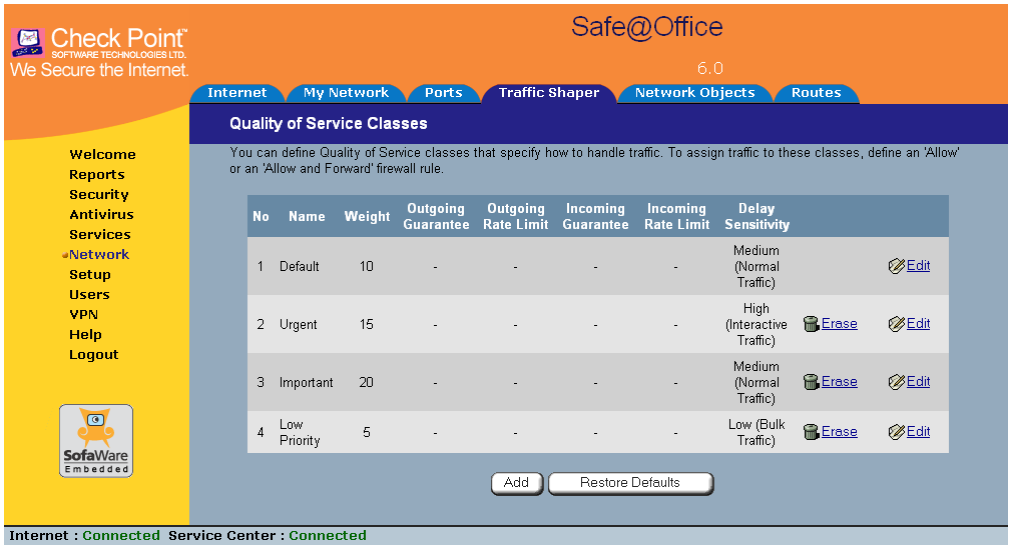
Adding and Editing Classes

Power Pack

To add or edit a QoS class

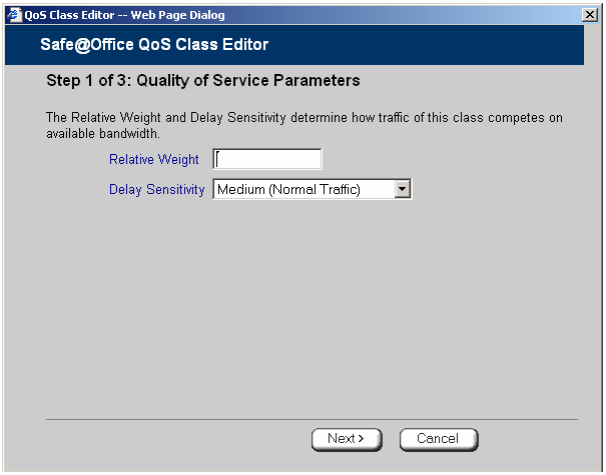
1. Click Network in the main menu, and click the Traffic Shaper tab.

   The Quality of Service Classes page appears.



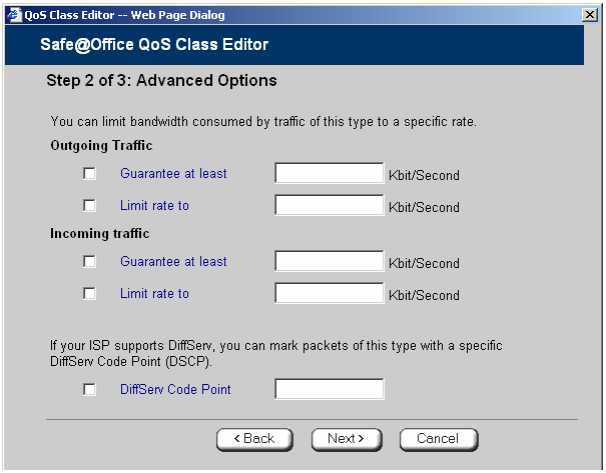
2. Click Add.

The **Safe@Office QoS Class Editor** wizard opens, with the **Step 1 of 3: Quality of Service Parameters** dialog box displayed.



3. Complete the fields using the relevant information in the table below.
4. Click **Next**.

   The **Step 2 of 3: Advanced Options** dialog box appears.

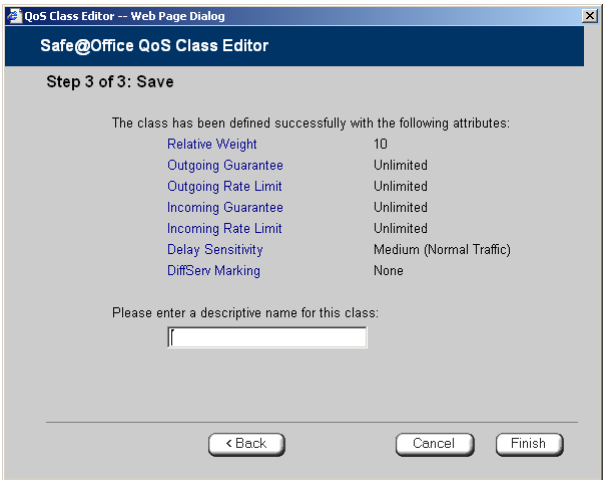


5. Complete the fields using the relevant information in the table below.

Note: Traffic Shaper may not enforce guaranteed rates and relative weights for incoming traffic as accurately as for outgoing traffic. This is because Traffic Shaper cannot control the number or type of packets it receives from the Internet; it can only affect the rate of incoming traffic by dropping received packets. It is therefore recommended to enable traffic shaping for incoming traffic only if necessary. For information on enabling Traffic Shaper for incoming and outgoing traffic, see ***Using Internet Setup*** on page 63.

6. Click Next.

   The Step 3 of 3: Save dialog box appears with a summary of the class.



7. Type a name for the class.

   For example, if you are creating a class for high priority Web connections, you can name the class "High Priority Web".

8. Click Finish.

   The new class appears in the Quality of Service Classes page.

Table 22: QoS Class Fields

In this field...	Do this...
Relative Weight	Type a value indicating the class's importance relative to the other defined classes. For example, if you assign one class a weight of 100, and you assign another class a weight of 50, the first class will be allocated twice the amount of bandwidth as the second when the lines are congested.
Delay Sensitivity	Select the degree of precedence to give this class in the transmission queue: • Low (Bulk Traffic) - Traffic that is not sensitive to long delays. For example, SMTP traffic (outgoing email). • Medium (Normal Traffic) - Normal traffic • High (Interactive Traffic) - Traffic that is highly sensitive to delay. For example, IP telephony, videoconferencing, and interactive protocols that require quick user response, such as telnet. Traffic Shaper serves delay-sensitive traffic with a lower latency. That is, Traffic Shaper attempts to send packets with a "High (Interactive Traffic)" level before packets with a "Medium (Normal Traffic)" or "Low (Bulk Traffic)" level.
Outgoing Traffic: Guarantee At Least	Select this option to guarantee a minimum bandwidth for outgoing traffic belonging to this class. Then type the minimum bandwidth (in kilobits/second) in the field provided.
Outgoing Traffic: Limit rate to	Select this option to limit the rate of outgoing traffic belonging to this class. Then type the maximum rate (in kilobits/second) in the field provided.
Incoming Traffic: Guarantee At Least	Select this option to guarantee a minimum bandwidth for incoming traffic belonging to this class. Then type the minimum bandwidth (in kilobits/second) in the field provided.

In this field...	Do this...
Incoming Traffic: Limit rate to	Select this option to limit the rate of incoming traffic belonging to this class. Then type the maximum rate (in kilobits/second) in the field provided.
DiffServ Code Point	Select this option to mark packets belonging to this class with a DiffServ Code Point (DSCP), which is an integer between 0 and 63. Then type the DSCP in the field provided. The marked packets will be given priority on the public network according to their DSCP. To use this option, your ISP or private WAN must support DiffServ. You can obtain the correct DSCP value from your ISP or private WAN administrator.

Deleting Classes

Power Pack

You cannot delete a class that is currently used by a rule. You can determine whether a class is in use or not, by viewing the Rules page.

To delete an existing QoS class

1. Click Network in the main menu, and click the Traffic Shaper tab.

   The Quality of Service Classes page appears.

2. Click the Erase icon of the class you wish to delete.

   A confirmation message appears.

3. Click OK.

   The class is deleted.

Restoring Traffic Shaper Defaults

Power Pack

If desired, you can reset the Traffic Shaper bandwidth policy to use the four predefined classes, and restore these classes to their default settings. For information on these classes and their defaults, see ***Predefined QoS Classes*** on page 154.

Note: This will delete any additional classes you defined in Traffic Shaper and reset all rules to use the Default class.

If one of the additional classes is currently used by a rule, you cannot reset Traffic Shaper to defaults. You can determine whether a class is in use or not, by viewing the Rules page.

To restore Traffic Shaper defaults

1. Click Network in the main menu, and click the Traffic Shaper tab.

   The Quality of Service Classes page appears.

2. Click Restore Defaults.

   A confirmation message appears.

3. Click OK.

Chapter 7

Configuring a Wireless Network

This chapter describes how to set up a wireless internal network.

This chapter includes the following topics:

Overview

In addition to the LAN and DMZ networks, you can define a wireless internal network called a WLAN (wireless LAN) network, when using Safe@Office 500W.

For information on default security policy rules controlling traffic to and from the WLAN, see ***Default Security Policy*** on page 203.

You can configure a WLAN network in either of the following ways:

- Wireless Configuration Wizard. Guides you through the WLAN setup step by step.

  See ***Using the Wireless Configuration Wizard*** on page 176.

- Manual configuration. Offers advanced setup options.

  See ***Manually Configuring a WLAN*** on page 165.

Note: It is recommended to configure the WLAN via Ethernet and not via a wireless connection, because the wireless connection could be broken after making a change to the configuration.

About the Wireless Hardware in Your Safe@Office 500W Appliance

Your Safe@Office 500W appliance features a built-in 802.11b/g access point that is tightly integrated with the firewall and hardware-accelerated VPN.

Safe@Office 500W supports the latest 802.11g standard (up to 54Mbps) and is backwards compatible with the older 802.11b standard (up to 11Mbps), so that both new and old adapters of these standards are interoperable. Safe@Office 500W also supports a special Super G mode that allows reaching a throughput of up to 108Mbps with Super G compatible stations. For more information on the Super G mode refer to: http://www.super-ag.com.

Safe@Office 500W transmits in 2.4GHz range, using dual diversity antennas to increase the range. In addition, the Safe@Office 500W supports a special extended range (XR) mode that allows up to three times the range of a regular 802.11g access point. XR dramatically stretches the performance of a wireless LAN, by enabling long-range connections. The architecture delivers receive sensitivities of up to 105dBm, over 20 dB more than the 802.11 specification. This allows ranges of up to 300 meters indoors, and up to 1 km (3200 ft) outdoors, with XR-enabled wireless stations (actual range depends on environment).

Wireless Security Protocols

The Safe@Office wireless security appliance supports the following security protocols:

Table 23: Wireless Security Protocols

Security Protocol	Description
None	No security method is used. This option is not recommended, because it allows unauthorized users to access your WLAN network, although you can still limit access from the WLAN by creating firewall rules. This method is suitable for creating public access points.
WEP encryption	In the WEP (Wired Equivalent Privacy) encryption security method, wireless stations must use a pre-shared key to connect to your network. This method is not recommended, due to known security flaws in the WEP protocol. It is provided for compatibility with existing wireless deployments. Note: The appliance and the wireless stations must be configured with the same WEP key.
802.1X: RADIUS authentication, no encryption	In the 802.1x security method, wireless stations (supplicants) attempting to connect to the access point (authenticator) must first be authenticated by a RADIUS server (authentication server) which supports 802.1x . All messages are passed in EAP (Extensible Authentication Protocol). This method is recommended for situations in which you want to authenticate wireless users, but do not need to encrypt the data. Note: To use this security method, you must first configure a RADIUS server. See ***Using RADIUS Authentication.*** on page 370

Security Protocol	Description
WPA: RADIUS authentication, encryption	The WPA (Wi-Fi Protected Access) security method uses MIC (message integrity check) to ensure the integrity of messages, and TKIP (Temporal Key Integrity Protocol) to enhance data encryption. Furthermore, WPA includes 802.1x and EAP authentication, based on a central RADIUS authentication server. This method is recommended for situations where you want to authenticate wireless stations using a RADIUS server, and to encrypt the transmitted data. Note: To use this security method, you must first configure a RADIUS server which supports 802.1x. See ***Using RADIUS Authentication.*** on page 370
WPA-PSK: password authentication, encryption	The WPA-PSK security method is a variation of WPA that does not require an authentication server. WPA-PSK periodically changes and authenticates encryption keys. This is called *rekeying*. This option is recommended for small networks, which want to authenticate and encrypt wireless data, but do not want to install a RADIUS server. Note: The appliance and the wireless stations must be configured with the same passphrase.
WPA2 (802.11i)	The WPA2 security method uses the more secure Advanced Encryption Standard (AES) cipher, instead of the RC4 cipher used by WPA and WEP. When using WPA or WPA-PSK security methods, the Safe@Office enables you to restrict access to the WLAN network to wireless stations that support the WPA2 security method. If this setting is not selected, the Safe@Office appliance allows clients to connect using both WPA and WPA2.

