Check Point Safe@Office

Internet Security Appliance

User Guide

Version 8.0

Part No: 700797, April 2008

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 network with the highest level of security. However, no single security product can provide you with absolute protection. We recommend using additional security measures to secure highly valuable or sensitive information.

Contents

About This Guide

To make finding information in this guide 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 or ADSL
500W	Safe@Office 500W *only*, with or without the Power Pack or ADSL
Power Pack	Safe@Office 500 or Safe@Office 500W, with or without ADSL, with the Power Pack *only*
USB	All products with USB ports – specifically, Safe@Office 500W, Safe@Office 500W ADSL, and Safe@Office 500 ADSL
ADSL	Safe@Office 500 or Safe@Office 500W, with or without the Power Pack, with ADSL *only*
~~ADSL~~	Safe@Office 500 or Safe@Office 500W, with or without the Power Pack, *without* ADSL *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, with and without an integrated ADSL modem. 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 500 ADSL Internet Security Appliance
- Safe@Office 500W Wireless Security Appliance
- Safe@Office 500W ADSL Wireless Internet 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.

Product Features

Table 1: Safe@Office Features

Feature	Safe@Office 500	Safe@Office 500W	Safe@Office 500 ADSL	Safe@Office 500W ADSL
SKU Prefix	CPSB-500G-n	CPSB-500WG-n	CPSB-500G-n-ADSL	CPSB-500WG-n-ADSL
Concurrent Users	5/25/Unlimited			
Capacity				
Firewall Throughput	190 Mbps			
VPN Throughput	35 Mbps			

Concurrent Firewall Connections	8,000			
Hardware Features				
4-Port LAN Switch	10/100 Mbps			
WAN Port	Ethernet, 10/100 Mbps		ADSL2+	
ADSL Standards	—		ADSL2, ADSL2+, T.1413 G.DMT (G.992.1) G.Lite (G.992.2) Either: ANNEX A (ADSL over POTS) Or: ANNEX B (ADSL over ISDN)	
DMZ/WAN2 Port	10/100 Mbps			
Dialup Backup	With external serial / USB modem			
Console Port (Serial)	✓			
Print Server	—	✓	✓	✓
USB 2.0 Ports	—	2	2	2
Firewall & Security Features				
Check Point Stateful Inspection Firewall	✓			
Application Intelligence	✓			

SmartDefense™ (IPS)	✓
Network Address Translation (NAT)	✓
Four Preset Security Policies	✓
Anti-spoofing	✓
Voice over IP Support	SIP, H.323
Instant Messenger Blocking / Monitoring	✓
P2P File Sharing Blocking / Monitoring	✓
Port-based and Tag-based VLAN	✓*
Port-based Security (802.1x)	✓*
EAP Authenticator	✓
Web Rules	✓
Secure HotSpot (Guest Access)	✓*
VPN	
VPN Tunnels	100

VPN Server with OfficeMode and RADIUS Support	SecuRemote, L2TP	
Site-to-Site VPN Gateway	✓	
Route-based VPN	✓	
Backup VPN Gateways	✓	
Remote Access VPN Client	SecuRemote (Included)	
IPSEC Features	Hardware-accelerated DES, 3DES, AES, MD5, SHA-1, Hardware Random Number Generator (RNG), Internet Key Exchange (IKE), Perfect Forward Secrecy (PFS), IPSEC Compression, IPSEC NAT Traversal (NAT-T), IPSEC VPN Pass-through	
Networking		
Supported Internet Connection Methods	Static IP, DHCP, PPPoE, PPTP, Telstra, Cable, Dialup	Static IP, DHCP, PPPoE, PPTP, Telstra, Cable, EoA, PPPoA, IPoA, Dialup
Transparent Bridge Mode	✓	
Spanning Tree Protocol (STP)	✓	
Traffic Shaper (QoS)	Basic/Advanced*	
Traffic Monitoring	✓	

Dead Internet Connection Detection (DCD)	✓
WAN Load Balancing	✓
Backup Internet Connection	✓
DHCP Server, Client, and Relay	✓
DNS Server	✓
MAC Cloning	✓
Network Address Translation (NAT) Rules	✓
Static Routes, Source Routes, and Service-Based Routes	✓
Ethernet Cable Type Recognition	✓
DiffServ Tagging	✓*
Automatic Gateway Failover (HA)	✓*
Dynamic Routing	✓*

Management	
Central Management	SMP
Local Management	HTTP / HTTPS / SSH / SNMP / Serial CLI
Remote Desktop	Integrated Microsoft Terminal Services Client
Local Diagnostics Tools	Ping, WHOIS, Packet Sniffer, Status Monitor, Traffic Monitor, My Computers Display, Connection Table Display, Network Interface Monitor, VPN Tunnel Monitor, Routing Table Display, Event Log, Security Log
NTP Automatic Time Setting	✓
Rapid Deployment	✓
Hardware Specifications	
Power	100/110/120/210/220/230VAC (Linear Power Adapter) or 100~240VAC (Switched Power Adapter)
Mounting Options	Desktop, Wall, or Rack Mounting**
Warranty	1 Year Hardware

* Requires Power Pack upgrade CPSB-500-UPG-PPACK.

** Rack mounting requires the optional rack mounting kit (sold separately).

Wireless Features

Table 2: Safe@Office Wireless Features

Feature	Safe@Office 500W / Safe@Office 500W ADSL
Wireless Protocols	802.11b (11 Mbps), 802.11g (54 Mbps), Super G (108 Mbps)**
Wireless Security	VPN over Wireless, WEP, WPA2 (802.11i), WPA-Personal, WPA-Enterprise, 802.1x
Wireless QoS (WMM)	✓
Dual Diversity Antennas	✓
Virtual Access Points (VAP)	✓*
Wireless Distribution System (WDS) Links	✓*
Wireless Range (Standard Mode)	Up to 100 m Indoors and 300 m Outdoors
Wireless Range (XR Mode)**	Up to 300 m Indoors and 1 km Outdoors

* Requires Power Pack upgrade CPSB-500-UPG-PPACK.

** Super G and XR mode are only available with select wireless network adapters. Actual ranges are subject to change in different environments.

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

These services require an additional purchase of subscription. For more information, contact your Check Point reseller.

Software Requirements

One of the following browsers:

- Microsoft Internet Explorer 6.0 or higher
- Netscape Navigator 6.0 and higher
- Mozilla Firefox

Note: For proper operation of the Safe@Office Portal, disable any pop-up blockers for http://my.firewall.

Getting to Know Your Safe@Office 500 Appliance

500

Package Contents

The Safe@Office 500 package includes the following:

- Safe@Office 500 Internet Security Appliance
- Power supply
- CAT5 Straight-through Ethernet cable
- Getting Started Guide
- Documentation CDROM
- Wall mounting kit
- RS232 serial adaptor (RJ45 to DB9); model SBX-166LHGE-5 only

Network Requirements

- 10BaseT or 100BaseT Network Interface Card installed on each computer
- CAT 5 STP (Category 5 Shielded Twisted Pair) Straight Through Ethernet cable for each attached device
- A broadband Internet connection via cable or DSL modem with Ethernet interface (RJ-45)

Rear Panel

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

Figure 1: Safe@Office 500 SBX-166LHGE-5 Appliance Rear Panel

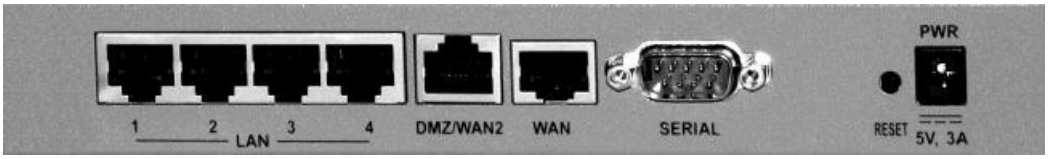


Figure 2: Safe@Office 500 SBX-166LHGE-6 Appliance Rear Panel

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

Table 3: Safe@Office 500 Appliance Rear Panel Elements

Label	Description
PWR	A power jack used for supplying power to the unit. Connect the supplied power supply 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.
Serial	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. Depending on the appliance model, this port may have either a DB9 RS232 connector, or an RJ-45 connector. In models with an RJ-45 connector, an RJ-45 to DB9 converter is supplied for your convenience. Warning: Do not connect an Ethernet cable to the RJ-45 serial port.
WAN	Wide Area Network: An Ethernet port (RJ-45) used for connecting your broadband modem, a wide area network router, or a network leading to the Internet.
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 following table.

Table 4: Safe@Office 500 Appliance Status LEDs

LED	State	Explanation
PWR/SEC	Off	Power off
	Flashing quickly (Green)	System boot-up, or rapid deployment in progress
	Flashing slowly (Green)	Establishing Internet connection
	Flashing (Red)	Hacker attack blocked, or error occurred during rapid deployment process
	On (Green)	Normal operation
	On (Red)	Error
LAN 1-4/ WAN/ DMZ/WAN2	LINK/ACT Off, 100 Off	Link is down

LED	State	Explanation
	LINK/ACT On, 100 Off	10 Mbps link established for the corresponding port
	LINK/ACT On, 100 On	100 Mbps link established for the corresponding port
	LNK/ACT Flashing	Data is being transmitted/received
VPN	Off	No VPN activity
	Flashing (Green)	VPN activity
	On (Green)	VPN tunnels established, no activity
Serial	Off	No Serial port activity
	Flashing (Green)	Serial port activity

Getting to Know Your Safe@Office 500W Appliance

500W

Package Contents

The Safe@Office 500W package includes the following:

- Safe@Office 500W Internet Security Appliance
- Power supply
- CAT5 Straight-through Ethernet cable
- Getting Started Guide
- Documentation CDROM
- Wall mounting kit
- RS232 serial adaptor (RJ45 to DB9); model SBXW-166LHGE-5 only
- Two antennas
- USB extension cable

Network Requirements

- 10BaseT or 100BaseT Network Interface Card installed on each computer
- CAT 5 STP (Category 5 Shielded Twisted Pair) Straight Through Ethernet cable for each attached device
- An 802.11b, 802.11g or 802.11 Super G wireless card installed on each wireless station
- A broadband Internet connection via cable or DSL modem with Ethernet interface (RJ-45)

Rear Panel

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

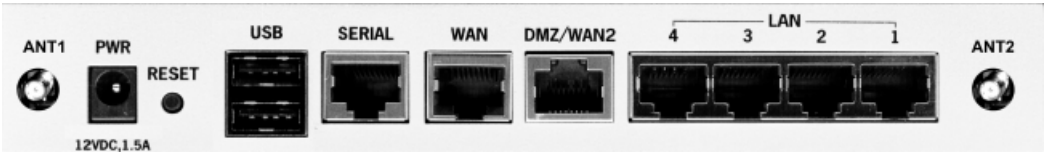


Figure 4: Safe@Office 500W SBXW-166LHGE-5 Appliance Rear Panel

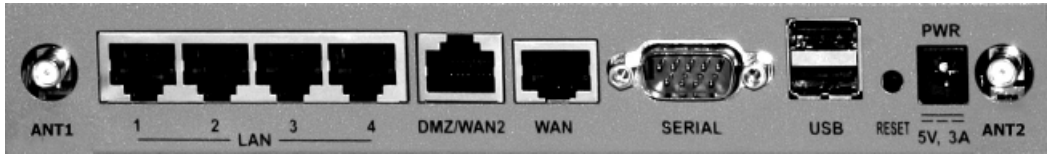


Figure 5: Safe@Office 500W SBXW-166LHGE-6 Appliance Rear Panel

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

Table 5: Safe@Office 500W Appliance Rear Panel Elements

Label	Description
PWR	A power jack used for supplying power to the unit. Connect the supplied power supply 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 or modems
Serial	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. Depending on the appliance model, this port may have either a DB9 RS232 connector, or an RJ-45 connector. In models with an RJ-45 connector, an RJ-45 to DB9 converter is supplied for your convenience. Warning: Do not connect an Ethernet cable to the RJ-45 serial port.
WAN	Wide Area Network: An Ethernet port (RJ-45) used for connecting your broadband modem, a wide area network router, or a network leading to the Internet.
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.