Note: For increased security, it is recommended to enable the Safe@Office internal VPN Server for users connecting from your internal networks, and to install SecuRemote on each computer in the WLAN. This ensures that all connections from the WLAN to the LAN are encrypted and authenticated. For information, see ***Internal VPN Server*** on page 306 and ***Setting Up Your Safe@Office Appliance as a VPN Server*** on page 307.

Manually Configuring a WLAN

500W

To manually configure a WLAN network

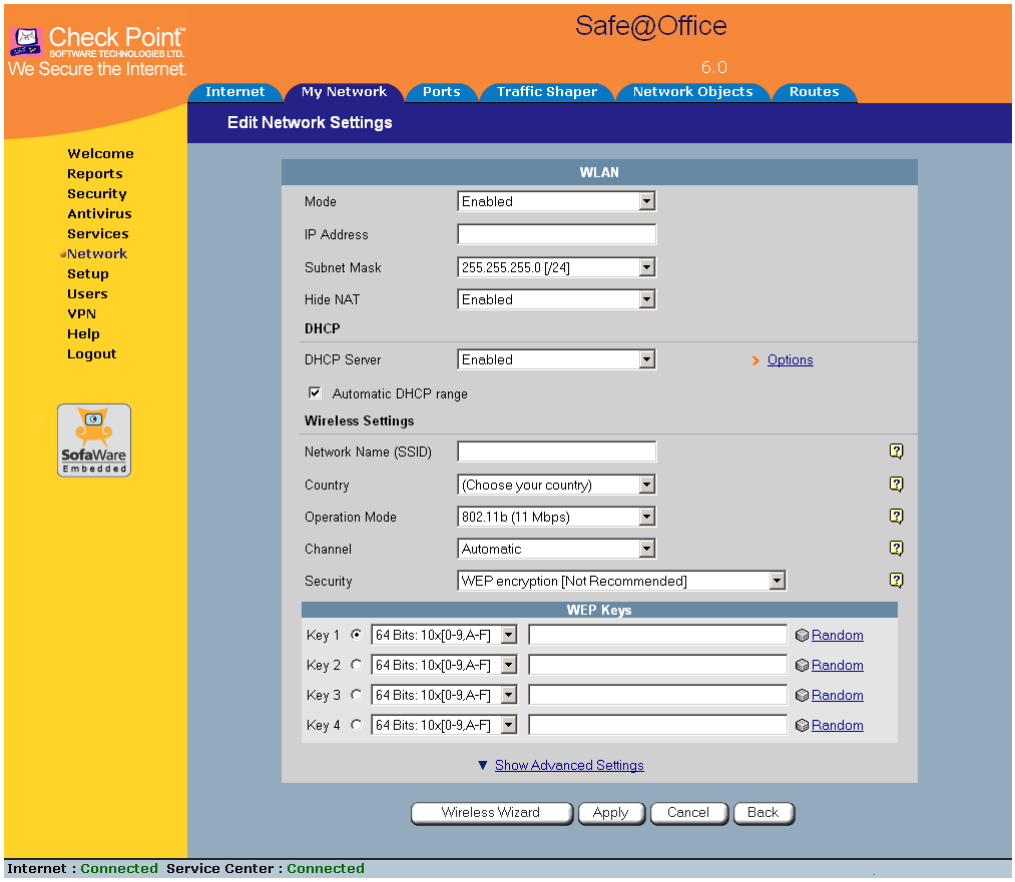
1. Prepare the appliance for a wireless connection as described in ***Network Installation*** on page 35.
2. If you want to use 802.1X or WPA security mode for the WLAN, configure a RADIUS server.

   For information on security modes, see ***Basic WLAN Settings Fields*** on page 168.

   For information on configuring RADIUS servers, see ***Using RADIUS Authentication*** on page 370.
3. Click Network in the main menu, and click the My Network tab.

   The My Network page appears.
4. In the WLAN network's row, click Edit.

The **Edit Network Settings** page appears.



5. In the **Mode** drop-down list, select **Enabled**.

   The fields are enabled.

6. If desired, enable or disable Hide NAT.

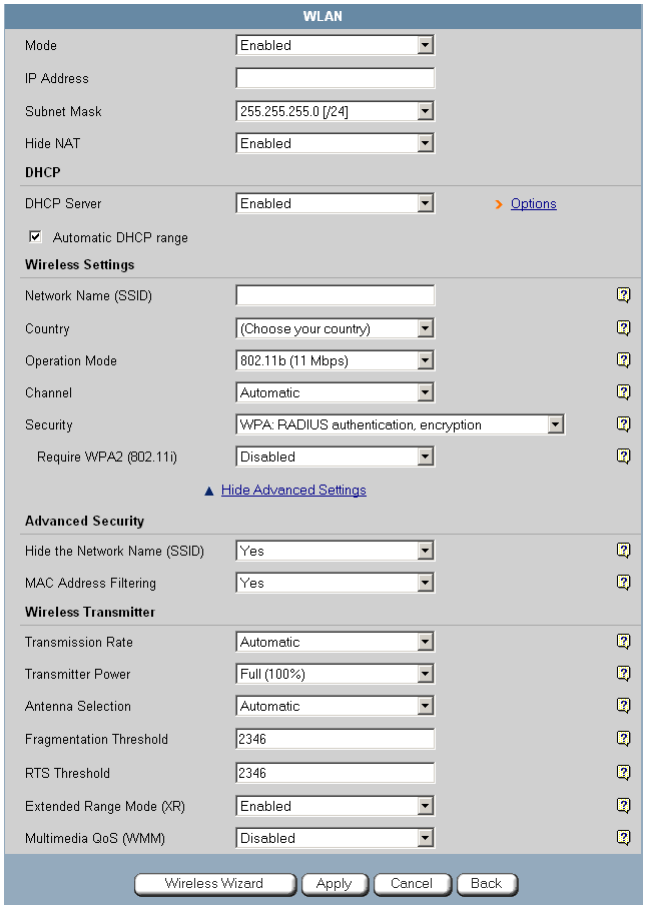
   See ***Enabling/Disabling Hide NAT*** on page 107.

7. If desired, configure a DHCP server.

   See ***Configuring a DHCP Server*** on page 94.

8. Complete the fields using the information in ***Basic WLAN Settings Fields*** on page 168.
9. To configure advanced settings, click Show Advanced Settings and complete the fields using the information in ***Advanced WLAN Settings Fields*** on page 172.

   New fields appear.



10. Click Apply.

    A warning message appears, telling you that you are about to change your network settings.

11. Click OK.

    A success message appears.

12. Prepare the wireless stations.

    See ***Preparing the Wireless Stations*** on page 182.

Table 24: WLAN Settings Fields

In this field…	Do this…
IP Address	Type the IP address of the WLAN network's default gateway.
	Note: The WLAN network must not overlap other networks.
Subnet Mask	Type the WLAN's internal network range.
Wireless Settings	
Network Name (SSID)	Type the network name (SSID) that identifies your wireless network. This name will be visible to wireless stations passing near your access point, unless you enable the Hide the Network Name (SSID) option.
	It can be up to 32 alphanumeric characters long and is case-sensitive.
Country	Select the country where you are located.
	Warning: Choosing an incorrect country may result in the violation of government regulations.

In this field…	Do this…
Operation Mode	Select an operation mode: • 802.11b (11Mbps). Operates in the 2.4 GHz range and offers a maximum theoretical rate of 11 Mbps. When using this mode, only 802.11b stations will be able to connect. • 802.11g (54 Mbps). Operates in the 2.4 GHz range, and offers a maximum theoretical rate of 54 Mbps. When using this mode, only 802.11g stations will be able to connect. • 802.11b/g (11/54 Mbps). Operates in the 2.4 GHz range, and offers a maximum theoretical rate of 54 Mbps. When using this mode, both 802.11b stations and 802.11g stations will be able to connect. • 802.11g Super (108 Mbps). Operates in the 2.4 GHz range, and offers a maximum theoretical rate of 108 Mbps. When using this mode, only 802.11g Super stations will be able to connect. • 802.11g Super (11/54/108). Operates in the 2.4 GHz range, and offers a maximum theoretical rate of 108 Mbps. When using this mode, 802.11b stations, 802.11g stations, and 802.11g Super stations will all be able to connect. Each operation mode indicates a wireless protocol (such as 802.11g Super), followed by the maximum bandwidth (such as 108 Mbps). The list of modes is dependent on the selected country. You can prevent older wireless stations from slowing down your network, by choosing an operation mode that restricts access to newer wireless stations. Note: The actual data transfer speed is usually significantly lower than the maximum theoretical bandwidth and degrades with distance. Important: The station wireless cards must support the selected operation mode. For a list of cards supporting 802.11g Super, refer to http://www.super-ag.com.

In this field…	Do this…
Channel	Select the radio frequency to use for the wireless connection: • Automatic. The Safe@Office appliance automatically selects a channel. This is the default. • A specific channel. The list of channels is dependent on the selected country and operation mode. Note: If there is another wireless network in the vicinity, the two networks may interfere with one another. To avoid this problem, the networks should be assigned channels that are at least 25 MHz (5 channels) apart. Alternatively, you can reduce the transmission power.
Security	Select the security protocol to use. For information on the supported security protocols, see ***Wireless Security Protocols*** on page 163. If you select WEP encryption, the WEP Keys area opens. If you select WPA, the Require WPA2 (802.11i) field appears. If you select WPA-PSK, the Passphrase and Require WPA2 (802.11i) fields appear.
Passphrase	Type the passphrase for accessing the network, or click Random to randomly generate a passphrase. This must be between 8 and 63 characters. It can contain spaces and special characters, and is case-sensitive. For the highest security, choose a long passphrase that is hard to guess, or use the Random button. Note: The wireless stations must be configured with this passphrase as well.

In this field…	Do this…
Require WPA2 (802.11i)	Specify whether you want to require wireless stations to connect using WPA2, by selecting one of the following: • Enable. Only wireless stations using WPA2 can access the WLAN network. • Disable. Wireless stations using either WPA or WPA2 can access the WLAN network. This is the default.
WEP Keys	If you selected WEP encryption, you must configure at least one WEP key. The wireless stations must be configured with the same key, as well.
Key 1, 2, 3, 4 radio button	Click the radio button next to the WEP key that this gateway should use for transmission. The selected key must be entered in the same key slot (1-4) on the station devices, but the key need not be selected as the transmit key on the stations. Note: You can use all four keys to receive data.
Key 1, 2, 3, 4 length	Select the WEP key length from the drop-down list. The possible key lengths are: • 64 Bits. The key length is 10 characters. • 128 Bits. The key length is 26 characters. • 152 Bits. The key length is 32 characters. Note: Some wireless card vendors call these lengths 40/104/128, respectively. Note: WEP is generally considered to be insecure, regardless of the selected key length.

In this field…	Do this…
Key 1, 2, 3, 4 text box	Type the WEP key, or click Random to randomly generate a key matching the selected length. The key is composed of hexadecimal characters 0-9 and A-F, and is not case-sensitive.

Table 25: Advanced WLAN Settings Fields

In this field…	Do this…
Advanced Security	
Hide the Network Name (SSID)	Specify whether you want to hide your network's SSID, by selecting one of the following: • Yes. Hide the SSID. Only devices to which your SSID is known can connect to your network. • No. Do not hide the SSID. Any device within range can detect your network name using the wireless network discovery features of some products, such as Microsoft Windows XP, and attempt to connect to your network. This is the default. Note: Hiding the SSID does not provide strong security, because by a determined attacker can still discover your SSID. Therefore, it is not recommended to rely on this setting alone for security.

In this field…	Do this…
MAC Address Filtering	Specify whether you want to enable MAC address filtering, by selecting one of the following: • Yes. Enable MAC address filtering. Only MAC addresses that you added as network objects can connect to your network. For information on network objects, see ***Using Network Objects*** on page 129. • No. Disable MAC address filtering. This is the default. Note: MAC address filtering does not provide strong security, since MAC addresses can be spoofed by a determined attacker. Therefore, it is not recommended to rely on this setting alone for security.
Wireless Transmitter	
Transmission Rate	Select the transmission rate: • Automatic. The Safe@Office appliance automatically selects a rate. This is the default. • A specific rate
Transmitter Power	Select the transmitter power. Setting a higher transmitter power increases the access point's range. A lower power reduces interference with other access points in the vicinity. The default value is Full. It is not necessary to change this value, unless there are other access points in the vicinity.

In this field…	Do this…
Antenna Selection	Multipath distortion is caused by the reflection of Radio Frequency (RF) signals traveling from the transmitter to the receiver along more than one path. Signals that were reflected by some surface reach the receiver after non-reflected signals and distort them. Safe@Office appliances avoid the problems of multipath distortion by using an antenna diversity system. To provide antenna diversity, each wireless security appliance has two antennas. Specify which antenna to use for communicating with wireless stations: • Automatic. The Safe@Office appliance receives signals through both antennas and automatically selects the antenna with the lowest distortion signal to use for communicating. The selection is made on a per-station basis. This is the default. • ANT 1. The ANT 1antenna is always used for communicating. • ANT 2. The ANT 2 antenna is always used for communicating. Use manual diversity control (ANT 1 or ANT 2), if there is only one antenna connected to the appliance.
Fragmentation Threshold	Type the smallest IP packet size (in bytes) that requires that the IP packet be split into smaller fragments. If you are experiencing significant radio interference, set the threshold to a low value (around 1000), to reduce error penalty and increase overall throughput. Otherwise, set the threshold to a high value (around 2000), to reduce overhead. The default value is 2346.

In this field…	Do this…
RTS Threshold	Type the smallest IP packet size for which a station must send an RTS (Request To Send) before sending the IP packet. If multiple wireless stations are in range of the access point, but not in range of each other, they might send data to the access point simultaneously, thereby causing data collisions and failures. RTS ensures that the channel is clear before the each packet is sent. If your network is congested, and the users are distant from one another, set the RTS threshold to a low value (around 500). Setting a value equal to the fragmentation threshold effectively disables RTS. The default value is 2346.
Extended Range Mode (XR)	Specify whether to use Extended Range (XR) mode: • **Disabled.** XR mode is disabled. • **Enabled.** XR mode is enabled. XR will be automatically negotiated with XR-enabled wireless stations and used as needed. This is the default. For more information on XR mode, see ***About the Wireless Hardware in Your Safe@Office 500W Appliance*** on page 162.
Multimedia QoS (WMM)	Specify whether to use the Wireless Multimedia (WMM) standard to prioritize traffic from WMM-compliant multimedia applications: • **Disabled.** WMM is disabled. This is the default. • **Enabled.** WMM is enabled. The Safe@Office appliance will prioritize multimedia traffic according to four access categories (Voice, Video, Best Effort, and Background). This allows for smoother streaming of voice and video when using WMM aware applications.

Using the Wireless Configuration Wizard

500W

The Wireless Configuration Wizard provides a quick and simple way of setting up your basic WLAN parameters for the first time.

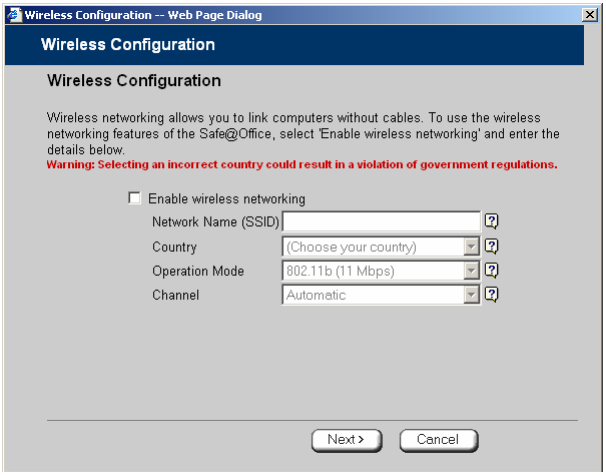
To configure a WLAN using the Wireless Configuration Wizard

1. Prepare the appliance for a wireless connection as described in ***Network Installation*** on page 35.
2. Click Network in the main menu, and click the My Network tab.

   The My Network page appears.
3. In the WLAN network's row, click Edit.

   The Edit Network Settings page appears.
4. Click Wireless Wizard.

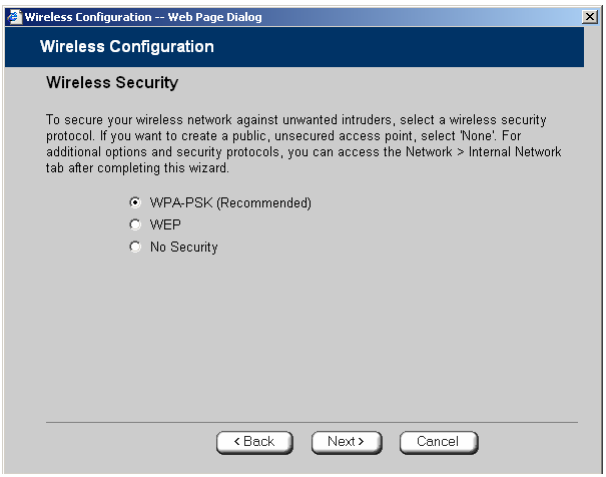
   The Wireless Configuration Wizard opens, with the Wireless Configuration dialog box displayed.



5. Select the Enable wireless networking check box to enable the WLAN.

The fields are enabled.

6. Complete the fields using the information in ***Basic WLAN Settings Fields*** on page 168.
7. Click Next.
8. The Wireless Security dialog box appears.



9. Do one of the following:

   - Click WPA-PSK to use the WPA-PSK security mode.

     WPA-PSK periodically changes and authenticates encryption keys. This is a recommended security mode for small, private wireless networks, which want to authenticate and encrypt wireless data but do not want to install a RADIUS server. Both WPA and the newer, more secure WPA2 (802.11i) will be accepted.

   - Click WEP to use the WEP security mode.

     Using WEP, wireless stations must use a pre-shared key to connect to your network. WEP is widely known to be insecure, and is supported mainly for compatibility with existing networks and stations that do not support other methods.

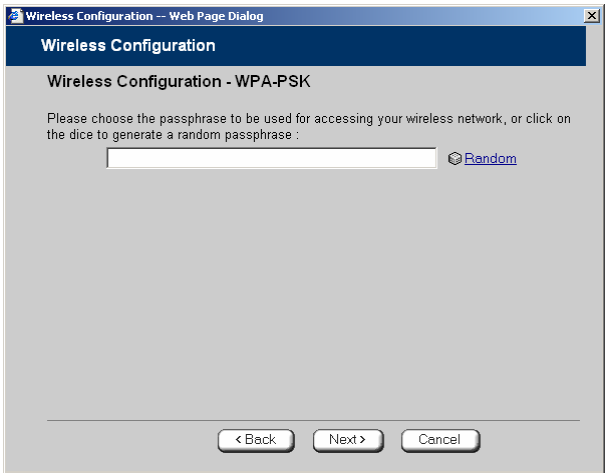
- Click No Security to use no security to create a public, unsecured access point.

Note: You cannot configure WPA and 802.1x using this wizard. For information on configuring these modes, see ***Manually Configuring a WLAN*** on page 165.

10. Click Next.

WPA-PSK

If you chose WPA-PSK, the Wireless Configuration-WPA-PSK dialog box appears.



Do the following:

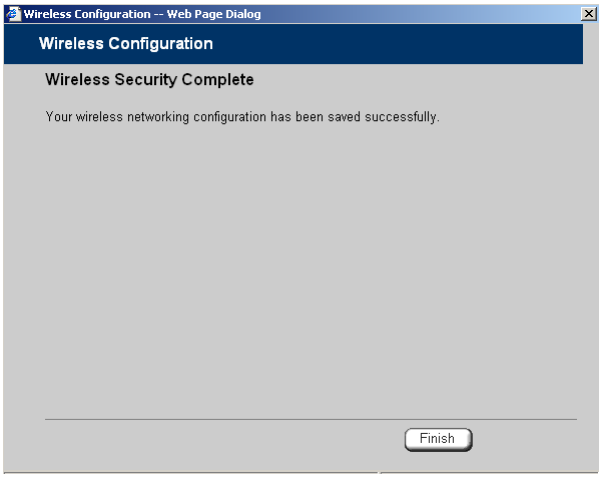
1. In the text box, type the passphrase for accessing the network, or click Random to randomly generate a passphrase.

   This must be between 8 and 63 characters. It can contain spaces and special characters, and is case-sensitive.

2. Click Next.

The **Wireless Security Confirmation** dialog box appears.

3. Click **Next**.
4. The **Wireless Security Complete** dialog box appears.



5. Click **Finish**.

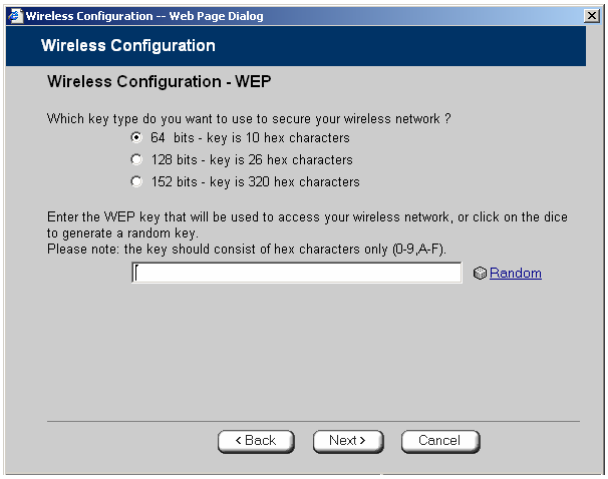
   The wizard closes.

6. Prepare the wireless stations.

See ***Preparing the Wireless Stations*** on page 182.

WEP

If you chose WEP, the Wireless Configuration-WEP dialog box appears.



Do the following:

1. Choose a WEP key length.

   The possible key lengths are:

   - 64 Bits - The key length is 10 hexadecimal characters.
   - 128 Bits - The key length is 26 hexadecimal characters.
   - 152 Bits - The key length is 32 hexadecimal characters.

   Some wireless card vendors call these lengths 40/104/128, respectively.

   Note that WEP is generally considered to be insecure, regardless of the selected key length.

2. In the text box, type the WEP key, or click Random to randomly generate a key matching the selected length.

   The key is composed of characters 0-9 and A-F, and is not case-sensitive. The wireless stations must be configured with this same key.

3. Click Next.

   The Wireless Security Confirmation dialog box appears.

4. Click Next.

   The Wireless Security Complete dialog box appears.

5. Click Finish.

   The wizard closes.

6. Prepare the wireless stations.

   See ***Preparing the Wireless Stations*** on page 182.

No Security

The Wireless Security Complete dialog box appears.

- Click Finish.

  The wizard closes.

Preparing the Wireless Stations

500W

After you have configured a WLAN, the wireless stations must be prepared for connection to the WLAN.

To prepare the wireless stations

1. If you selected the WEP security mode, give the WEP key to the wireless stations' administrators.
2. If you selected the WPA-PSK security mode, give the passphrase to the wireless stations' administrator.
3. The wireless stations' administrators should configure the wireless stations and connect them to the WLAN.

   Refer to the wireless cards' documentation for details.

Note: Some wireless cards have "Infrastructure" and "Ad-hoc" modes. These modes are also called "Access Point" and "Peer to Peer". Choose the "Infrastructure" or "Access Point" mode.
You can set the wireless cards to either "Long Preamble" or "Short Preamble".

Note: The wireless cards' region and the Safe@Office appliance's region must both match the region of the world where you are located. If you purchased your Safe@Office appliance in a different region, contact technical support.

Troubleshooting Wireless Connectivity

I cannot connect to the WLAN from a wireless station. What should I do?

- Check that the SSID configured on the station matches the Safe@Office appliance's SSID. The SSID is case-sensitive.
- Check that the encryption settings configured on the station (encryption mode and keys) match the Safe@Office appliance's encryption settings.
- If MAC filtering is enabled, verify that the MAC address of all stations is listed in the Network Objects page (see ***Viewing and Deleting Network Objects*** on page 138).

How do I test wireless reception?

- Look at the Wireless page, and check for excessive errors or dropped packets.
- Look at the Active Computers page, to see information for specific wireless stations, such as the number of transmission errors, and the current reception power of each station.
- On the wireless station, open a command window and type ping my.firewall. If you see a large number of dropped packets, you are experiencing poor reception.

Wireless reception is poor. What should I do?

- Adjust the angle of the antennas, until the reception improves. The antennas radiate horizontally in all directions.
- If both antennas are connected to the Safe@Office appliance, check that the Antenna Selection parameter in the WLAN's advanced settings is set to Automatic (see ***Manually Configuring a WLAN*** on page 165).
- Relocate the Safe@Office appliance to a place with better reception, and avoid obstructions, such as walls and electrical equipment. For example, try mounting the appliance in a high place with a direct line of sight to the wireless stations.
- Check for interference with nearby electrical equipment, such as microwave ovens and cordless or cellular phones.

- Check the Transmission Power parameter in the WLAN's advanced settings (see ***Manually Configuring a WLAN*** on page 165).
- Make sure that you are not using two access points in close proximity and on the same frequency. For minimum interference, channel separation between nearby access points must be at least 25 MHz (5 channels).
- The Safe@Office appliance supports XR (Extended Range) technology. For best range, enable XR mode in the WLAN's advanced settings (see ***Manually Configuring a WLAN*** on page 165), and use XR-enabled stations.
- Range outdoors is normally much higher than indoors, depending on environmental conditions.

Note: You can observe any changes in the wireless reception in the Active Computers page. Make sure to refresh the page after making a change.