Label	Description
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 6: Safe@Office 500W Appliance Front Panel

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

Table 6: Safe@Office 500W Appliance Status LEDs

LED	State	Explanation
PWR/SEC	Off	Power off
	Flashing quickly (Green)	System boot-up, or rapid deployment in progress
	Flashing slowly (Green)	Establishing Internet connection
	Flashing (Red)	Hacker attack blocked, or error occurred during rapid deployment process
	On (Green)	Normal operation
	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
	LINK/ACT On, 100 On	100 Mbps link established for the corresponding port
	LNK/ACT Flashing	Data is being transmitted/received
VPN	Off	No VPN activity
	Flashing (Green)	VPN activity
	On (Green)	VPN tunnels established, no activity

LED	State	Explanation
Serial	Off	No Serial port activity
	Flashing (Green)	Serial port activity
USB	Off	No USB port activity
	Flashing (Green)	USB port activity
WLAN	Off	No WLAN activity
	Flashing (Green)	WLAN activity

Getting to Know Your Safe@Office 500 ADSL Appliance

ADSL

Package Contents

The Safe@Office 500 ADSL package includes the following:

- Safe@Office 500 ADSL Internet Security Appliance
- Power supply
- CAT5 Straight-through Ethernet cable
- Getting Started Guide
- Documentation CDROM
- Wall mounting kit
- RS232 serial adaptor (RJ45 to DB9)
- USB extension cable
- RJ11 telephone cable

Network Requirements

- 10BaseT or 100BaseT Network Interface Card installed on each computer
- CAT 5 STP (Category 5 Shielded Twisted Pair) Straight Through Ethernet cable for each attached device
- An ADSL line suitable for your appliance model:
  - For Annex A ADSL models, an ADSL over POTS line (regular telephone line)
  - For Annex B ADSL models, an ADSL over ISDN line (digital line)
- A splitter with a micro-filter, installed on all the jacks connected to the same phone line
- If desired, you can connect your appliance to an external broadband Internet connection via a cable or DSL modem with an Ethernet interface (RJ-45).

Rear Panel

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

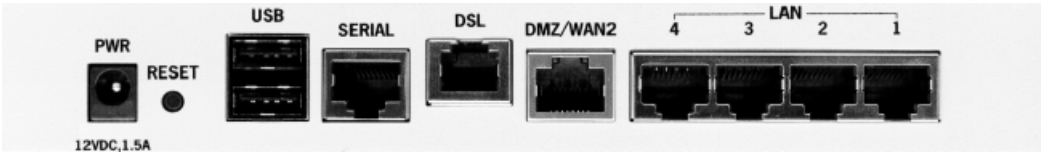


Figure 7: Safe@Office 500 ADSL Appliance Rear Panel

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

Table 7: Safe@Office 500 ADSL Appliance Rear Panel Elements

Label	Description
PWR	A power jack used for supplying power to the unit. Connect the supplied power supply 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 or modems
Serial	An RJ-45 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. An RJ-45 to DB9 converter is supplied for your convenience. Warning: Do not connect an Ethernet cable to the RJ-45 serial port.
DSL	An RJ-11 ADSL port used for connecting the integrated ADSL modem to an ADSL line. A splitter with a micro-filter is usually required when connecting this port to the phone jack. If unsure, check with your ADSL service provider. Before connecting this port to the line, make sure that you are using the correct Safe@Office model for your phone line: Annex A for POTS (regular) phone lines, and Annex B for ISDN (digital) phone lines. Your Safe@Office model's ADSL annex type appears on the bottom of the appliance.

Label	Description
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 ADSL appliance includes several status LEDs that enable you to monitor the appliance's operation.

Figure 8: Safe@Office 500 ADSL Appliance Front Panel

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

Table 8: Safe@Office 500 ADSL Appliance Status LEDs

LED	State	Explanation
PWR/SEC	Off	Power off
	Flashing quickly (Green)	System boot-up, or rapid deployment in progress
	Flashing slowly (Green)	Establishing Internet connection
	Flashing (Red)	Hacker attack blocked, or error occurred during rapid deployment process

LED	State	Explanation
	On (Green)	Normal operation
	On (Red)	Error
LAN 1-4/ DMZ/WAN2	LINK/ACT Off, 100 Off	Link is down
	LINK/ACT On, 100 Off	10 Mbps link established for the corresponding port
	LINK/ACT On, 100 On	100 Mbps link established for the corresponding port
	LNK/ACT Flashing	Data is being transmitted/received
DSL	Link Off	Link is down
	Link Flashing	Establishing ADSL connection
	Link On	ADSL connection established
	DAT Off	ADSL line is idle
	DAT Flashing	Data is being transmitted/received
VPN	Off	No VPN activity
	Flashing (Green)	VPN activity
	On (Green)	VPN tunnels established, no activity
Serial	Off	No Serial port activity
	Flashing (Green)	Serial port activity
USB	Off	No USB port activity

LED	State	Explanation
	Flashing (Green)	USB port activity

Getting to Know Your Safe@Office 500W ADSL Appliance

500W ADSL

Package Contents

The Safe@Office 500W ADSL package includes the following:

- Safe@Office 500W ADSL Internet Security Appliance
- Power supply
- CAT5 Straight-through Ethernet cable
- Getting Started Guide
- Documentation CDROM
- Wall mounting kit
- RS232 serial adaptor (RJ45 to DB9)
- Two antennas
- USB extension cable
- RJ11 telephone cable

Network Requirements

- 10BaseT or 100BaseT Network Interface Card installed on each computer
- CAT 5 STP (Category 5 Shielded Twisted Pair) Straight Through Ethernet cable for each attached device
- An ADSL line suitable for your appliance model:
  - For Annex A ADSL models, an ADSL over POTS line (regular telephone line)
  - For Annex B ADSL models, an ADSL over ISDN line (digital line)
- A splitter with a micro-filter, installed on all the jacks connected to the same phone line
- If desired, you can connect your appliance to an external broadband Internet connection via a cable or DSL modem with an Ethernet interface (RJ-45).
- An 802.11b, 802.11g or 802.11 Super G wireless card installed on each wireless station

Rear Panel

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

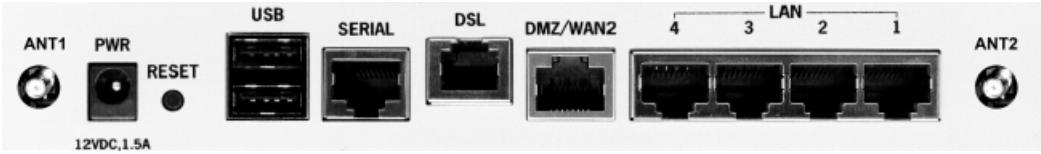


Figure 9: Safe@Office 500W ADSL Appliance Rear Panel

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

Table 9: Safe@Office 500W ADSL Appliance Rear Panel Elements

Label	Description
PWR	A power jack used for supplying power to the unit. Connect the supplied power supply to this jack.
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 or modems
Serial	An RJ-45 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. An RJ-45 to DB9 converter is supplied for your convenience. Warning: Do not connect an Ethernet cable to the RJ-45 serial port.

Label	Description
DSL	An RJ-11 ADSL port used for connecting the integrated ADSL modem to an ADSL line. A splitter with a micro-filter is usually required when connecting this port to the phone jack. If unsure, check with your ADSL service provider. Before connecting this port to the line, make sure that you are using the correct Safe@Office model for your phone line: Annex A for POTS (regular) phone lines, and Annex B for ISDN (digital) phone lines. Your Safe@Office model's ADSL annex type appears on the bottom of the appliance.
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.
ANT1 / ANT2	Antenna connectors, used to connect the supplied wireless antennas .

Front Panel

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

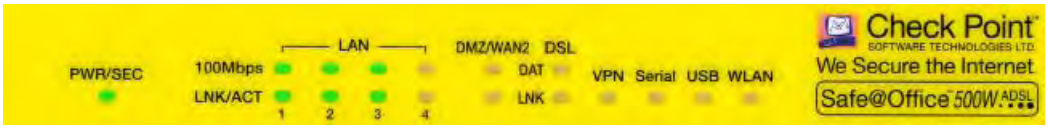


Figure 10: Safe@Office 500W ADSL Appliance Front Panel

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

Table 10: Safe@Office 500 ADSL Appliance Status LEDs

LED	State	Explanation
PWR/SEC	Off	Power off
	Flashing quickly (Green)	System boot-up, or rapid deployment in progress
	Flashing slowly (Green)	Establishing Internet connection
	Flashing (Red)	Hacker attack blocked, or error occurred during rapid deployment process
	On (Green)	Normal operation
	On (Red)	Error
LAN 1-4/ DMZ/WAN2	LINK/ACT Off, 100 Off	Link is down
	LINK/ACT On, 100 Off	10 Mbps link established for the corresponding port
	LINK/ACT On, 100 On	100 Mbps link established for the corresponding port
	LNK/ACT Flashing	Data is being transmitted/received
DSL	Link Off	Link is down
	Link Flashing	Establishing ADSL connection
	Link On	ADSL connection established
	DAT Off	ADSL line is idle
	DAT Flashing	Data is being transmitted/received

LED	State	Explanation
VPN	Off	No VPN activity
	Flashing (Green)	VPN activity
	On (Green)	VPN tunnels established, no activity
Serial	Off	No Serial port activity
	Flashing (Green)	Serial port activity
USB	Off	No USB port activity
	Flashing (Green)	USB port activity
WLAN	Off	No WLAN activity
	Flashing (Green)	WLAN activity

Contacting Technical Support

In case of 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

Safe@Office Security

This chapter explains the basic security concepts on which Safe@Office security is based.

This chapter includes the following topics:

Introduction to Information Security

Network security is but a small part of information security, which in turn is only a fraction of general security. In order to understand why the Safe@Office appliance is the best product for securing the business network, we must first examine information security requirements in general.

Information is Valuable!

The most valuable asset an organization has is its information. The type of information maintained by an organization depends on the organization's type and purpose. For example:

- Almost every organization stores information about its operations, such as employees' names and other personal details, salaries, and so on.
- Depending on the role of different governmental offices, they may store personal information about citizens, residential addresses, car licenses registration, and so on.
- The army stores information about its soldiers, weapons inventory, and intelligence information about other armies. Much of this information is confidential.
- A bank stores information about its customers' accounts, their money transactions, ATM machine access codes, and so on. Much of this information is confidential.

- Commercial companies store information about their revenues, business and marketing plans, current and future product lines, information about competitors, and so on.

Just as the type of information may differ from organization to organization, the form in which it is stored may vary. For example, some forms of information are:

- Information recorded in written media, such as paper documents, books, and files
- Knowledge that is stored in a person's mind and can be exchanged verbally
- Information stored on electronic media, such as computers' hard drives, CDs, and tapes

The form in which an organization stores its information may make the information more or less accessible to people outside the organization.

Why Protect Business Information?

There are various reasons why it is necessary to protect business information:

- To prevent the theft, abuse, misuse, or any form of damage to crucial information

  For example, no business wants to find its customer list or future secret product line plans in the hands of the competition.

- To comply with local laws

  Local laws may enforce the protection, integrity, and availability of specific information, such as an individual's personal details, in order to respect the individual's right to privacy. Local laws may also enforce the security requirements made in the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

- To comply with another organization's security requirements

  Some organizations require their business partners to comply with international standards of security.

Information Security Challenges

The challenges of information security can be divided into the following areas:

- Confidentiality and Privacy - Ensuring that only the intended recipients can read certain information
- Authentication - Ensuring that information is actually sent by the stated sender
- Integrity - Ensuring that the original information was not altered and that no one tampered with it
- Availability - Ensuring that important information can be accessed at all times and places

The Security Policy

In order to meet these challenges, an organization must create and enforce a *security policy*. A security policy is a set of rules that defines how and by whom sensitive information should be accessed, handled, and distributed, both within and outside of the organization. For example, a security policy may include the following rules regarding visitors who arrive at an enterprise building's lobby:

- Visitors must sign in at the entrance desk.
- Visitors must wear a visitor badge and be escorted while in the building.
- Visitors cannot use their badge to open electronic doors.

Other types of security policy rules and measures might be:

- Only the executive manager has access to financial reports.
- Visitors must open their bags for a security check.
- Surveillance cameras should be positioned in the area of the building.
- Passwords must be changed on a daily basis.
- Confidential papers must be shredded after use.

An organization's security policy is usually designed by a person who is in charge of handling all security matters for the organization. This person is called a *security manager*.

In order for a security policy be effective, it must be accompanied by the following measures:

- Awareness - A security policy must be accompanied by steps taken to increase the employees' awareness of security issues. If employees are unaware of a security policy rule and the reason for it, they are likely to break it.
- Enforcement - To enforce a security policy, an organization can take various measures, both human and electronic. For example:
    - Installing surveillance cameras in strategic locations throughout the organization
    - Positioning human guards who have the authority to prevent other people from entering the premises or certain areas on the premises
    - Installing alarms that are triggered upon certain conditions
    - Using magnetic identification tags to enforce and log access permissions to different areas on the premises
    - Using “red phones” to encrypt highly confidential voice phone calls
- Updating - A security policy is a living thing that must be updated from time to time according to changing situations.

Unfortunately, even when a security policy is accompanied by these measures, its effectiveness is limited against a person with malicious intent.

Computer and Network Security

A great deal of an organization's existing information is processed and stored electronically by single (standalone) computers or computer networks. Therefore, an attack on an organization's computers or computer networks can result in extensive information theft or abuse. However, computers and computer networks today are not just tools used to store information; they are the heart of an organization's operations and crucial to its communication and business transactions. For example:

- Nowadays, most of an organization's communication and business transactions are conducted via email (regardless of the organization's size).
- Online stores process orders and supply products over the Internet.
- Emerging technology today allows an organization's branch offices to communicate, share data, and even establish low-cost VoIP (Voice over IP) communications, rather then using the traditional phone system.
- Applications are hosted on a main computer rather than on personal workstations. This helps organizations share application resources. For example, in service departments, the customer database is located on a main computer, while all customer relations transactions are managed by software clients running on the agents' computers.
- In order to withdraw money from any ATM machine, your PIN and the details on your magnetic card are scanned and verified against the details on the main bank computer.
- A department store in New York can query the inventory of the main warehouse located in Chicago and enter orders for missing products, all in real time.

In other words, on top of the damage done by computer information theft or abuse, unauthorized access to a computer or a computer network can seriously damage the entire organization's essential operations, communications, and productivity. For example:

- An online store's Web site can be hacked, so customers cannot enter orders.
- An unauthorized user can take advantage of an organization's email server to send unsolicited bulks of email. As a result, the organization's Internet communication lines will be overloaded, and employees in the organization will be unable to send or receive emails.

Since computer and network security has become a central part of information and general security, security managers must either have an understanding of computers and networking, or work closely with network administrators and network security specialists.

Network Security and the Small Business

Network security has been and continues to be a major concern for large, enterprise-sized organizations. However, small businesses are no less of a target for Internet attacks, and they require a similar network security level, for the following reasons:

- Small business owners lack awareness of network security and unwittingly leave the door open to threats from within the network. For example, peer-to-peer applications are a source of virus-infected files, Trojans, and worms, any of which can be used to steal confidential information such as credit card numbers; however, many small business owners are unaware of the risk, and therefore do not block their employees from using peer-to-peer applications.
- Large businesses have the funds and expertise to constantly enhance their security and are therefore a difficult target for hackers. This makes small businesses a far more attractive target for network attacks.
- The state's awareness of privacy and data protection is enforced through legislation. For example, the Health Insurance Portability and Accountability Act (HIPAA) that was enacted by the U.S. Congress in 1996 gives patients access to their medical files electronically, and therefore strictly defines the requirements for protecting electronic confidential data.

Not only are small businesses more vulnerable to Internet attacks, but due to their relative lack of technical and financial resources, they may suffer more damage than large organizations and the recovery may be more difficult.

The Safe@Office Firewall

What Is a Firewall?

The most effective way to secure an Internet link is to put a firewall between the local network and the Internet. A *firewall* is a system designed to prevent unauthorized access to or from a secured network. Firewalls act as locked doors between internal and external networks: data that meets certain requirements is allowed through, while unauthorized data is not.

To provide robust security, a firewall must track and control the flow of communication passing through it. To reach control decisions for TCP/IP-based services, (such as whether to accept, reject, authenticate, encrypt, and/or log communication attempts), a firewall must obtain, store, retrieve, and manipulate information derived from all communication layers and other applications.

Security Requirements

In order to make control decisions for new communication attempts, it is not sufficient for the firewall to examine packets in isolation. Depending upon the communication attempt, both the communication state (derived from past communications) and the application state (derived from other applications) may be critical in the control decision. Thus, to ensure the highest level of security, a firewall must be capable of accessing, analyzing, and utilizing the following:

- Communication information - Information from all seven layers in the packet
- Communication-derived state - The state derived from previous communications. For example, the outgoing PORT command of an FTP session could be saved so that an incoming FTP data connection can be verified against it.
- Application-derived state - The state information derived from other applications. For example, a previously authenticated user would be allowed access through the firewall for authorized services only.
- Information manipulation - The ability to perform logical or arithmetic functions on data in any part of the packet. For example, the ability to encrypt packets.

Old Firewall Technologies

Older firewall technologies, such as packet filtering and application-layer gateways, are still in use in some environments. It is important to familiarize yourself with these technologies, so as to better understand the benefits and advantages of the Check Point Stateful Inspection firewall technology.

Packet Filters

Historically implemented on routers, packet filters filter user-defined content, such as IP addresses. They examine a packet at the network or transport layer and are application-independent, which allows them to deliver good performance and scalability.

Packet filters are the least secure type of firewall, as they are not application-aware, meaning that they cannot understand the context of a given communication. This makes them relatively easy targets for unauthorized entry to a network. A limitation of this type of filtering is its inability to provide security for basic protocols.

Packet filters have the following advantages and disadvantages:

Table 11: Packet Filter Advantages and Disadvantages

Advantages	Disadvantages
Application independence	Low security
High performance	No screening above the network layer
Scalability	

Application-Layer Gateways

Application-layer gateways improve security by examining all application layers, bringing context information into the decision-making process. However, the method they use to do this disrupts the client/server model, reducing scalability. Ordinarily, a client sends requests for information or action according to a specific protocol, and the server responds, all in one connection. With application-layer gateways, each client/server communications requires two connections: one from a client to a proxy, and one from a proxy to a server. In addition, each proxy requires a different process (or daemon), making support for new applications a problem.

Application-layer gateways have the following advantages and disadvantages:

Table 12: Application-Layer Gateway Advantages and Disadvantages

Advantages	Disadvantages
Good security	Poor performance
Full application-layer awareness	Limited application support
	Poor scalability (breaks the client/server model)

Check Point Stateful Inspection Technology

Invented by Check Point, Stateful Inspection is the industry standard for network security solutions. A powerful inspection module examines every packet, ensuring that packets do not enter a network unless they comply with the network's security policy.

Stateful Inspection technology implements all necessary firewall capabilities between the data and network layers. Packets are intercepted at the network layer for best performance (as in packet filters), but the data derived from layers 3-7 is accessed and analyzed for improved security (compared to layers 4-7 in application-layer gateways). Stateful Inspection incorporates communication and application-derived state and context information, which is stored and updated dynamically. This provides cumulative data against which subsequent communication attempts can be evaluated. Stateful Inspection also delivers the ability to create virtual-session information for tracking connectionless protocols, such as UDP-based and RPC applications.

Safe@Office appliances use Stateful Inspection technology to analyze all packet communication layers and extract the relevant communication and application state information. The Safe@Office appliance is installed at the entry point to your network, and serves as the gateway for the internal network computers. In this ideal location, the inspection module can inspect all traffic before it reaches the network.

Packet State and Context Information

To track and act on both state and context information for an application is to treat that traffic *statefully*. The following are examples of state and context-related information that a firewall should track and analyze:

- Packet-header information (source and destination address, protocol, source and destination port, and packet length)
- Connection state information (which ports are being opened for which connection)
- TCP and IP fragmentation data (including fragments and sequence numbers)
- Packet reassembly, application type, and context verification (to verify that the packet belongs to the communication session)
- Packet arrival and departure interface on the firewall
- Layer 2 information (such as VLAN ID and MAC address)
- Date and time of packet arrival or departure

The Safe@Office firewall examines IP addresses, port numbers, and any other information required. It understands the internal structures of the IP protocol family and applications, and is able to extract data from a packet's application content and store it, to provide context in cases where the application does not provide it. The Safe@Office firewall also stores and updates the state and context information in dynamic tables, providing cumulative data against which it inspects subsequent communications.

The Stateful Inspection Advantage - Passive FTP Example

In order to discuss the strength of Stateful Inspection technology in comparison to the other firewall technologies mentioned, we will examine the Passive FTP protocol and the ways that firewalls handle Passive FTP traffic pass-through.

FTP connections are unique, since they are established using two sessions or channels: one for command (AKA control) and one for data. The following table describes the steps of establishing a Passive FTP connection, where:

- C is the client port used in the command session,
- D is the client port used in the data session, and
- P is the server port used in the data session.

Table 13: Establishment of Passive FTP Connection

Step	Channel Type	Description	Source	TCP Source Port	Destination	TCP Destination Port
1	CMD	Client initiates a PASV command to the FTP server on port 21	FTP client	C > 1023	FTP server	21
2	CMD	Server responds with data port information P > 1023	FTP server	21	FTP client	C
3	Data	Client initiates data connection to server on port P	FTP client	D > 1023	FTP server	P
4	Data	Server acknowledges data connection	FTP server	P	FTP client	D

The following diagram demonstrates the establishment of a Passive FTP connection through a firewall protecting the FTP server.