Note: Professional companies are available for help in setting up reliable wireless networks, with access to specialized testing equipment and procedures.

There are excessive collisions between wireless stations. What should I do?

If you have many concurrently active wireless stations, there may be collisions between them. Such collisions may be the result of a "hidden node" problem: not all of the stations are within range of each other, and therefore are "hidden" from one another. For example, if station A and station C do not detect each other, but both stations detect and are detected by station B, then both station A and C may attempt to send packets to station B simultaneously. In this case, the packets will collide, and Station B will receive corrupted data.

The solution to this problem lies in the use of the RTS protocol. Before sending a certain size IP packet, a station sends an RTS (Request To Send) packet. If the recipient is not currently receiving packets from another source, it sends back a CTS (Clear To Send) packet, indicating that the station can send the IP packet. Try setting the RTS Threshold parameter in the WLAN's advanced settings (see ***Manually Configuring a WLAN*** on page 165) to a lower value. This will cause stations to use RTS for smaller IP packets, thus decreasing the likeliness of collisions.

In addition, try setting the Fragmentation Threshold parameter in the WLAN's advanced settings (see ***Manually Configuring a WLAN*** on page 165) to a lower value. This will cause stations to fragment IP packets of a certain size into smaller packets, thereby reducing the likeliness of collisions and increasing network speed.

Note: Reducing the RTS Threshold and the Fragmentation Threshold too much can have a negative impact on performance.

Note: Setting an RTS Threshold value equal to the Fragmentation Threshold value effectively disables RTS.

I am not getting the full speed. What should I do?

- The actual speed is always less then the theoretical speed, and degrades with distance.
- Read the section about reception problems. Better reception means better speed.
- Check that all your wireless stations support the wireless standard you are using (802.11g or 802.11g Super), and that this standard is enabled in the station software. Transmission speed is determined by the slowest station associated with the access point. For a list of wireless stations that support 802.11g Super, see www.super-ag.com.

Chapter 8

Viewing Reports

This chapter describes the Safe@Office Portal reports.

This chapter includes the following topics:

Viewing the Event Log

500

You can track network activity using the Event Log. The Event Log displays the most recent events and color-codes them.

Table 26: Event Log Color Coding

An event marked in this color…	Indicates…
Blue	Changes in your setup that you have made yourself or as a result of a security update implemented by your Service Center.
Red	Connection attempts that were blocked by your firewall.
Orange	Connection attempts that were blocked by your custom security rules.

An event marked in this color…	Indicates…
Green	Traffic accepted by the firewall. By default, accepted traffic is not logged. However, such traffic may be logged if specified by a security policy downloaded from your Service Center, or if specified in user-defined rules.

You can create firewall rules specifying that certain types of connections should be logged, whether the connections are incoming or outgoing, blocked or accepted. For information, see ***Using Rules*** on page 209.

The logs detail the date and the time the event occurred, and its type. If the event is a communication attempt that was rejected by the firewall, the event details include the source and destination IP address, the destination port, and the protocol used for the communication attempt (for example, TCP or UDP). If the event is a connection made or attempted over a VPN tunnel, the event is marked by a lock icon in the VPN column.

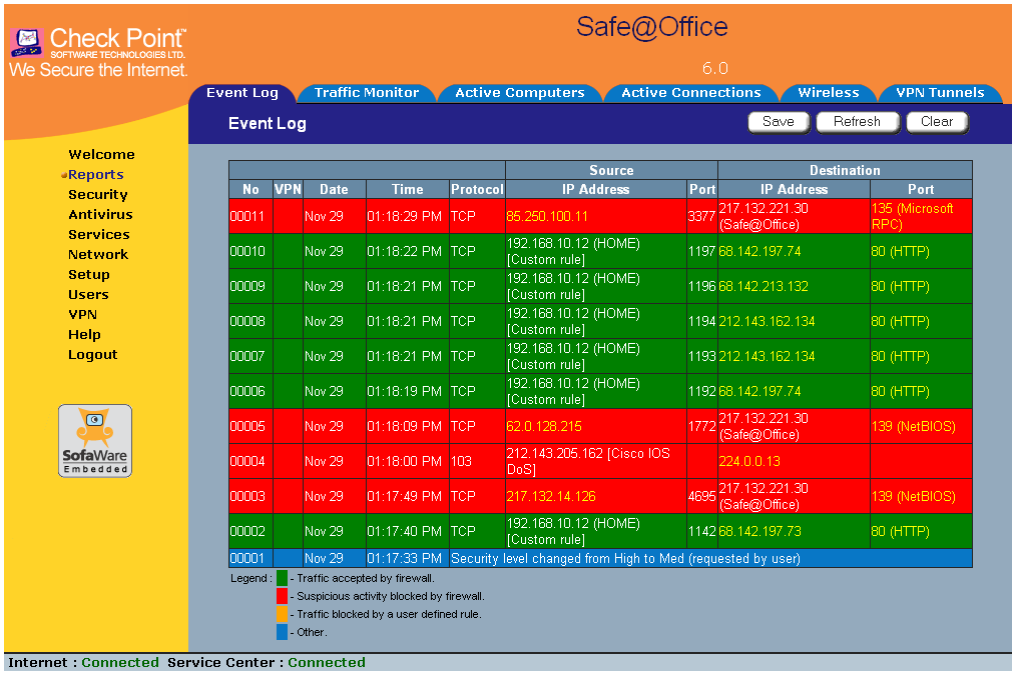
This information is useful for troubleshooting. You can export the logs to an *.xls (Microsoft Excel) file, and then store it for analysis purposes or send it to technical support.

Note: You can configure the Safe@Office appliance to send event logs to a Syslog server. For information, see ***Configuring Syslog Logging*** on page 386.

To view the event log

1. Click **Reports** in the main menu, and click the **Event Log** tab.

   The **Event Log** page appears.



2. If an event is highlighted in red, indicating a blocked attack on your network, you can display the attacker's details, by clicking on the IP address of the attacking machine.

   The Safe@Office appliance queries the Internet WHOIS server, and a window displays the name of the entity to whom the IP address is registered and their contact information. This information is useful in tracking down hackers.

3. To refresh the display, click **Refresh**.

4. To save the displayed events to an *.xls file:

   a. Click **Save**.

A standard File Download dialog box appears.

b. Click Save.

The Save As dialog box appears.

c. Browse to a destination directory of your choice.

d. Type a name for the configuration file and click Save.

The *.xls file is created and saved to the specified directory.

5. To clear all displayed events:

a. Click Clear.

A confirmation message appears.

b. Click OK.

All events are cleared.

Using the Traffic Monitor

500

You can view incoming and outgoing traffic for selected network interfaces and QoS classes using the Traffic Monitor. This enables you to identify network traffic trends and anomalies, and to fine tune Traffic Shaper QoS class assignments.

The Traffic Monitor displays separate bar charts for incoming traffic and outgoing traffic, and displays traffic rates in kilobits/second. If desired, you can change the number of seconds represented by the bars in the charts, using the procedure ***Configuring Traffic Monitor Settings*** on page 193.

In network traffic reports, the traffic is color-coded as described in the table below. In the All QoS Classes report, the traffic is color-coded by QoS class.

Table 27: Traffic Monitor Color Coding for Networks

Traffic marked in this color…	Indicates…
Blue	VPN-encrypted traffic
Red	Traffic blocked by the firewall
Green	Traffic accepted by the firewall

You can export a detailed traffic report for all enabled networks and all defined QoS classes, using the procedure ***Exporting General Traffic Reports*** on page 194.

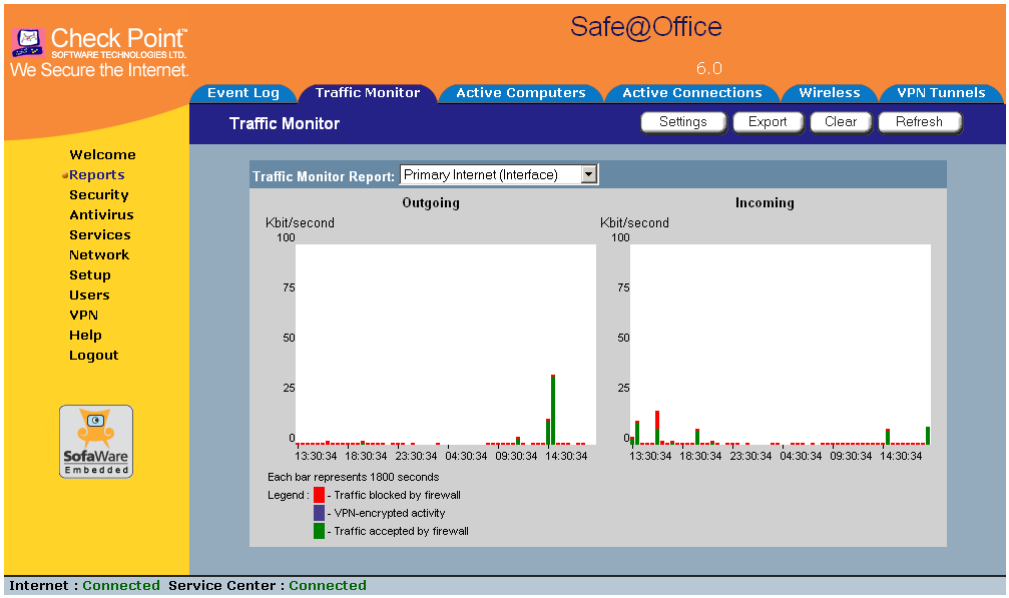
Viewing Traffic Reports

500

To view a traffic report

1. Click Reports in the main menu, and click the Traffic Monitor tab.

The Traffic Monitor page appears.



2. In the Traffic Monitor Report drop-down list, select the network interface for which you want to view a report.

   The list includes all currently enabled networks. For example, if the DMZ network is enabled, it will appear in the list.

   If Traffic Shaper is enabled, the list also includes the defined QoS classes. Choose All QoS Classes to display a report including all QoS classes. For information on enabling Traffic Shaper see ***Using Internet Setup*** on page 63.

   The selected report appears in the Traffic Monitor page.

3. To refresh all traffic reports, click Refresh.

4. To clear all traffic reports, click Clear.

Note: The firewall blocks broadcast packets used during the normal operation of your network. This may lead to a certain amount of traffic of the type "Traffic blocked by firewall" that appears under normal circumstances and usually does not indicate an attack.

Configuring Traffic Monitor Settings

500

You can configure the interval at which the Safe@Office appliance should collect traffic data for network traffic reports.

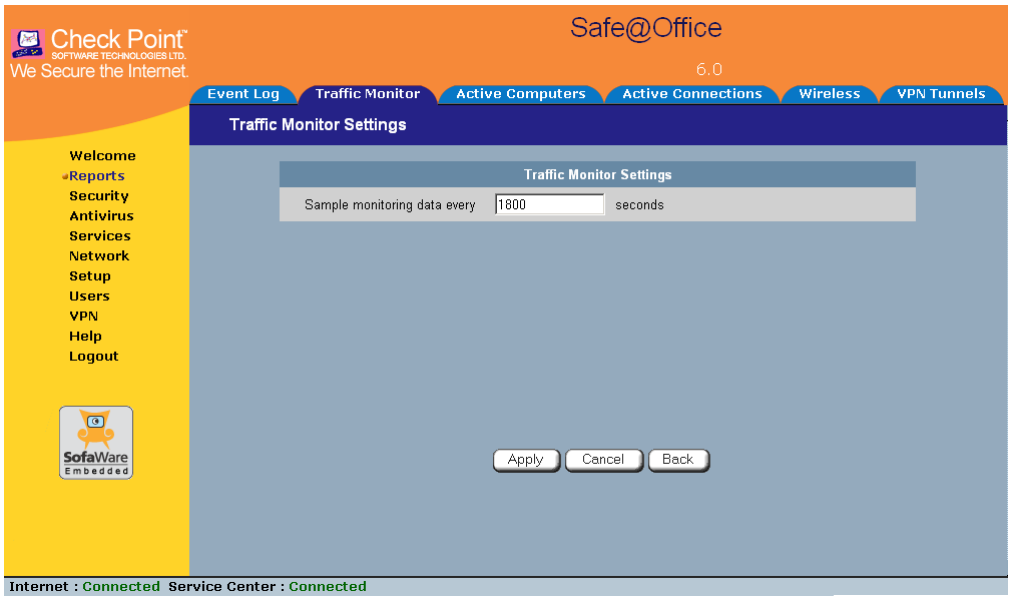
To configure Traffic Monitor settings

1. Click Reports in the main menu, and click the Traffic Monitor tab.

   The Traffic Monitor page appears.

2. Click Settings.

   The Traffic Monitor Settings page appears.



3. In the Sample monitoring data every field, type the interval (in seconds) at which the Safe@Office appliance should collect traffic data.

   The default value is one sample every 1800 seconds (30 minutes).

4. Click Apply.

Exporting General Traffic Reports

500

You can export a general traffic report that includes information for all enabled networks and all defined QoS classes to a *.csv (Comma Separated Values) file. You can open and view the file in Microsoft Excel.