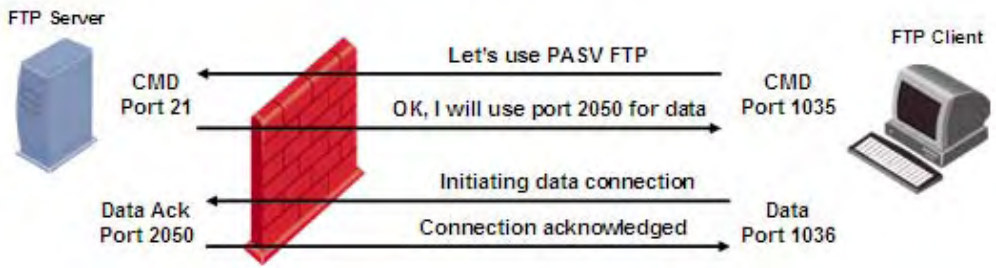


Figure 11: Establishment of Passive FTP Connection

From the FTP server's perspective, the following connections are established:

- Command connection from the client on a port greater than 1023, to the server on port 21
- Data connection from the client on a port greater than 1023, to the server *on a port greater than 1023*

The fact that both of the channels are established by the client presents a challenge for the firewall protecting the FTP server: while a firewall can easily be configured to identify incoming command connections over the default port 21, it must also be able to handle incoming data connections over a dynamic port that is negotiated randomly as part of the FTP client-server communication. The following table examines how different firewall technologies handle this challenge:

Table 14: Firewall Technologies and Passive FTP Connections

Firewall Technology	Action
Packet Filter	Packet filters can handle outbound FTP connections in either of the following ways: • By leaving the entire upper range of ports (greater than 1023) open. While this allows the file transfer session to take place over the dynamically allocated port, it also exposes the internal network. • By shutting down the entire upper range of ports. While this secures the internal network, it also blocks other services. Thus packet filters' handling of Passive FTP comes at the expense of either application support or security.
Application-Layer Gateway (Proxy)	Application-layer gateways use an FTP proxy that acts as a go-between for all client-server sessions. This approach overcomes the limitations of packet filtering by bringing application-layer awareness to the decision process; however, it also takes a high toll on performance. In addition, each service requires its own proxy (an FTP proxy for FTP sessions, an HTTP proxy for HTTP session, and so on), and since the application-layer gateway can only support a certain number of proxies, its usefulness and scalability is limited. Finally, this approach exposes the operating system to external threats.

Firewall Technology	Action
Stateful Inspection Firewall	A Stateful Inspection firewall examines the FTP application-layer data in an FTP session. When the client initiates a command session, the firewall extracts the port number from the request. The firewall then records both the client and server's IP addresses and port numbers in an FTP-data pending request list. When the client later attempts to initiate a data connection, the firewall compares the connection request's parameters (ports and IP addresses) to the information in the FTP-data pending request list, to determine whether the connection attempt is legitimate. Since the FTP-data pending request list is dynamic, the firewall can ensure that only the required FTP ports open. When the session is closed, the firewall immediately closes the ports, guaranteeing the FTP server's continued security.

What Other Stateful Inspection Firewalls Cannot Do

The level of security that a stateful firewall provides is determined by the richness of data tracked, and how thoroughly the data is analyzed. Treating traffic statefully requires application awareness. Firewalls without application awareness must open a range of ports for certain applications, which leads to exploitable holes in the firewall and violates security “best practices”.

TCP packet reassembly on all services and applications is a fundamental requirement for any Stateful Inspection firewall. Without this capability, fragmented packets of legitimate connections may be dropped, or those carrying network attacks may be allowed to enter a network. The implications in either case are potentially severe. When a truly stateful firewall receives fragmented packets, the packets are reassembled into their original form. The entire stream of data is analyzed for conformity to protocol definition and for packet-payload validity.

True Stateful Inspection means tracking the state and context of all communications. This requires a detailed level of application awareness. The Safe@Office appliance provides true Stateful Inspection.

Chapter 3

Installing and Setting Up Safe@Office

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.

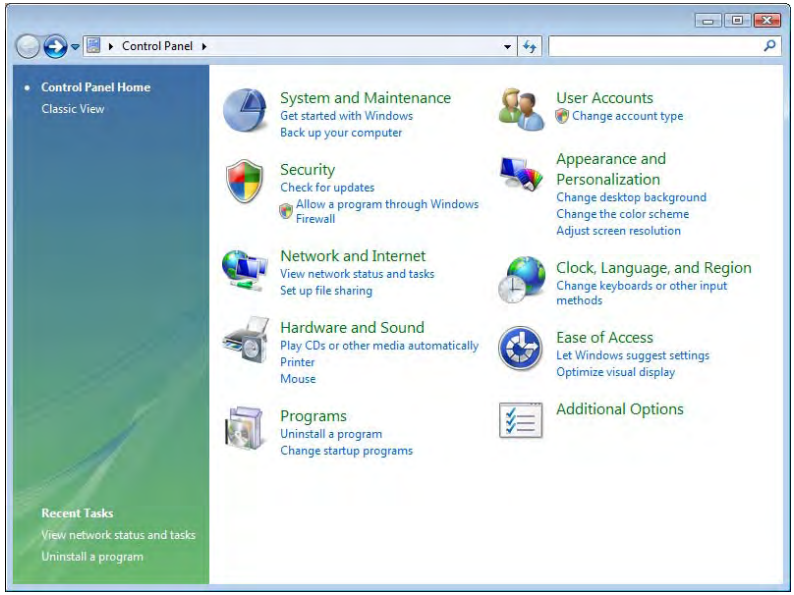
Refer to the relevant section in this guide in accordance with the operating system that runs on your computer. The sections below will guide you through the TCP/IP setup and installation process.

Windows Vista

Checking the TCP/IP Installation

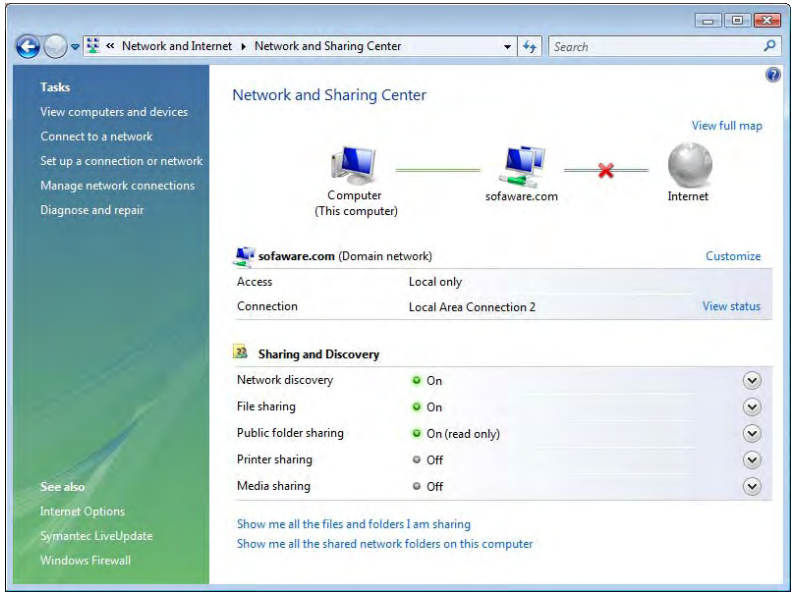
1. Click Start > Control Panel.

   The Control Panel window appears.



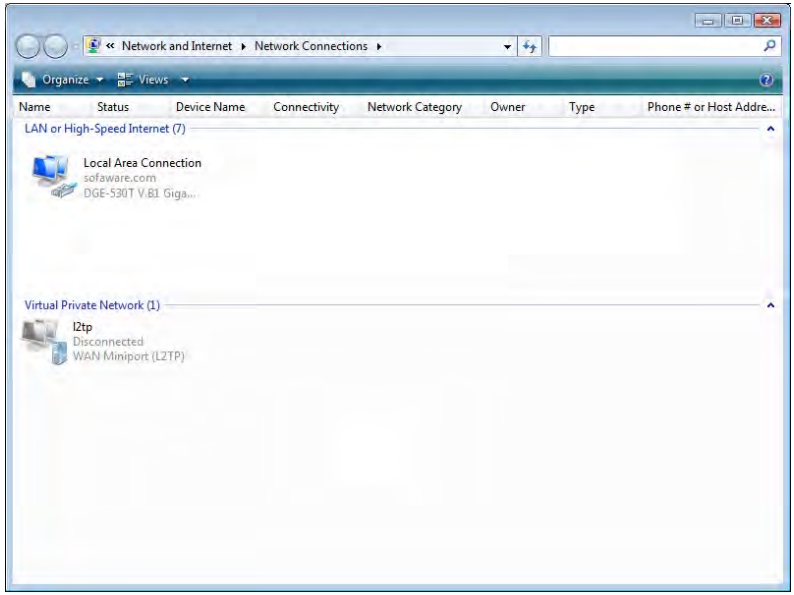
2. Under Network and Internet, click View network status and tasks.

The **Network Sharing Center** screen appears.



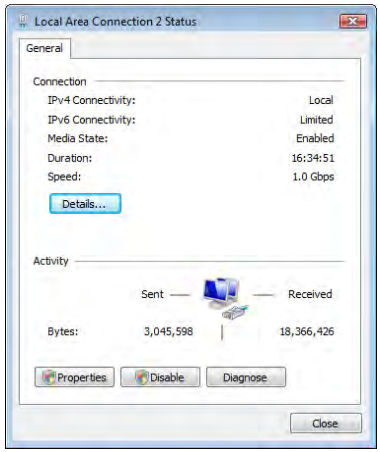
3. In the **Tasks** pane, click **Manage network connections**.

The **Network Connections** screen appears.



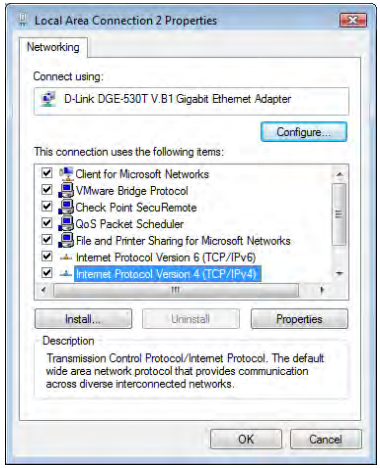
4. Double-click the **Local Area Connection** icon.

   The **Local Area Connection Status** window opens.



5. Click **Properties**.

The Local Area Connection Properties window opens.

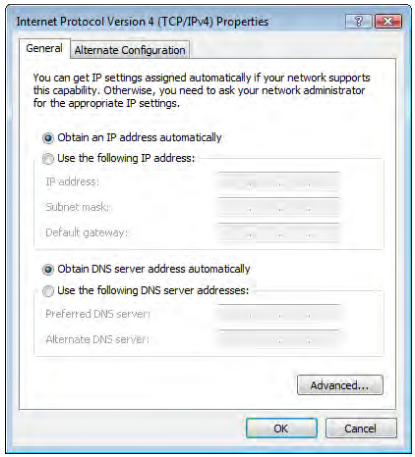


6. Check if Internet Protocol Version 4 (TCP/IPv4) appears in the list box and if it is properly configured with the Ethernet card installed on your computer.

TCP/IP Settings

1. In the Local Area Connection Properties window, double-click the Internet Protocol Version 4 (TCP/IPv4) component, or select it and click Properties.

   The Internet Protocol Version 4 (TCP/IPv4) Properties window appears.



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 Network > My Network page.)