To export a general traffic report

1. Click Reports in the main menu, and click the Traffic Monitor tab.

   The Traffic Monitor page appears.
2. Click Export.

   A standard File Download dialog box appears.
3. Click Save.

   The Save As dialog box appears.
4. Browse to a destination directory of your choice.
5. Type a name for the configuration file and click Save.

   A *.csv file is created and saved to the specified directory.

Viewing Computers

500

This option allows you to view the currently active computers on your network. The active computers are graphically displayed, each with its name, IP address, and settings (DHCP, Static, etc.). You can also view node limit information.

To view the active computers

1. Click Reports in the main menu, and click the Active Computers tab.

The **Active Computers** page appears.

If you configured High Availability, both the master and backup appliances are shown. If you configured OfficeMode, the OfficeMode network is shown.

If you are using Safe@Office 500W, the wireless stations are shown. For information on viewing statistics for these computers, see ***Viewing Wireless Statistics*** on page 198. If a wireless station has been blocked from accessing the Internet through the Safe@Office appliance, the reason why it was blocked is shown in red.

If you are exceeding the maximum number of computers allowed by your license, a warning message appears, and the computers over the node limit are marked in red. These computers are still protected, but they are blocked from accessing the Internet through the Safe@Office appliance.

If HotSpot mode is enabled for some networks, each computer's HotSpot status is displayed next to it. The possible statuses include:

- Authenticated. The computer is logged on to My HotSpot.
- Not Authenticated. The computer is not logged on to My HotSpot.
- Excluded from HotSpot. The computer is in an IP address range excluded from HotSpot enforcement. To enforce HotSpot, you must edit the network object. See ***Adding and Editing Network Objects*** on page 130.

Note: Computers that did not communicate through the firewall are not counted for node limit purposes, even though they are protected by the firewall.

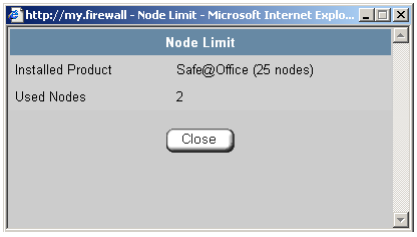
Note: To increase the number of computers allowed by your license, you can upgrade your product. For further information, see ***Upgrading Your Software Product*** on page 381.

Next to each computer, an Add button enables you to add a network object for the computer, or an Edit button enables you to edit an existing network object for the computer. For information on adding and editing network objects, see ***Adding and Editing Network Objects*** on page 130.

2. To refresh the display, click Refresh.
3. To view node limit information, do the following:

   a. Click Node Limit.

   The Node Limit window appears with installed software product and the number of nodes used.



   b. Click Close to close the window.

Viewing Connections

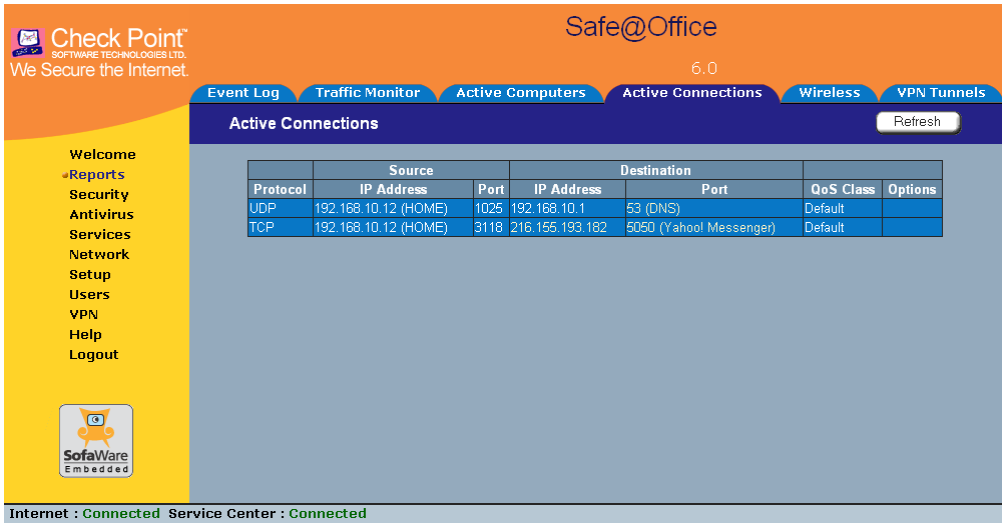
500

This option allows you to view the currently active connections between your network and the external world.

To view the active connections

1. Click Reports in the main menu, and click the Active Connections tab.

   The Active Connections page appears.



   The page displays the information in the table below.

2. To refresh the display, click Refresh.

3. To view information on the destination machine, click its IP address.

   The Safe@Office appliance queries the Internet WHOIS server, and a window displays the name of the entity to which the IP address is registered and their contact information.

4. To view information about a port, click the port.

   A window opens displaying information about the port.

Table 28: Active Connections Fields

This field…	Displays…
Protocol	The protocol used (TCP, UDP, etc.)
Source - IP Address	The source IP address
Source - Port	The source port
Destination - IP Address	The destination IP address
Destination -Port	The destination port
QoS Class	The QoS class to which the connection belongs
Options	An icon indicating further details: • - The connection is encrypted. • - The connection is being scanned by VStream Antivirus.

Viewing Wireless Statistics

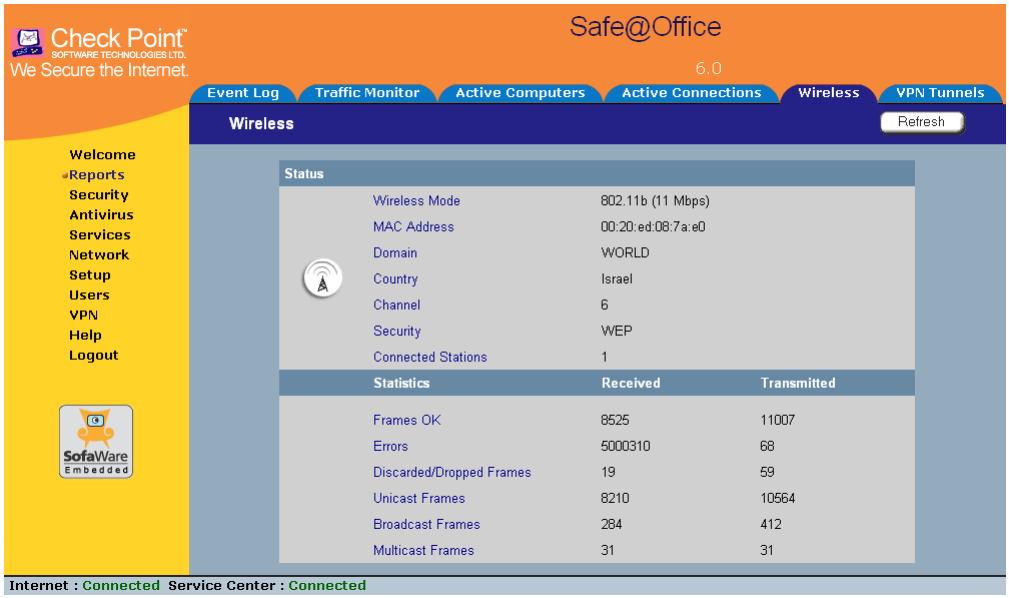
500W

If your WLAN is enabled, you can view wireless statistics for the WLAN or for individual wireless stations.

To view statistics for the WLAN

1. Click Reports in the main menu, and click the Wireless tab.

The **Wireless** page appears.



The page displays the information in the table below.

2. To refresh the display, click **Refresh**.

Table 29: WLAN Statistics

This field...	Displays...
Wireless Mode	The operation mode used by the WLAN, followed by the transmission rate in Mbps
MAC Address	The MAC address of the Safe@Office appliance's WLAN interface
Domain	The Safe@Office access point's region
Country	The country configured for the WLAN
Channel	The radio frequency used by the WLAN

This field…	Displays…
Security	The security mode used by the WLAN
Connected Stations	The number of wireless stations currently connected to the WLAN
Frames OK	The total number of frames that were successfully transmitted and received
Errors	The total number of transmitted and received frames for which an error occurred
Discarded/ Dropped Frames	The total number of discarded or dropped frames transmitted and received
Unicast Frames	The number of unicast frames transmitted and received
Broadcast Frames	The number of broadcast frames transmitted and received
Multicast Frames	The number of multicast frames transmitted and received

To view statistics for a wireless station

1. Click Reports in the main menu, and click the Active Computers tab.

   The Active Computers page appears.

   The following information appears next to each wireless station:

   - The signal strength in dB
   - A bar chart representing the signal strength
2. Mouse-over the information icon next to the wireless station.

   A tooltip displays displays statistics for the wireless station, as described in the table below.

3. To refresh the display, click Refresh.

Table 30: Wireless Station Statistics

This field…	Displays…
Current Rate	The current reception and transmission rate in Mbps
Frames OK	The total number of frames that were successfully transmitted and received
Errors	The total number of transmitted and received frames for which an error occurred
Discarded/ Dropped Frames	The total number of discarded or dropped frames transmitted and received
Unicast Frames	The number of unicast frames transmitted and received
Broadcast Frames	The number of broadcast frames transmitted and received
Multicast Frames	The number of multicast frames transmitted and received
WLAN Mode	The wireless client's operation mode, indicating the client's maximum speed. Possible values are B, G, and 108G. For more information, see ***Basic WLAN Settings Fields*** on page 168.
XR	Indicates whether the wireless client supports Extended Range (XR) mode. Possible values are: • yes. The wireless client supports XR mode. • no. The wireless client does not support XR mode.

This field…	Displays…
Cipher	The security protocol used for the connection with the wireless client. For more information, see ***Wireless Security Protocols*** on page 163.

Chapter 9

Setting Your Security Policy

This chapter describes how to set up your Safe@Office appliance security policy.

You can enhance your security policy by subscribing to services such as Web Filtering and Email Filtering. For information on subscribing to services, see ***Using Subscription Services*** on page 281.

This chapter includes the following topics:

Default Security Policy

The Safe@Office default security policy includes the following rules:

- Access is blocked from the WAN (Internet) to all internal networks (LAN, DMZ, WLAN, VLANs, and OfficeMode).
- Access is allowed from the internal networks to the WAN, according to the firewall security level (Low/Medium/High).
- Access is allowed from the LAN network to the other internal networks (DMZ, WLAN, VLANs, and OfficeMode).
- Access is blocked from the DMZ, WLAN, VLAN, and OfficeMode networks to the other internal networks, (including between different VLANs).
- HTTP access to the Safe@Office Portal (my.firewall and my.vpn) is allowed from all internal networks except the WLAN. The WLAN can only access the Safe@Office Portal using HTTPS, unless a specific user-defined rule allows this.
- When using the print server function (see ***Using Network Printers*** on page 425), access from internal networks to connected network printers is allowed.
- Access from the WAN to network printers is blocked.

These rules are independent of the firewall security level.

You can easily override the default security policy, by creating user-defined firewall rules. For further information, see ***Using Rules*** on page 209.

Setting the Firewall Security Level

500

The firewall security level can be controlled using a simple lever available on the Firewall page. You can set the lever to three states.

Table 31: Firewall Security Levels

This level…	Does this…	Further Details
Low	Enforces basic control on incoming connections, while permitting all outgoing connections.	All inbound traffic is blocked to the external Safe@Office appliance IP address, except for ICMP echoes ("pings"). All outbound connections are allowed.
Medium	Enforces strict control on all incoming connections, while permitting safe outgoing connections. This is the default level and is recommended for most cases. Leave it unchanged unless you have a specific need for a higher or lower security level.	All inbound traffic is blocked. All outbound traffic is allowed to the Internet except for Windows file sharing (NBT ports 137, 138, 139 and 445).
High	Enforces strict control on all incoming and outgoing connections.	All inbound traffic is blocked. Restricts all outbound traffic except for the following: Web traffic (HTTP, HTTPS), email (IMAP, POP3, SMTP), ftp, newsgroups, Telnet, DNS, IPSEC IKE and VPN traffic.