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

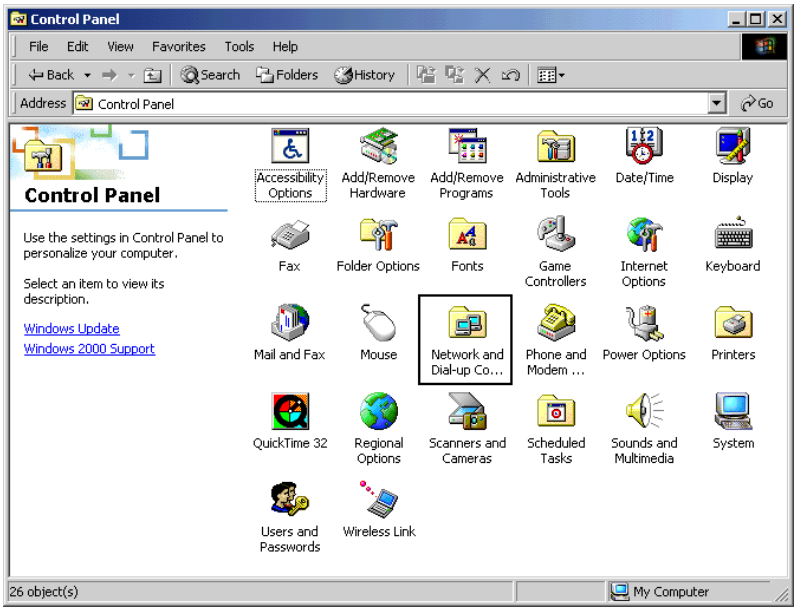
   Your computer is now ready to access your Safe@Office appliance.

Windows 2000/XP

Checking the TCP/IP Installation

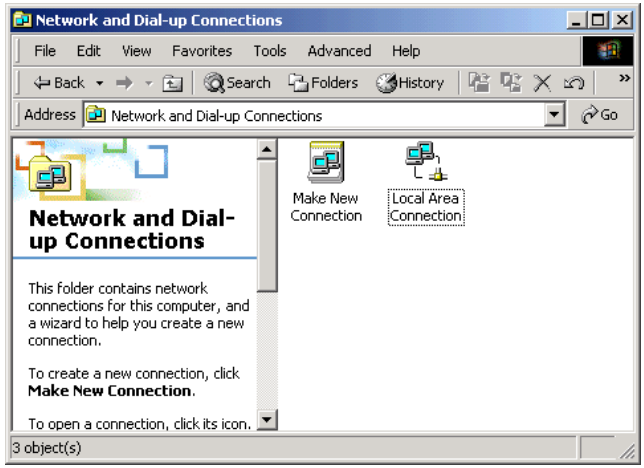
1. Click Start > Settings > Control Panel.

   The Control Panel window appears.



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

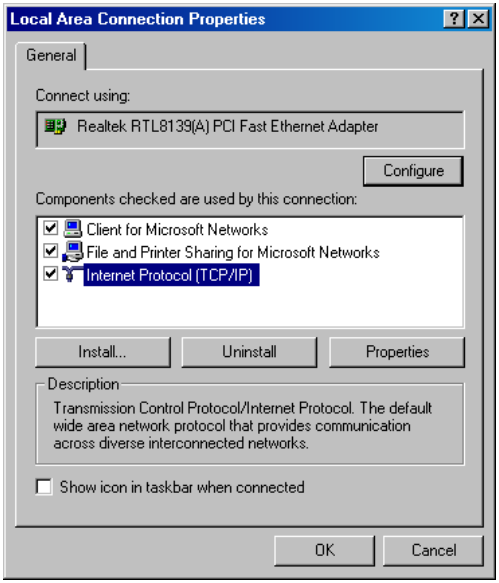
   The **Network and Dial-up Connections** window appears.



3. Right-click the 

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

The Local Area Connection Properties window appears.

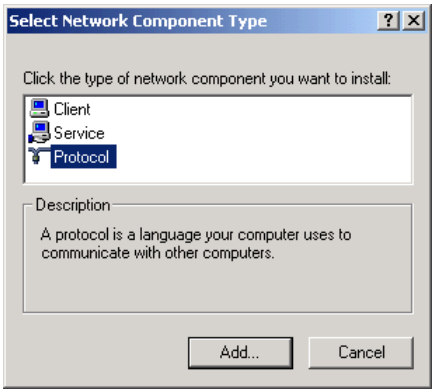


4. In the above window, check if TCP/IP appears in the components list and if it is properly configured with the Ethernet card installed on your computer. If TCP/IP does not appear in the Components list, you must install it as described in the next section.

Installing TCP/IP Protocol

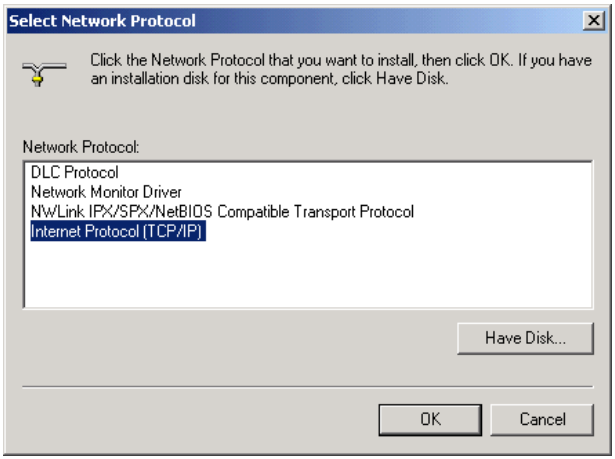
1. In the Local Area Connection Properties window click Install.

   The Select Network Component Type window appears.



2. Select Protocol and click Add.

   The Select Network Protocol window appears.



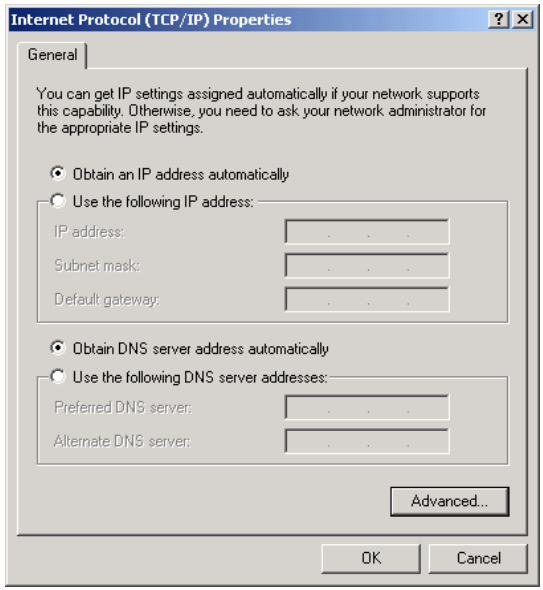
3. Choose Internet Protocol (TCP/IP) and click OK.

   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 Network > My Network page.)

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

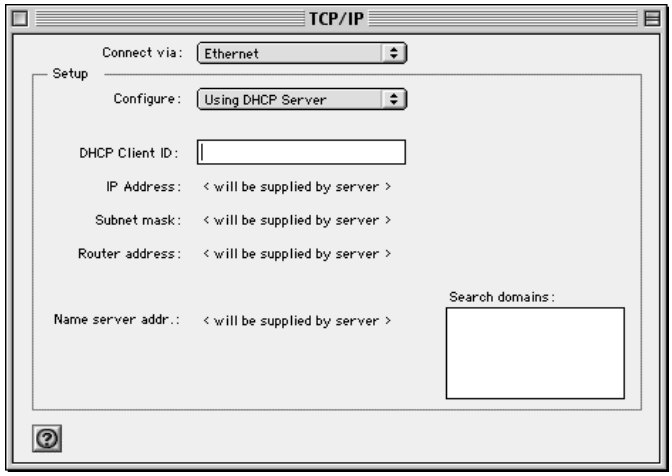
   Your computer is now ready to access your Safe@Office appliance.

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

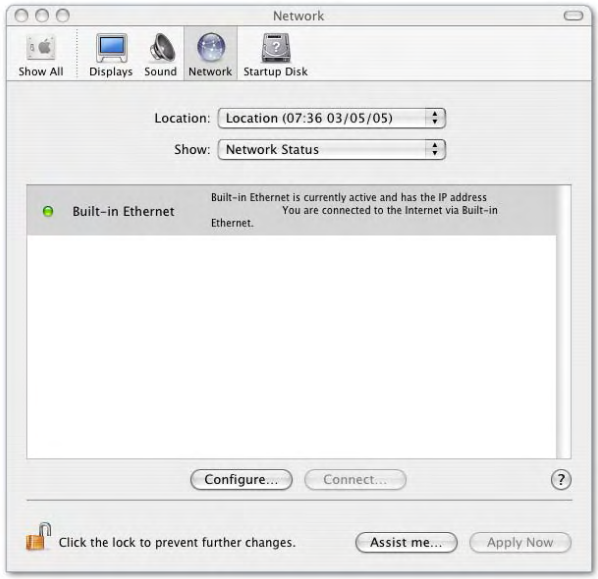
Use the following procedure for setting up the TCP/IP Protocol.

1. Choose Apple -> System Preferences.

   The System Preferences window appears.

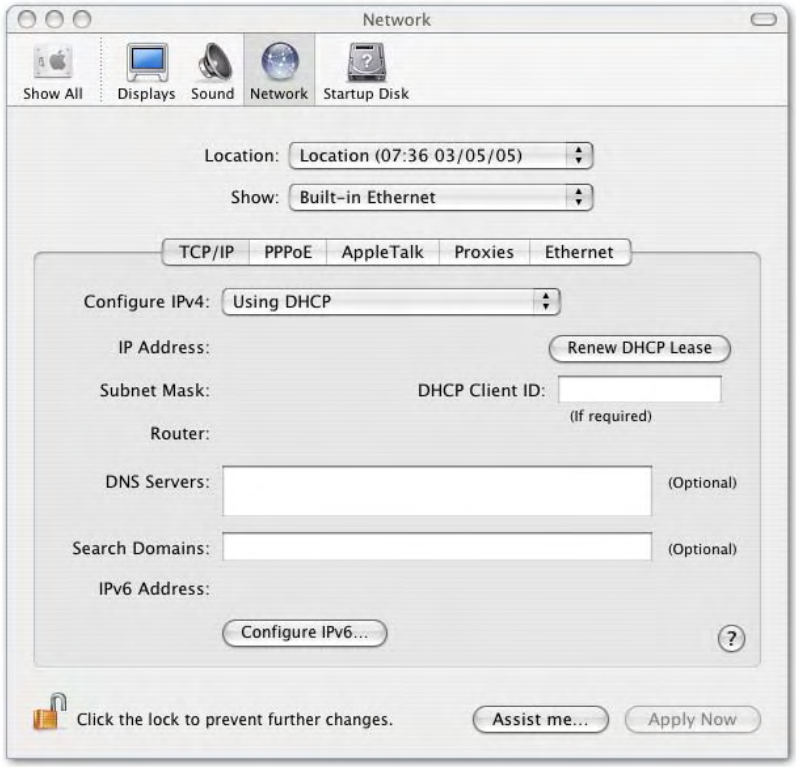
2. Click Network.

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**.

Appliance Installation

Installing Non-ADSL Models

ADSL

To install the Safe@Office appliance

1. Verify that you have the correct cable type.

   For information, see ***Network Requirements*** on page 15.

2. Connect the LAN cable:

   a. Connect one end of the Ethernet cable to one of the appliance's LAN ports.

   b. Connect the other end to PCs, hubs, or other network devices.

3. Connect the WAN cable:

   a. Connect one end of the Ethernet cable to the appliance's WAN port.

   b. Connect the other end of the cable to a cable modem, DSL modem, or office network.

4. Connect the power supply to the appliance's power socket, labeled PWR.

5. Plug the power supply into the wall electrical outlet.

Warning: The Safe@Office appliance power supply 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 supply. Failure to observe this warning may result in injuries or damage to equipment.

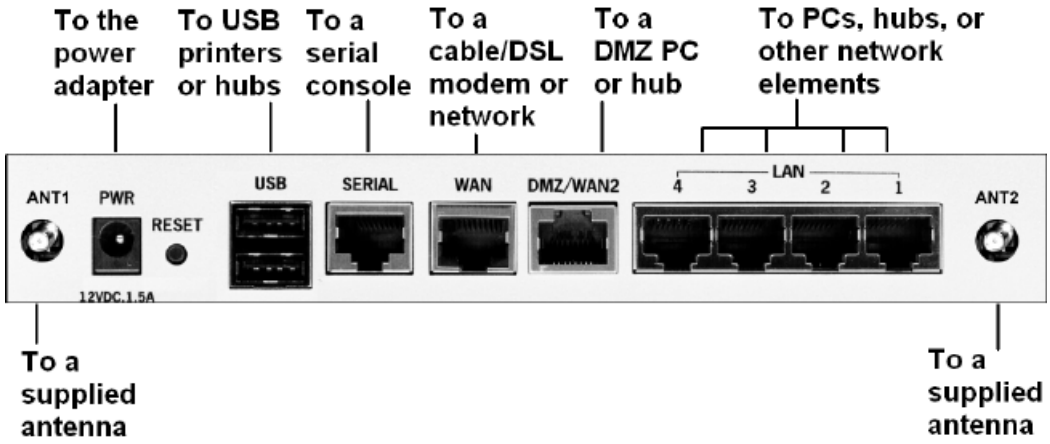


Figure 12: Typical Connection Diagram

Installing ADSL Models

ADSL

To install the Safe@Office appliance

1. Verify that you have the correct cable type.

   For information, see ***Network Requirements*** on page 15.

2. Connect the LAN cable:

   a. Connect one end of the Ethernet cable to one of the appliance's LAN ports.

   b. Connect the other end to PCs, hubs, or other network devices.

3. Connect the ADSL cable:

   a. Connect one end of the telephone cable to the appliance's DSL port.

   b. Connect the other end of the cable to the ADSL line or micro-filter.

   In most cases, a micro-filter is required for each phone jack on your line. The micro-filter prevents the standard phone lines from interfering with your ADSL

service. Check with your service provider whether a micro-filter is required at your location.

4. To use the appliance with a non-ADSL connection, or with an existing ADSL modem, connect an Ethernet cable:
   a. Connect one end of the Ethernet cable to the appliance's DMZ/WAN2 port.
   b. Connect the other end of the cable to an external cable modem, DSL modem, or office network.
5. Connect the power supply to the appliance's power socket, labeled PWR.
6. Plug the power supply into the wall electrical outlet.

Warning: The Safe@Office appliance power supply 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 supply. Failure to observe this warning may result in injuries or damage to equipment.

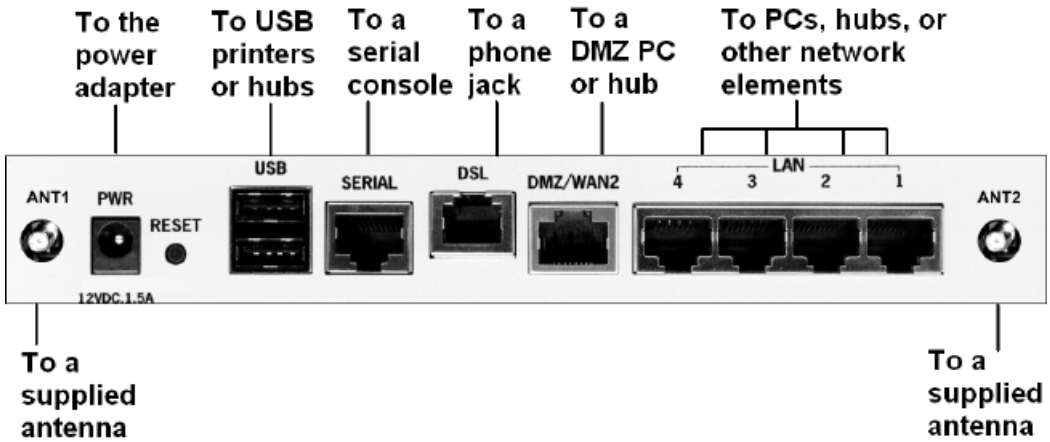


Figure 13: Typical Connection Diagram

Cascading Your Appliance

500

The Safe@Office appliance protects all computers and network devices that are connected to its LAN and DMZ ports. If desired, you can increase the appliance's port capacity by cascading hubs or switches.

To cascade the Safe@Office appliance to a hub or switch

1. Connect a standard Ethernet cable to one of the appliance's LAN ports or to its DMZ/WAN2 port.

   The Safe@Office appliance automatically detects cable types, so you can use either a straight-through or crossed Ethernet cable.

2. Connect the other end of the cable to an Ethernet hub or switch.
3. Connect additional computers and network devices to the hub or switch as desired.

Preparing the Appliance for a Wireless Connection

500W

To prepare the Safe@Office appliance for a wireless connection

1. Connect the antennas that came with your Safe@Office appliance to the ANT1 and ANT2 antenna connectors in the appliance's rear panel.
2. Bend the antennas at the hinges, so that they point upwards.

Connecting the Appliance to Network Printers

USB

In models with a print server, you can connect network printers.

To connect network printers

1. Connect one end of a USB cable to one of the appliance's USB ports.

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

2. 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 734.

Wall Mounting the Safe@Office Appliance

500

For your convenience, the Safe@Office appliance includes a wall mounting kit, which consists of two plastic conical anchors and two cross-head screws.

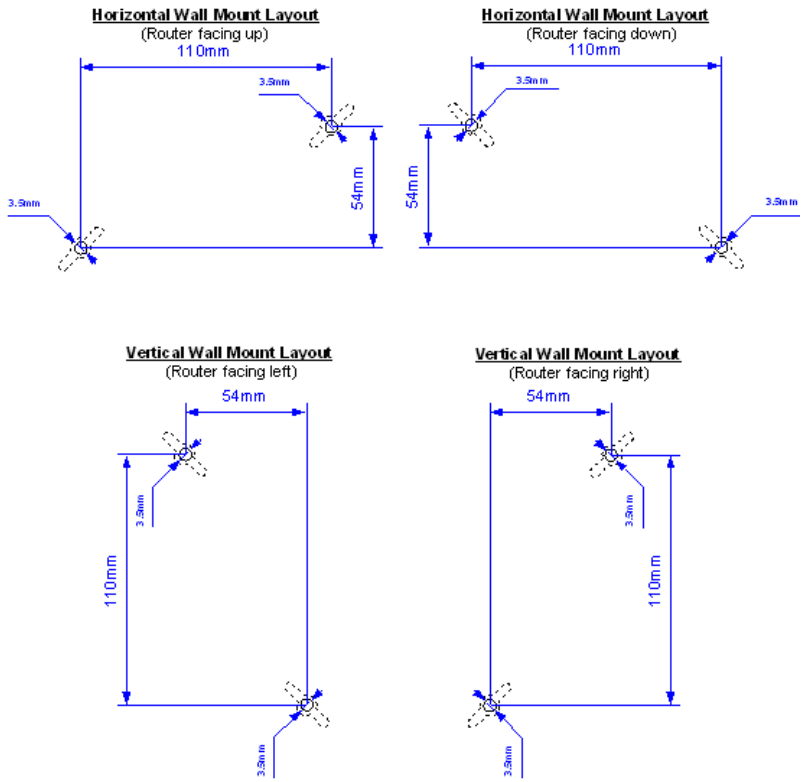
To mount the Safe@Office appliance on the wall

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 with the ports facing upwards 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.

Securing the Safe@Office Appliance against Theft

500

The Safe@Office appliance 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.

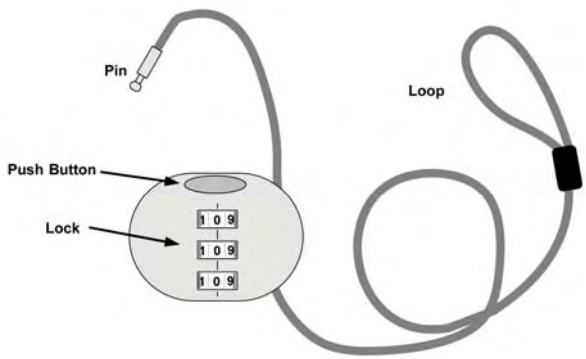


Figure 14: Looped Security Cable

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

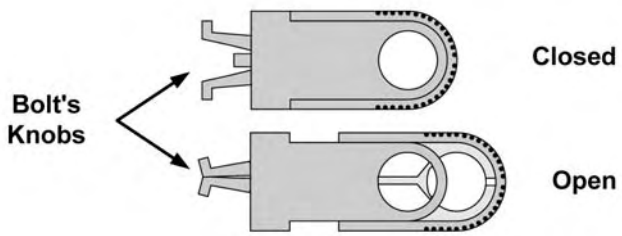
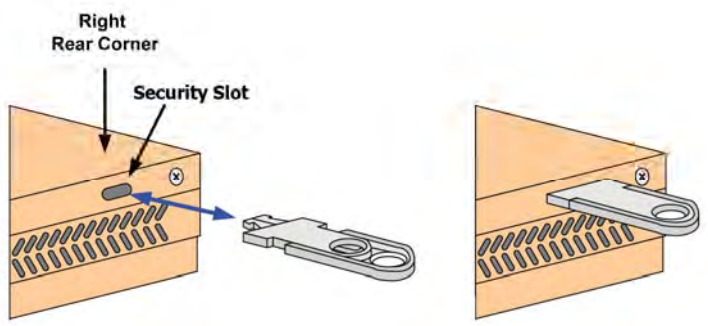


Figure 15: Looped Security Cable Bolt

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 bolts holes are aligned.



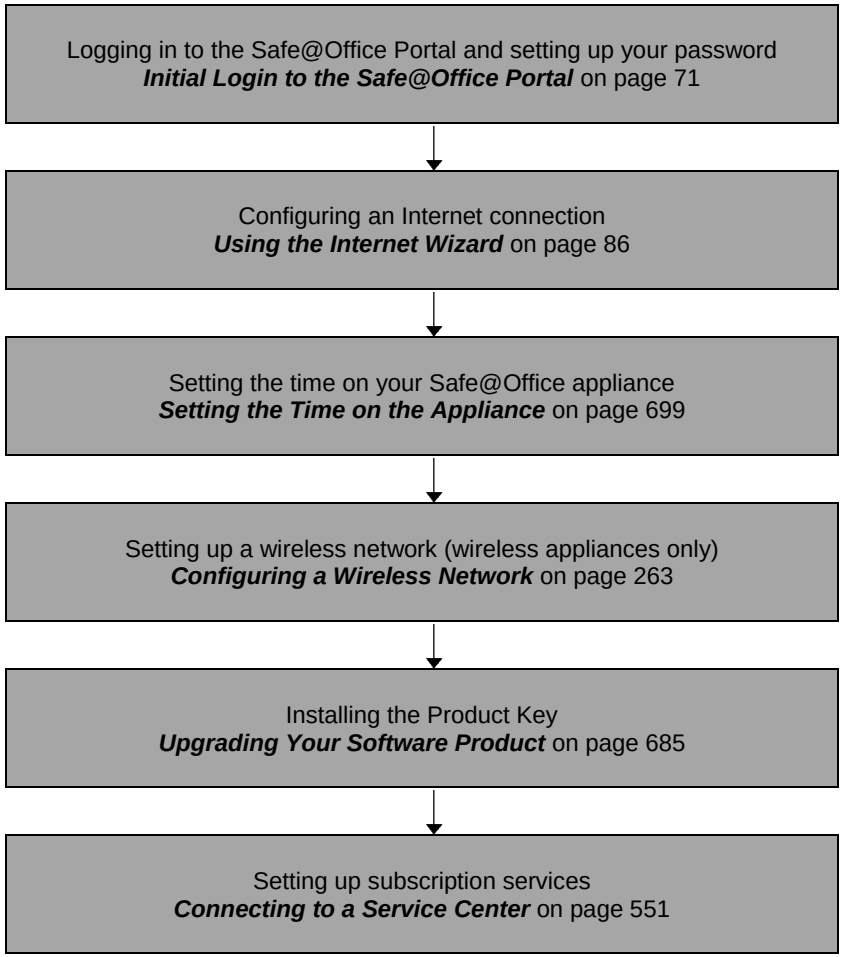
5. Thread the anti-theft device's pin through the bolt’s holes, and insert the pin into the main body of the anti-theft device, as described in the documentation that came with your device.