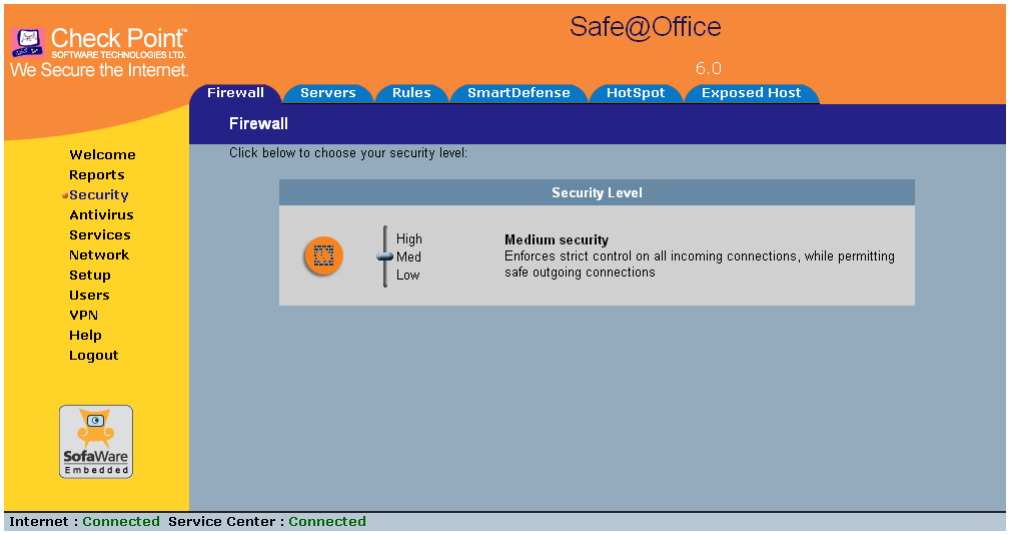
Note: If the security policy is remotely managed, this lever might be disabled.

Note: The definitions of firewall security levels provided in this table represent the Safe@Office appliance's default security policy. Security updates downloaded from a Service Center may alter this policy and change these definitions.

To change the firewall security level

1. Click Security in the main menu, and click the Firewall tab.

   The Firewall page appears.



2. Drag the security lever to the desired level.

   The Safe@Office appliance security level changes accordingly.

Configuring Servers

500

Note: If you do not intend to host any public Internet servers (Web Server, Mail Server etc.) in your network, you can skip this section.

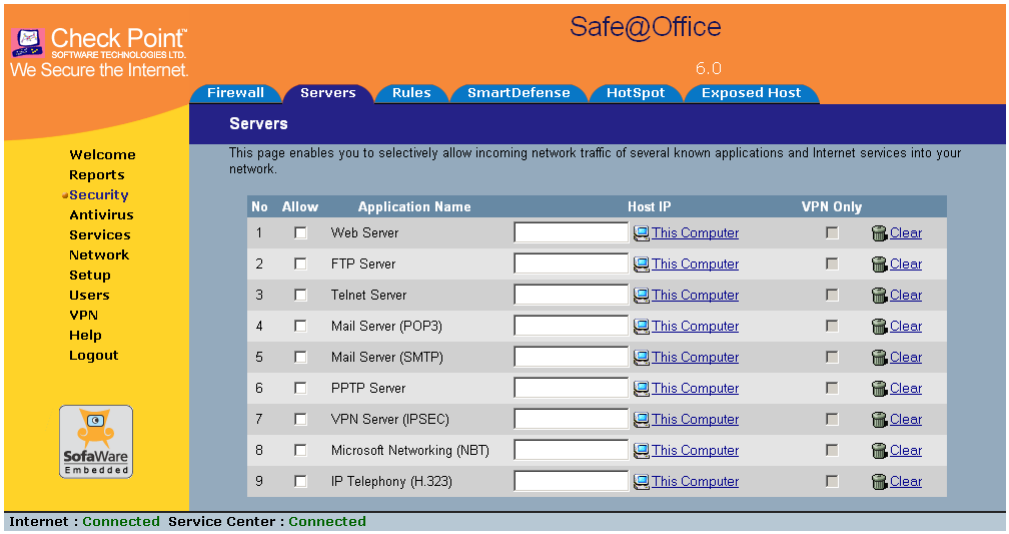
Using the Safe@Office Portal, you can selectively allow incoming network connections into your network. For example, you can set up your own Web server, Mail server or FTP server.

Note: Configuring servers allows you to create simple Allow and Forward rules for common services, and it is equivalent to creating Allow and Forward rules in the Rules page. For information on creating rules, see ***Using Rules*** on page 209.

To allow a service to be run on a specific host

1. Click Security in the main menu, and click the Servers tab.

   The Servers page appears, displaying a list of services and a host IP address for each allowed service.



2. Complete the fields using the information in the table below.
3. Click Apply.

   A success message appears, and the selected computer is allowed to run the desired service or application.

Table 32: Servers Page Fields

In this column…	Do this…
Allow	Select the desired service or application.
VPN Only	Select this option to allow only connections made through a VPN.
Host IP	Type the IP address of the computer that will run the service (one of your network computers) or click the corresponding This Computer button to allow your computer to host the service.

To stop the forwarding of a service to a specific host

1. Click Security in the main menu, and click the Servers tab.

   The Servers page appears, displaying a list of services and a host IP address for each allowed service.
2. In the desired service or application's row, click Clear.

   The Host IP field of the desired service is cleared.
3. Click Apply.

   The service or application is not allowed on the specific host.

Using Rules

500

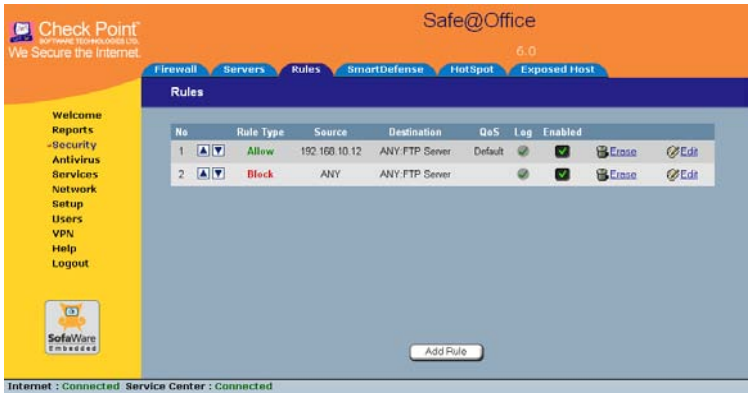
The Safe@Office appliance checks the protocol used, the ports range, and the destination IP address, when deciding whether to allow or block traffic.

User-defined rules have priority over the default security policy rules and provide you with greater flexibility in defining and customizing your security policy.

For example, if you assign your company's accounting department to the LAN network and the rest of the company to the DMZ network, then as a result of the default security policy rules, the accounting department will be able to connect to all company computers, while the rest of the employees will not be able to access any sensitive information on the accounting department computers. You can override the default security policy rules, by creating firewall rules that allow specific DMZ computers (such a manager's computer) to connect to the LAN network and the accounting department.

The Safe@Office appliance processes user-defined rules in the order they appear in the Rules table, so that rule 1 is applied before rule 2, and so on. This enables you to define exceptions to rules, by placing the exceptions higher up in the Rules table.

For example, if you want to block all outgoing FTP traffic, except traffic from a specific IP address, you can create a rule blocking all outgoing FTP traffic and move the rule down in the Rules table. Then create a rule allowing FTP traffic from the desired IP address and move this rule to a higher location in the Rules table than the first rule. In the figure below, the general rule is rule number 2, and the exception is rule number 1.



The Safe@Office appliance will process rule 1 first, allowing outgoing FTP traffic from the specified IP address, and only then it will process rule 2, blocking all outgoing FTP traffic.

The following rule types exist:

Table 33: Firewall Rule Types

Rule	Description
Allow and Forward	This rule type enables you to do the following: • Permit incoming access from the Internet to a specific service in your internal network. • Forward all such connections to a specific computer in your network. • Redirect the specified connections to a specific port. This option is called Port Address Translation (PAT). • Assign traffic to a QoS class. If Traffic Shaper is enabled for incoming traffic, then Traffic Shaper will handle relevant connections as specified in the bandwidth policy for the selected QoS class. For example, if Traffic Shaper is enabled for incoming traffic, and you create an Allow and Forward rule associating all incoming Web traffic with the Urgent QoS class, then Traffic Shaper will handle incoming Web traffic as specified in the bandwidth policy for the Urgent class. For information on Traffic Shaper and QoS classes, see ***Using Traffic Shaper*** on page 151. Creating an Allow and Forward rule is equivalent to defining a server in the Servers page. Note: You must use this type of rule to allow incoming connections if your network uses Hide NAT. Note: You cannot specify two Allow and Forward rules that forward the same service to two different destinations.

Rule	Description
Allow	This rule type enables you to do the following: • Permit outgoing access from your internal network to a specific service on the Internet. Note: You can allow outgoing connections for services that are not permitted by the default security policy. • Permit incoming access from the Internet to a specific service in your internal network. • Assign traffic to a QoS class. If Traffic Shaper is enabled for the direction of traffic specified in the rule (incoming or outgoing), then Traffic Shaper will handle relevant connections as specified in the bandwidth policy for the selected QoS class. For example, if Traffic Shaper is enabled for outgoing traffic, and you create an Allow rule associating all outgoing Web traffic with the Urgent QoS class, then Traffic Shaper will handle outgoing Web traffic as specified in the bandwidth policy for the Urgent class. For information on Traffic Shaper and QoS classes, see ***Using Traffic Shaper*** on page 151. Note: You cannot use an Allow rule to permit incoming traffic, if the network or VPN uses Hide NAT. However, you can use Allow rules for static NAT IP addresses.
Block	This rule type enables you to do the following: • Block outgoing access from your internal network to a specific service on the Internet. • Block incoming access from the Internet to a specific service in your internal network.

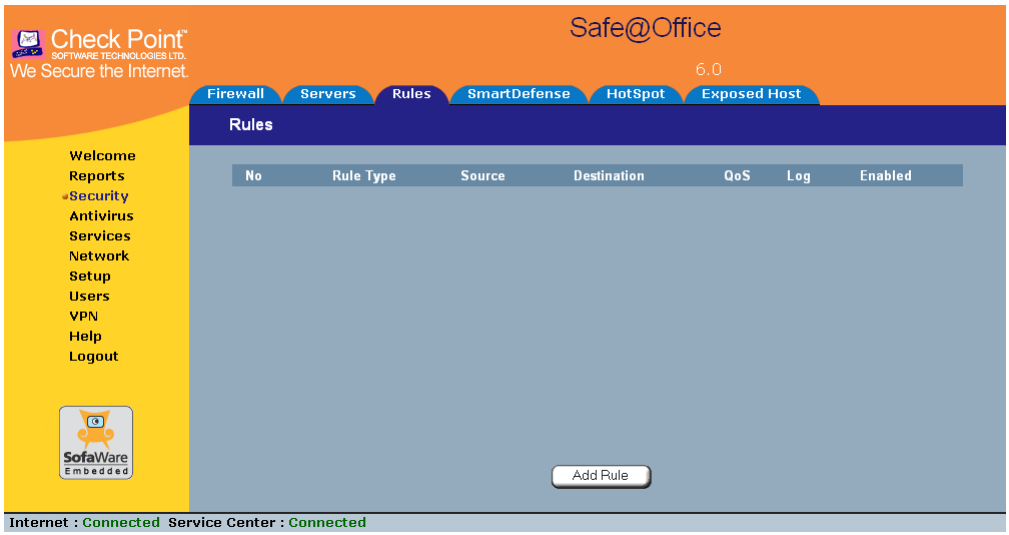
Adding and Editing Rules

500

To add or edit a rule

1. Click Security in the main menu, and click the Rules tab.

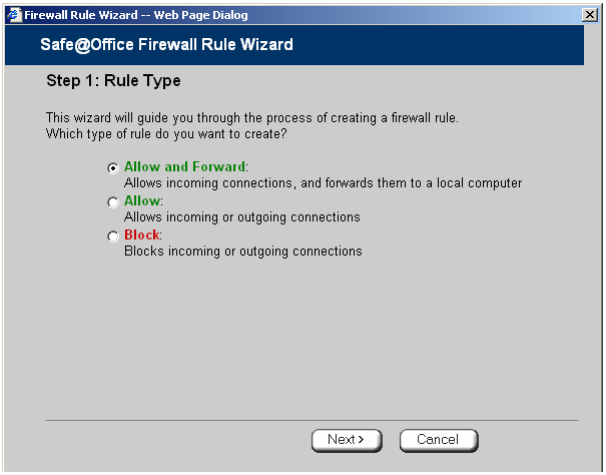
   The Rules page appears.



2. Do one of the following:

   - To add a new rule, click Add Rule.
   - To edit an existing rule, click the Edit icon next to the desired rule.

The **Safe@Office Firewall Rule** wizard opens, with the **Step 1: Rule Type** dialog box displayed.



3. Select the type of rule you want to create.
4. Click **Next**.

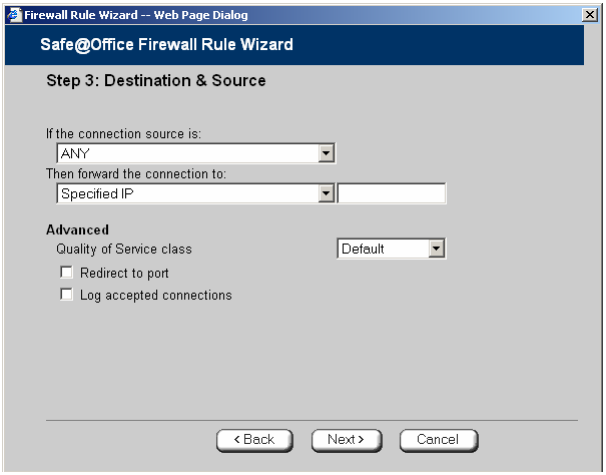
   The **Step 2: Service** dialog box appears.