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 in and set up your password, the Safe@Office Setup Wizard automatically opens and displays the dialog boxes for performing the initial configuration of the router. If desired, you can exit the Setup Wizard and perform each of these steps separately.

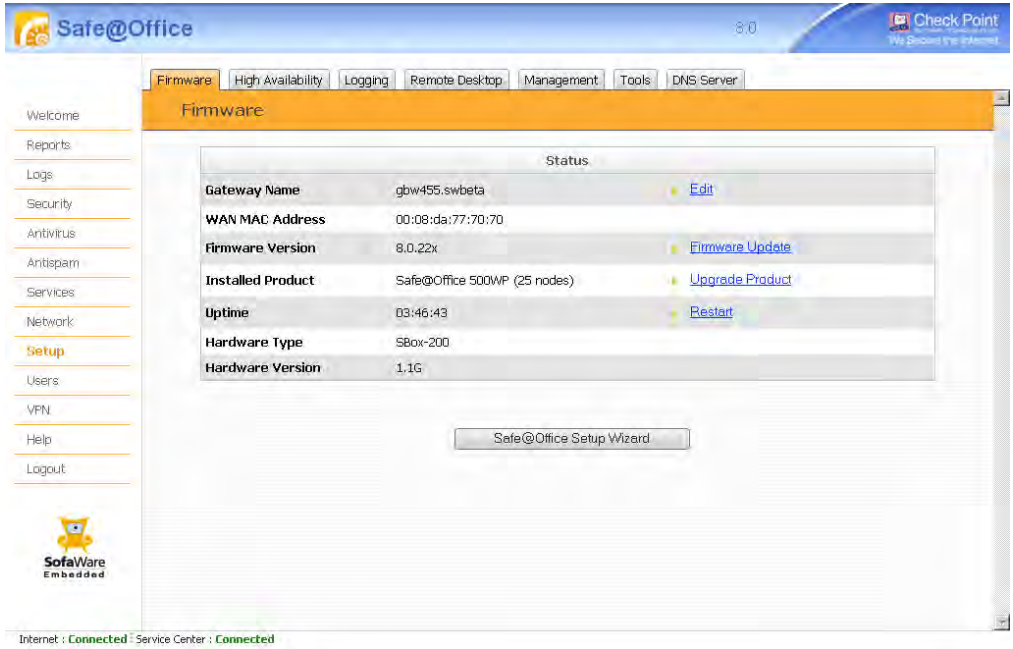


You can access the Setup Wizard at any time after initial setup, using the procedure below.

To access the Setup Wizard

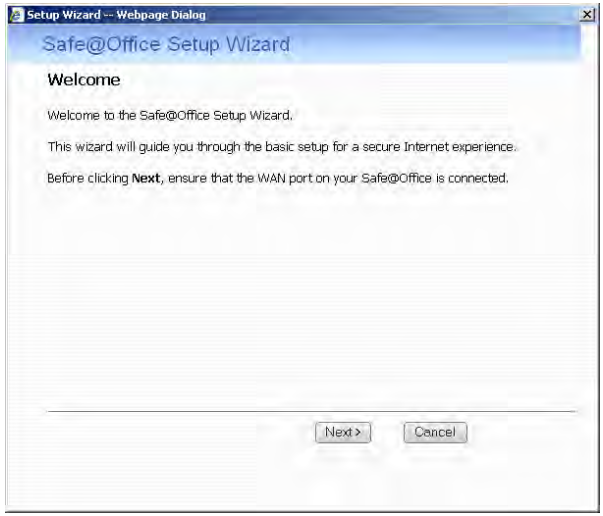
1. Click **Setup** in the main menu, and click the **Firmware** tab.

   The **Firmware** page appears.



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

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



Chapter 4

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

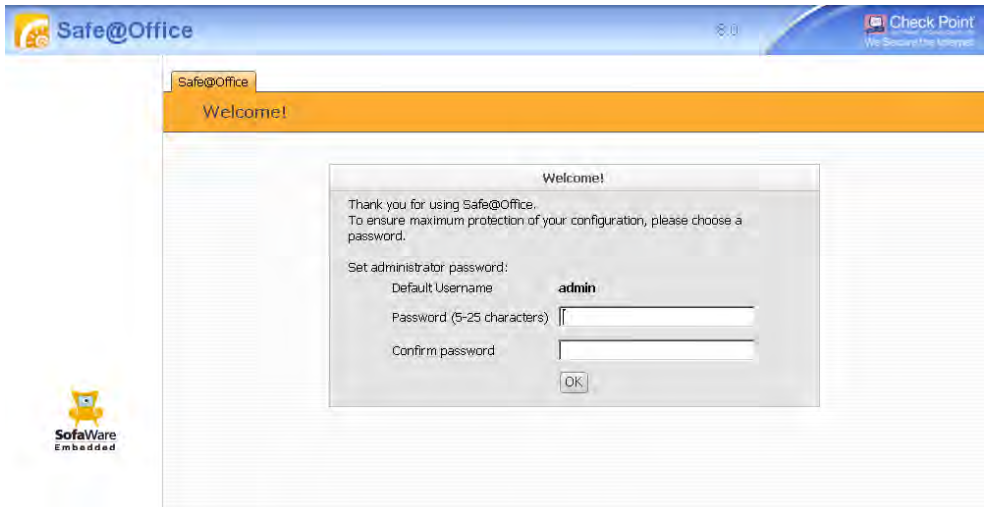
500

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

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

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

The initial login page appears.



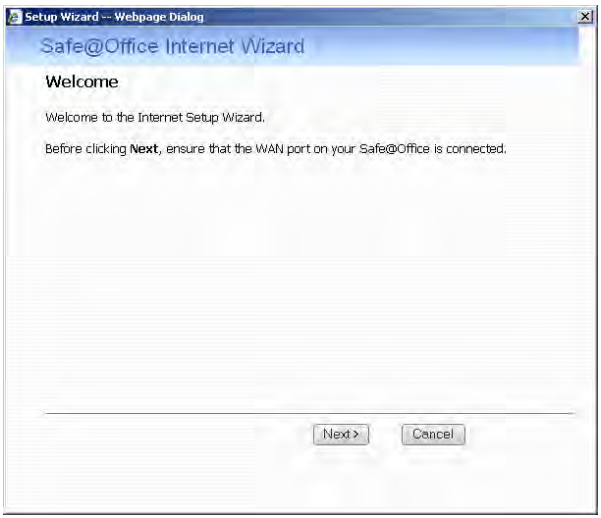
2. Type a password both in the **Password** and the **Confirm password** fields.

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

Note: You can change your username and password at any time. For further information, see ***Changing Your Password*** on page 639.

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 86.

  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*** on page 67.

- 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 102.

Logging in 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 360.

  Or

- Enable HTTPS access from the Internet. See ***Configuring HTTPS*** on page 691.

To log in to the Safe@Office Portal

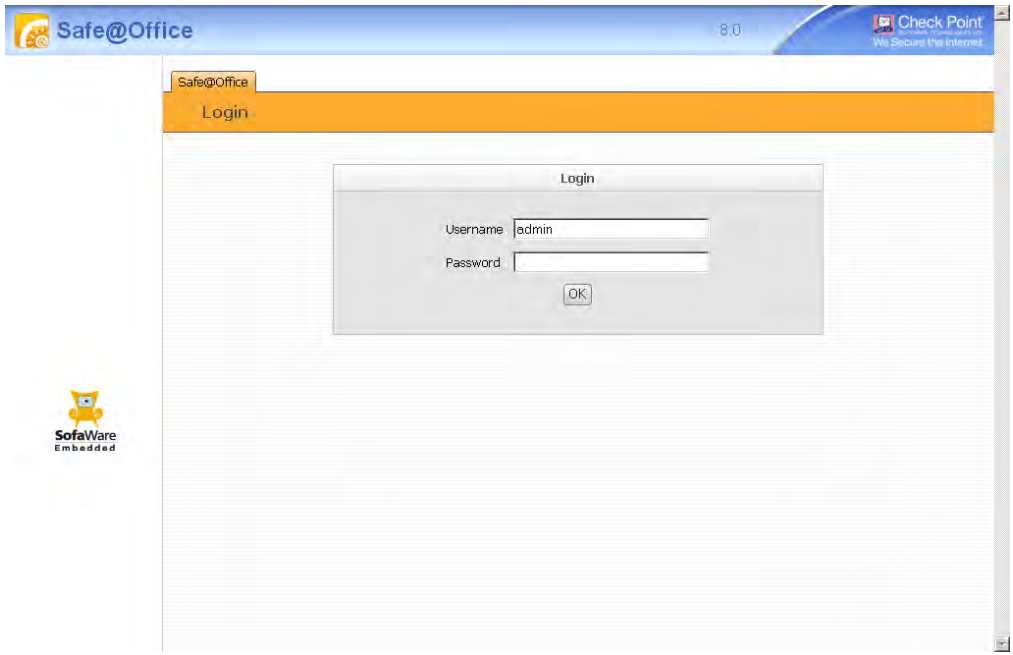
1. Do one of the following:

   - Browse to http://my.firewall.

     Or

   - To log in through HTTPS (locally or remotely), follow the procedure ***Accessing the Safe@Office Portal Remotely*** on page 77.

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 71.
- Configure HTTPS Remote Access. See ***Configuring HTTPS*** on page 691.

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 6, 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 15: 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 16: Safe@Office Portal

Main Menu

The main menu includes the following submenus.

Table 16: Main Menu Submenus

This submenu…	Does this…
Welcome	Displays general welcome information.
Reports	Provides reporting capabilities in terms of appliance status, traffic monitoring, active computers, established connections, and more.
Logs	Provides a general event log displaying appliance events, and a security event log displaying firewall events.
Security	Provides controls and options for setting the security of any computer in the network.
Antivirus	Allows you to configure VStream Antivirus settings.
Antispam	Allows you to configure VStream Antispam settings.
Services	Allows you to control your subscription to subscription services.
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 in to VPN sites.

This submenu…	Does this…
Help	Provides context-sensitive online help.
Logout	Allows you to log out 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 17: 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 85.

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 Out

500

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

To log out of the Safe@Office Portal

- Click Logout in the main menu.

  The Login page appears.

Chapter 5

Configuring the Internet Connection

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

This chapter includes the following topics:

Overview

In order to access the Internet through your Safe@Office appliance, you must configure one of the following connection types:

- Ethernet-based connection

  You can configure an Ethernet-based connection in all models. An Ethernet-based connection can be connected to another network by means of a switch, a router, a bridge, or an Ethernet-enabled broadband modem.

  In ADSL models, the Ethernet-based connection is configured on the DMZ/WAN2 port. In non-ADSL models, you can use the WAN port, the DMZ/WAN2 port, or both ports for an Ethernet-based Internet connection.