   The example below shows an Allow rule.

5. Complete the fields using the relevant information in the table below.

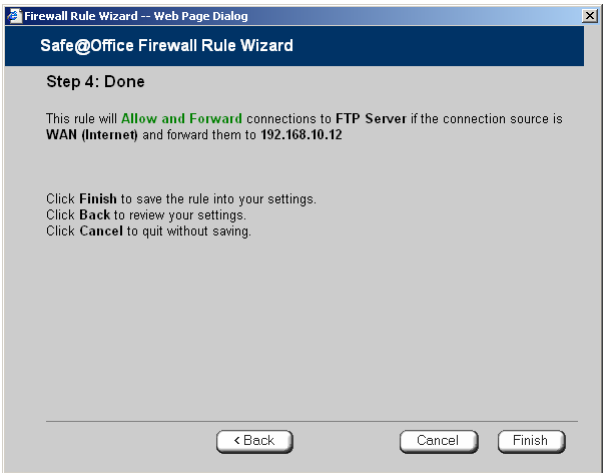
6. Click **Next.**

   The **Step 3: Destination & Source** dialog box appears.



7. Complete the fields using the relevant information in the table below.

   The **Step 4: Done** dialog box appears.



8. Click **Finish.**

   The new rule appears in the **Firewall Rules** page.

Table 34: Firewall Rule Fields

In this field…	Do this…
Any Service	Click this option to specify that the rule should apply to any service.
Standard Service	Click this option to specify that the rule should apply to a specific standard service. You must then select the desired service from the drop-down list.
Custom Service	Click this option to specify that the rule should apply to a specific non-standard service. The Protocol and Port Range fields are enabled. You must fill them in.
Protocol	Select the protocol (ESP, GRE, TCP, UDP or ANY) for which the rule should apply.
Ports	To specify the port range to which the rule applies, type the start port number in the left text box, and the end port number in the right text box. Note: If you do not enter a port range, the rule will apply to all ports. If you enter only one port number, the range will include only that port.
Source	Select the source of the connections you want to allow/block. To specify an IP address, select Specified IP and type the desired IP address in the filed provided. To specify an IP address range, select Specified Range and type the desired IP address range in the fields provided.

In this field…	Do this…
Destination	Select the destination of the connections you want to allow or block. To specify an IP address, select Specified IP and type the desired IP address in the text box. To specify an IP address range, select Specified Range and type the desired IP address range in the fields provided. This option is not available in Allow and Forward rules. To specify the Safe@Office IP address, select This Gateway. This option is not available in Allow and Forward rules. To specify any destination *except* the Safe@Office Portal and network printers, select ANY.
Quality of Service class	Select the QoS class to which you want to assign the specified connections. If Traffic Shaper is enabled, Traffic Shaper will handle these connections as specified in the bandwidth policy for the selected QoS class. If Traffic Shaper is not enabled, this setting is ignored. For information on Traffic Shaper and QoS classes, see ***Using Traffic Shaper*** on page 151. This drop-down list only appears when defining an Allow rule or an Allow and Forward rule.
Log accepted connections / Log blocked connections	Select this option to log the specified blocked or allowed connections. By default, accepted connections are not logged, and blocked connections are logged. You can modify this behavior by changing the check box's state.

In this field…	Do this…
Redirect to port	Select this option to redirect the connections to a specific port. You must then type the desired port in the field provided. This option is called Port Address Translation (PAT), and is only available when defining an Allow and Forward rule.

Enabling/Disabling Rules

500

You can temporarily disable a user-defined rule.

To enable/disable a rule

1. Click Security in the main menu, and click the Rules tab.

   The Rules page appears.

2. Next to the desired rule, do one of the following:

   - To enable the rule, click .

     The button changes to and the rule is enabled.

   - To disable the rule, click .

     The button changes to and the rule is disabled.

Changing Rules' Priority

500

To change a rule's priority

1. Click Security in the main menu, and click the Rules tab.

   The Rules page appears.

2. Do one of the following:

   - Click ▲ next to the desired rule, to move the rule up in the table.
   - Click ▼ next to the desired rule, to move the rule down in the table.

   The rule's priority changes accordingly.

Deleting Rules

500

To delete an existing rule

1. Click Security in the main menu, and click the Rules tab.

   The Rules page appears.

2. Click the Erase icon of the rule you wish to delete.

   A confirmation message appears.

3. Click OK.

   The rule is deleted.

Using SmartDefense

500

The Safe@Office appliance includes Check Point SmartDefense Services, based on Check Point Application Intelligence. SmartDefense provides a combination of attack safeguards and attack-blocking tools that protect your network in the following ways:

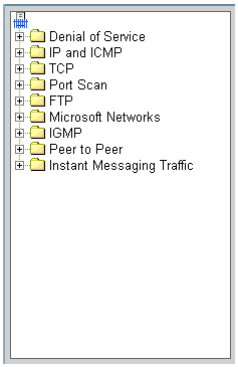
- Validating compliance to standards
- Validating expected usage of protocols (Protocol Anomaly Detection)
- Limiting application ability to carry malicious data
- Controlling application-layer operations

In addition, SmartDefense aids proper usage of Internet resources, such as FTP, instant messaging, Peer-to-Peer (P2P) file sharing, file-sharing operations, and File Transfer Protocol (FTP) uploading, among others.

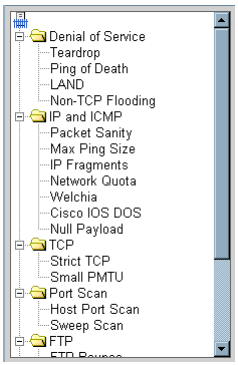
Configuring SmartDefense

500

For convenience, SmartDefense is organized as a tree, in which each branch represents a category of settings.



When a category is expanded, the settings it contains appear as nodes. For information on each category and the nodes it contains, see ***SmartDefense Categories*** on page 224.

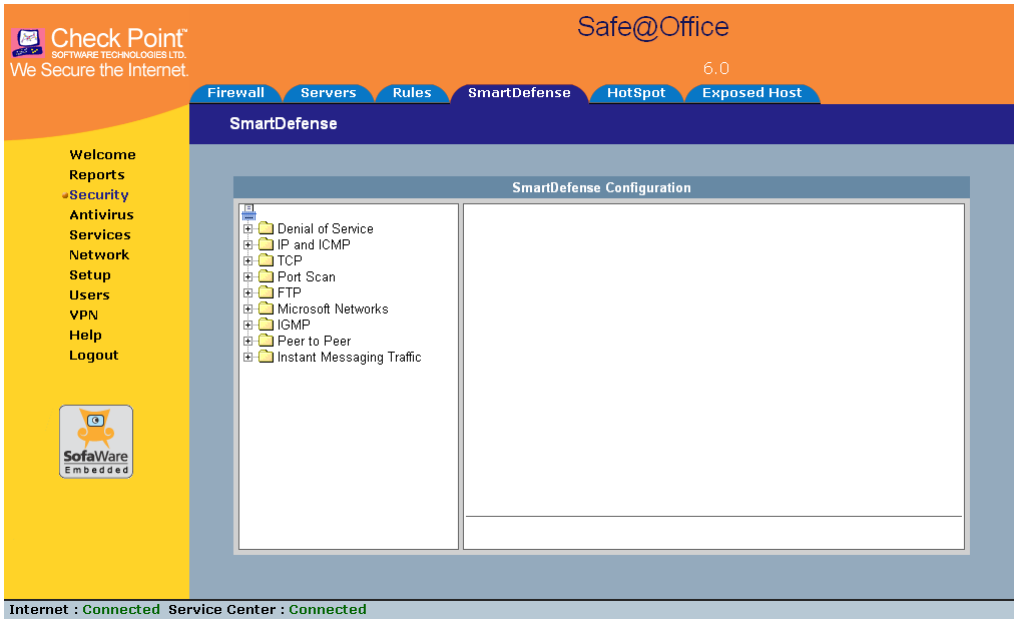


Each node represents an attack type, a sanity check, or a protocol or service that is vulnerable to attacks. To control how SmartDefense handles an attack, you must configure the relevant node's settings.

To configure a SmartDefense node

1. Click Security in the main menu, and click the SmartDefense tab.

   The SmartDefense page appears.

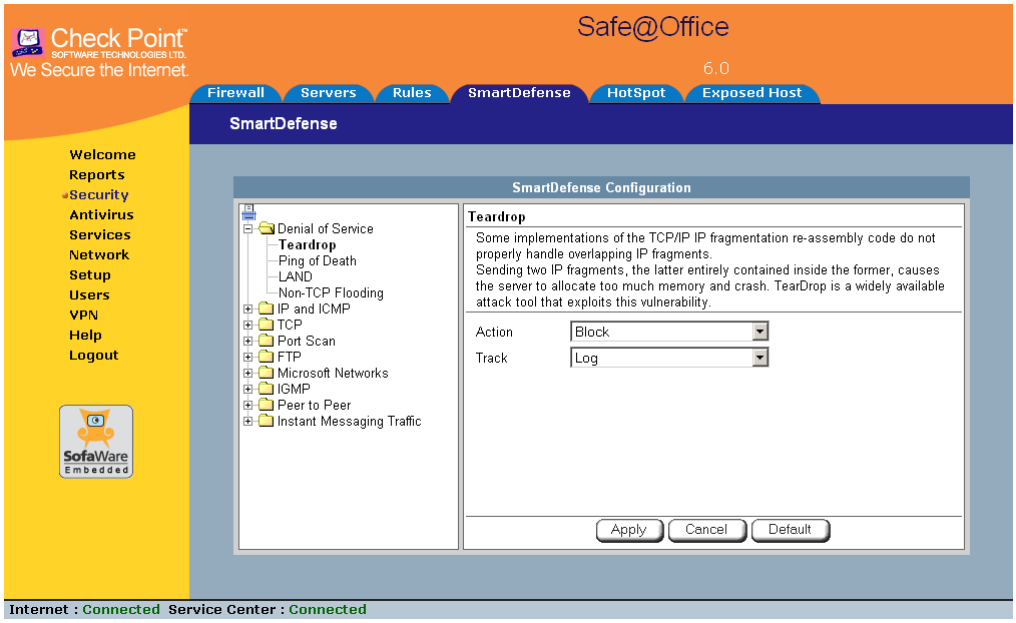


   The left pane displays a tree containing SmartDefense categories.

   - To expand a category, click the ⊞ icon next to it.
   - To collapse a category, click the ⊟ icon next to it.

2. Expand the relevant category, and click on the desired node.

The right pane displays a description of the node, followed by fields.



3. To modify the node's current settings, do the following:

   a) Complete the fields using the relevant information in ***SmartDefense Categories*** on page 224.

   b) Click Apply.

4. To reset the node to its default values:

   a) Click Default.

      A confirmation message appears.

   b) Click OK.

      The fields are reset to their default values, and your changes are saved.

SmartDefense Categories

SmartDefense includes the following categories:

Denial of Service

Denial of Service (DoS) attacks are aimed at overwhelming the target with spurious data, to the point where it is no longer able to respond to legitimate service requests.

This category includes the following attacks:

Teardrop

In a Teardrop attack, the attacker sends two IP fragments, the latter entirely contained within the former. This causes some computers to allocate too much memory and crash.

You can configure how Teardrop attacks should be handled.

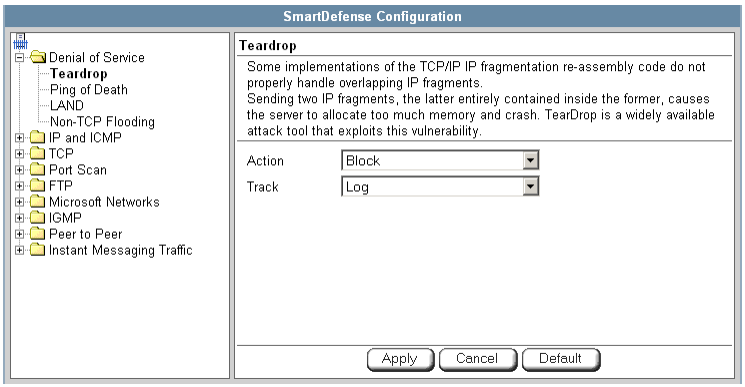


Table 35: Teardrop Fields

In this field…	Do this…
Action	Specify what action to take when a Teardrop attack occurs, by selecting one of the following: • Block. Block the attack. This is the default. • None. No action.
Track	Specify whether to log Teardrop attacks, by selecting one of the following: • Log. Log the attack. This is the default. • None. Do not log the attack.

Ping of Death

In a Ping of Death attack, the attacker sends a fragmented PING request that exceeds the maximum IP packet size (64KB). Some operating systems are unable to handle such requests and crash.

You can configure how Ping of Death attacks should be handled.

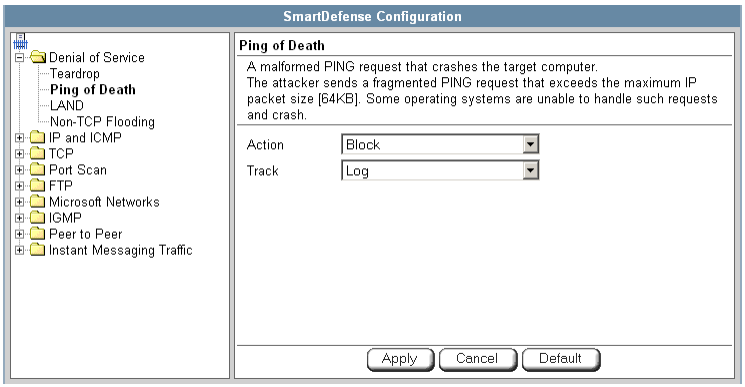


Table 36: Ping of Death Fields

In this field…	Do this…
Action	Specify what action to take when a Ping of Death attack occurs, by selecting one of the following: • Block. Block the attack. This is the default. • None. No action.
Track	Specify whether to log Ping of Death attacks, by selecting one of the following: • Log. Log the attack. This is the default. • None. Do not log the attack.

LAND

In a LAND attack, the attacker sends a SYN packet, in which the source address and port are the same as the destination (the victim computer). The victim computer then tries to reply to itself and either reboots or crashes.

You can configure how LAND attacks should be handled.

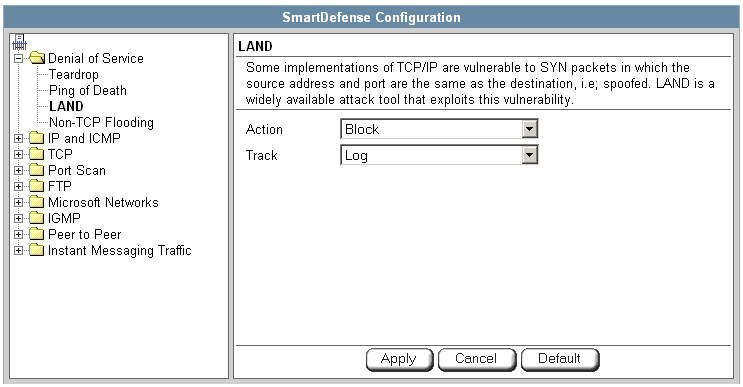


Table 37: LAND Fields

In this field...	Do this...
Action	Specify what action to take when a LAND attack occurs, by selecting one of the following: • Block. Block the attack. This is the default. • None. No action.
Track	Specify whether to log LAND attacks, by selecting one of the following: • Log. Log the attack. This is the default. • None. Do not log the attack.

Non-TCP Flooding

Advanced firewalls maintain state information about connections in a State table. In non-TCP Flooding attacks, the attacker sends high volumes of non-TCP traffic. Since such traffic is connectionless, the related state information cannot be cleared or reset, and the firewall State table is quickly filled up. This prevents the firewall from accepting new connections and results in a Denial of Service (DoS).

You can protect against Non-TCP Flooding attacks by limiting the percentage of state table capacity used for non-TCP connections.

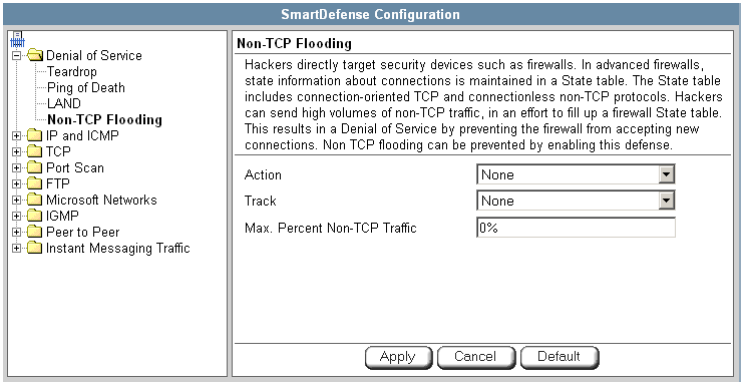


Table 38: Non-TCP Flooding Fields

In this field...	Do this...
Action	Specify what action to take when the percentage of state table capacity used for non-TCP connections reaches the Max. percent non TCP traffic threshold. Select one of the following: • Block. Block any additional non-TCP connections. • None. No action. This is the default.
Track	Specify whether to log non-TCP connections that exceed the Max. Percent Non-TCP Traffic threshold, by selecting one of the following: • Log. Log the connections. • None. Do not log the connections. This is the default.
Max. Percent Non-TCP Traffic	Type the maximum percentage of state table capacity allowed for non-TCP connections. The default value is 0%.

IP and ICMP

This category allows you to enable various IP and ICMP protocol tests, and to configure various protections against IP and ICMP-related attacks. It includes the following:

- ***Packet Sanity*** on page 229
- ***Max Ping Size*** on page 231
- ***IP Fragments*** on page 232
- ***Network Quota*** on page 234
- ***Welchia*** on page 235
- ***Cisco IOS DOS*** on page 236
- ***Null Payload*** on page 238

Packet Sanity

Packet Sanity performs several Layer 3 and Layer 4 sanity checks. These include verifying packet size, UDP and TCP header lengths, dropping IP options, and verifying the TCP flags.

You can configure whether logs should be issued for offending packets.

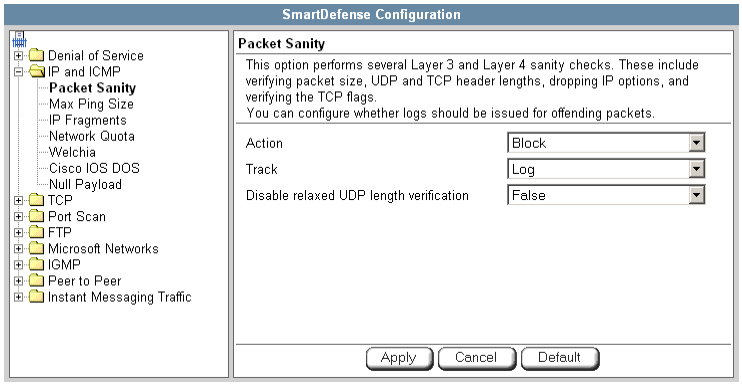


Table 39: Packet Sanity Fields

In this field…	Do this…
Action	Specify what action to take when a packet fails a sanity test, by selecting one of the following: • Block. Block the packet. This is the default. • None. No action.
Track	Specify whether to issue logs for packets that fail the packet sanity tests, by selecting one of the following: • Log. Issue logs. This is the default. • None. Do not issue logs.
Disable relaxed UDP length verification	The UDP length verification sanity check measures the UDP header length and compares it to the UDP header length specified in the UDP header. If the two values differ, the packet may be corrupted. However, since different applications may measure UDP header length differently, the Safe@Office appliance relaxes the UDP length verification sanity check by default, performing the check but not dropping offending packets. This is called relaxed UDP length verification. Specify whether the Safe@Office appliance should relax the UDP length verification sanity check or not, by selecting one of the following: • True. Disable relaxed UDP length verification. The Safe@Office appliance will drop packets that fail the UDP length verification check. • False. Do not disable relaxed UDP length verification. The Safe@Office appliance will not drop packets that fail the UDP length verification check. This is the default.

Max Ping Size

PING (ICMP echo request) is a program that uses ICMP protocol to check whether a remote machine is up. A request is sent by the client, and the server responds with a reply echoing the client's data.

An attacker can echo the client with a large amount of data, causing a buffer overflow. You can protect against such attacks by limiting the allowed size for ICMP echo requests.

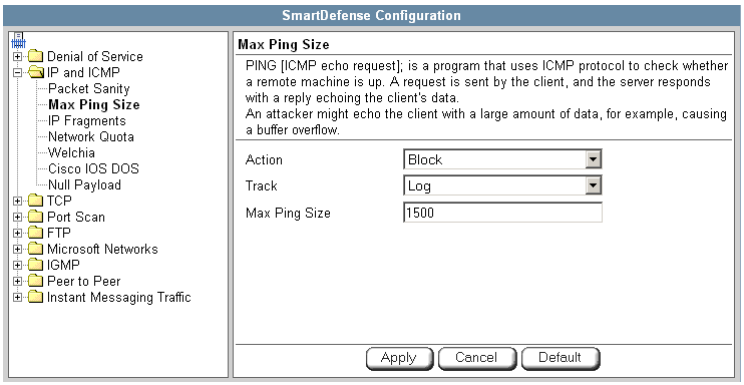


Table 40: Max Ping Size Fields

In this field…	Do this…
Action	Specify what action to take when an ICMP echo response exceeds the Max Ping Size threshold, by selecting one of the following: • Block. Block the request. This is the default. • None. No action.
Track	Specify whether to log ICMP echo responses that exceed the Max Ping Size threshold, by selecting one of the following: • Log. Log the responses. This is the default. • None. Do not log the responses.

In this field...	Do this...
Max Ping Size	Specify the maximum data size for ICMP echo response. The default value is 1500.

IP Fragments

When an IP packet is too big to be transported by a network link, it is split into several smaller IP packets and transmitted in fragments. To conceal a known attack or exploit, an attacker might imitate this common behavior and break the data section of a single packet into several fragmented packets. Without reassembling the fragments, it is not always possible to detect such an attack. Therefore, the Safe@Office appliance always reassembles all the fragments of a given IP packet, before inspecting it to make sure there are no attacks or exploits in the packet.

You can configure how fragmented packets should be handled.

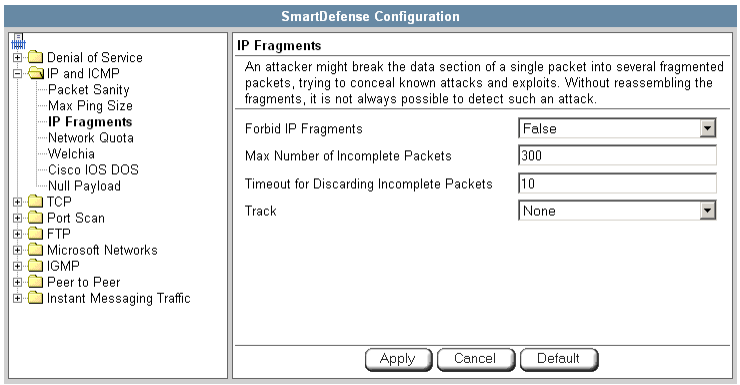


Table 41: IP Fragments Fields

In this field…	Do this…
Forbid IP Fragments	Specify whether all fragmented packets should be dropped, by selecting one of the following: • True. Drop all fragmented packets. • False. No action. This is the default. Under normal circumstances, it is recommended to leave this field set to False. Setting this field to True may disrupt Internet connectivity, because it does not allow any fragmented packets.
Max Number of Incomplete Packets	Type the maximum number of fragmented packets allowed. Packets exceeding this threshold will be dropped. The default value is 300.
Timeout for Discarding Incomplete Packets	When the Safe@Office appliance receives packet fragments, it waits for additional fragments to arrive, so that it can reassemble the packet. Type the number of seconds to wait before discarding incomplete packets. The default value is 10.
Track	Specify whether to log fragmented packets, by selecting one of the following: • Log. Log all fragmented packets. • None. Do not log the fragmented packets. This is the default.

Network Quota

An attacker may try to overload a server in your network by establishing a very large number of connections per second. To protect against Denial Of Service (DoS) attacks, Network Quota enforces a limit upon the number of connections per second that are allowed from the same source IP address.

You can configure how connection that exceed that limit should be handled.

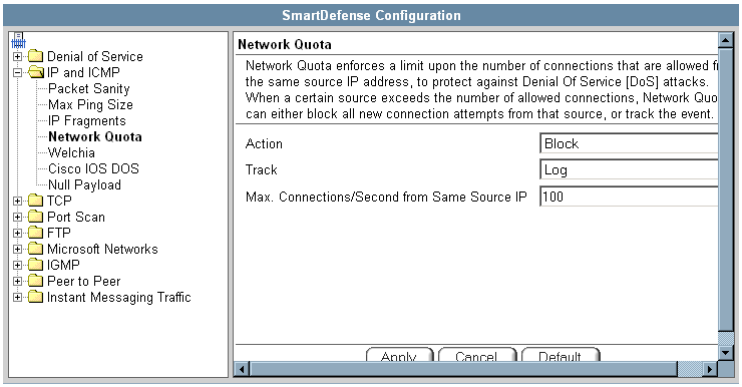


Table 42: Network Quota Fields

In this field…	Do this…
Action	Specify what action to take when the number of network connections from the same source reaches the Max. Connections/Second per Source IP threshold. Select one of the following: • Block. Block all new connections from the source. Existing connections will not be blocked. This is the default. • None. No action.
Track	Specify whether to log connections from a specific source that exceed the Max. Connections/Second per Source IP threshold, by selecting one of the following: • Log. Log the connections. This is the default. • None. Do not log the connections.