- Direct ADSL connection

  You can configure a direct ADSL connection in Safe@Office ADSL models only. These models include an integrated ADSL modem, which enables you to connect the appliance directly to your ADSL line without using an additional modem or router.

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*** on page 67.
- Internet Wizard. Guides you through the Internet connection configuration process step by step. For further information, see ***Using the Internet Wizard*** on page 86.
- Internet Setup. Offers the following advanced setup options:
  - Configure two Internet connections.

    For information, see ***Configuring a Backup Internet Connection*** on page 149.
  - Enable Traffic Shaper for traffic flowing through the connection.

    For information on Traffic Shaper, see ***Using Traffic Shaper*** on page 251.
  - Configure a dialup Internet connection.

    Before configuring the connection, you must first set up the modem. For information, see ***Setting Up Modems*** on page 136.

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.

Note: The first time you log in 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 following procedure.

Configuring an Ethernet-Based Connection on Non-ADSL Models

ADSL

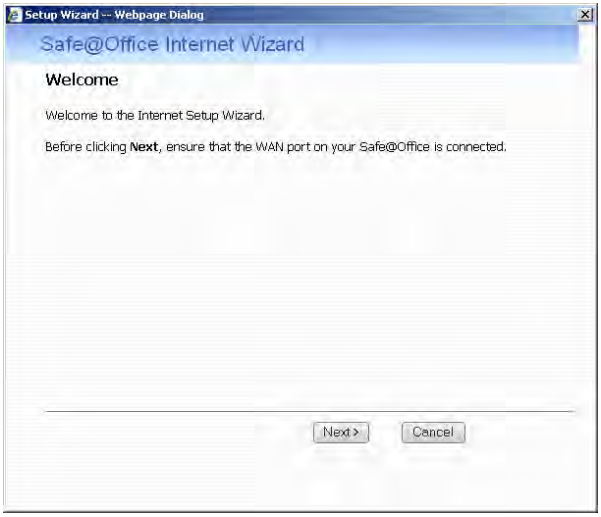
To configure an Ethernet-Based connection

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.

   If you are uncertain regarding which connection method to use contact your xDSL provider.

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

5. Click **Next**.

   If you chose PPPoE, continue at ***Using a PPPoE Connection*** on page 89.

   If you chose PPTP, continue at ***Using a PPTP Connection*** on page 91.

   If you chose Cable Modem, continue at ***Using a Cable Modem Connection*** on page 92.

   If you chose Static IP, continue at ***Using a Static IP Connection*** on page 93.

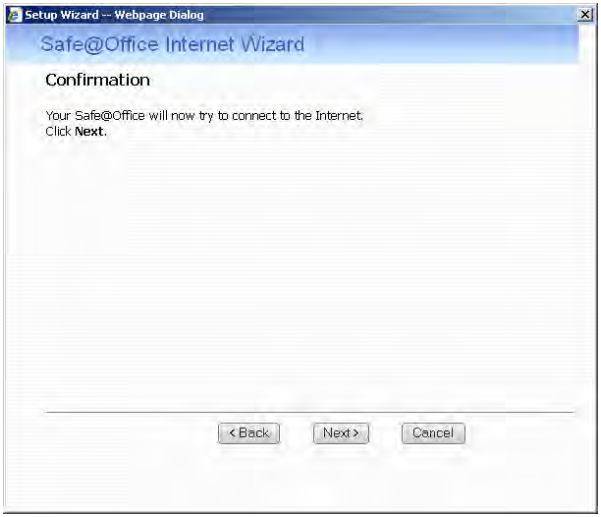
   If you chose DHCP, continue at ***Using a DHCP Connection*** on page 94.

Using a PPPoE Connection

If you selected the PPPoE (PPP over Ethernet) connection method, the PPP Configuration dialog box appears.

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

   The Confirmation screen appears.



3. Click **Next**.

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

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

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

4. Click **Finish**.

Table 18: 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 a PPTP Connection

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

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

   The Confirmation screen appears.
3. Click Next.

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

   The Connecting... screen appears.

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

Table 19: 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	Select the subnet mask of the PPTP modem.

Using a Cable Modem Connection

No further settings are required for a cable modem connection. The Confirmation screen appears.

1. Click Next.

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

   The Connecting... screen appears.

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

2. Click Finish.

Using a Static IP Connection

If you selected the Static IP connection method, the Static IP Configuration dialog box appears.

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

   The Confirmation screen appears.
3. Click Next.

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

   The Connecting... screen appears.

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

Table 20: PPPoE Connection Fields

In this field…	Do this…
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.
Default Gateway	Type the IP address of your ISP’s default gateway.
Primary DNS Server	Type the IP address of your ISP's primary DNS server.
Secondary DNS Server	Type the IP address of your ISP's secondary DNS server. This field is optional.
WINS Server	Type the IP address of your ISP's WINS server. This field is optional.

Using a DHCP Connection

No further settings are required for a DHCP (Dynamic IP) connection. The Confirmation screen appears.

1. Click Next.

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

   The Connecting... screen appears.

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

2. Click Finish.

Configuring an Ethernet-Based Connection on ADSL Models

ADSL

Note: In ADSL models, an Ethernet-based connection is made on the DMZ/WAN2 port.

To configure an Ethernet-based connection

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 Port dialog box appears.

4. Click Use the WAN2 port to connect to another network or router.
5. Click Next.

The Internet Connection Method dialog box appears.

6. Select the Internet connection method you want to use for connecting to the Internet.
7. Click Next.

   If you chose PPPoE, continue at ***Using a PPPoE Connection*** on page 89.

   If you chose PPTP, continue at ***Using a PPTP Connection*** on page 91.

   If you chose Cable Modem, continue at ***Using a Cable Modem Connection*** on page 92.

   If you chose Static IP, continue at ***Using a Static IP Connection*** on page 93.

   If you chose DHCP, continue at ***Using a DHCP Connection*** on page 94.

Configuring a Direct ADSL Connection

ADSL

To configure a direct ADSL connection

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

   The Internet page appears.

2. Click Internet Wizard.

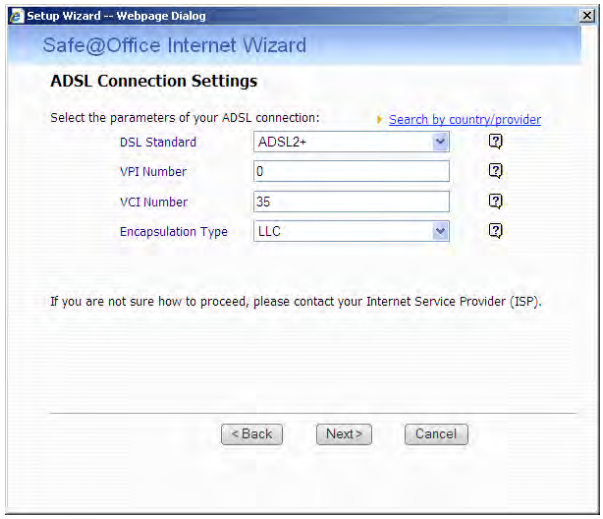
   The Internet Wizard opens with the Welcome page displayed.

3. Click Next.

   The Internet Connection Port dialog box appears.

4. Click Use the ADSL port.

   The ADSL Connection Settings dialog box appears.



5. Do one of the following:

   - To automatically fill in the supported ADSL settings for your ISP, do the following:

     1) Click Search by country and ISP.

        The ADSL Configuration Assistant opens.

     2) In the Country drop-down list, select your country.

     3) In the ISP / Telco drop-down list, select your ISP or telephone company.

        The ADSL Configuration Assistant closes, and the fields are filled in with the correct values for your ISP.

   - To manually fill in the supported ADSL settings for your ISP, complete the fields using the information in the following table.

6. Click Next.

The Internet Connection Method dialog box appears.

7. Select the Internet connection method you want to use for connecting to the Internet.
8. Click Next.

   If you chose PPPoE or PPPoA, continue at ***Using a PPPoE or PPPoA Connection*** on page 101.

   If you chose Static IP, continue at ***Using a Static IP Connection*** on page 93.

   If you chose DHCP, continue at ***Using a DHCP Connection*** on page 94.

Table 21: ADSL Connection Fields

In this field…	Do this…
DSL Standard	Select the standard to support for the DSL line, as specified by your ISP. This can be one of the following: • ADSL2 • ADSL2+ • Multimode • T.1413 • G.lite • G.DMT
VPI Number	Type the VPI number to use for the ATM virtual path, as specified by your ISP.
VCI Number	Type the VCI number to use for the ATM virtual circuit, as specified by your ISP.
Encapsulation Type	Select the encapsulation type to use for the DSL line, as specified by your ISP. This can be one of the following: • LLC • VCMUX

Using a PPPoE or PPPoA Connection

If you selected the PPPoE (PPP over Ethernet) or PPPoA (PPP over ATM) connection method, the PPP Configuration dialog box appears.

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

   The Confirmation screen appears.
3. Click Next.

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

   The Connecting... screen appears.

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

Table 22: PPPoE Connection Fields

In this field…	Do this…
Username	Type your user name.
Password	Type your password.
Confirm password	Type your password again.

Using Internet Setup

500

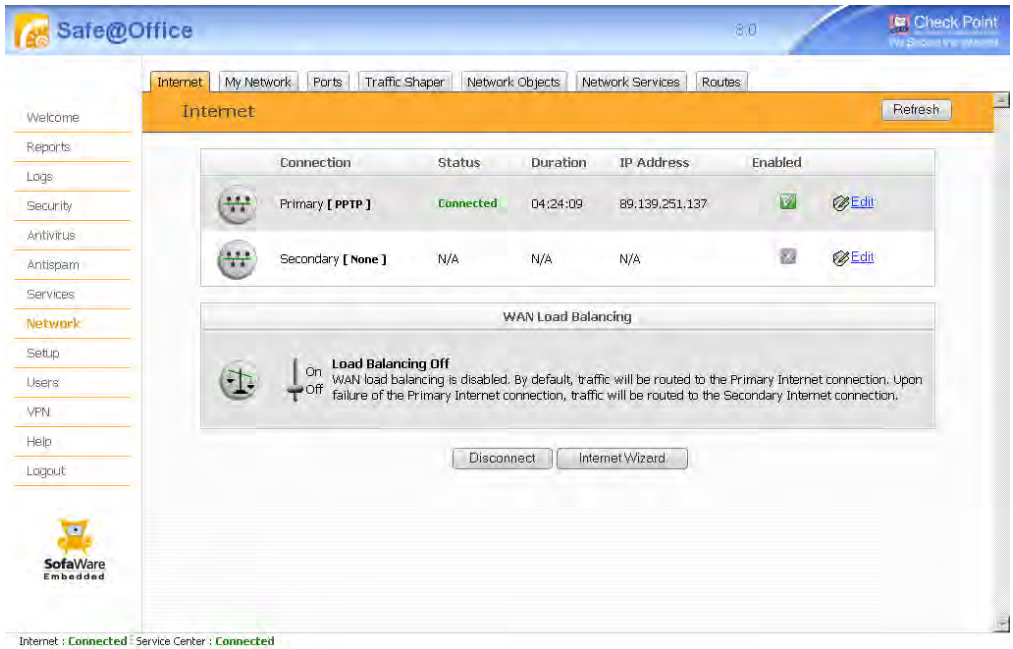
Internet Setup allows you to manually configure your Internet connection.

For information on configuring bridged Internet connections, see ***Adding Internet Connections to Bridges*** on page 233.

To configure the Internet connection using Internet Setup

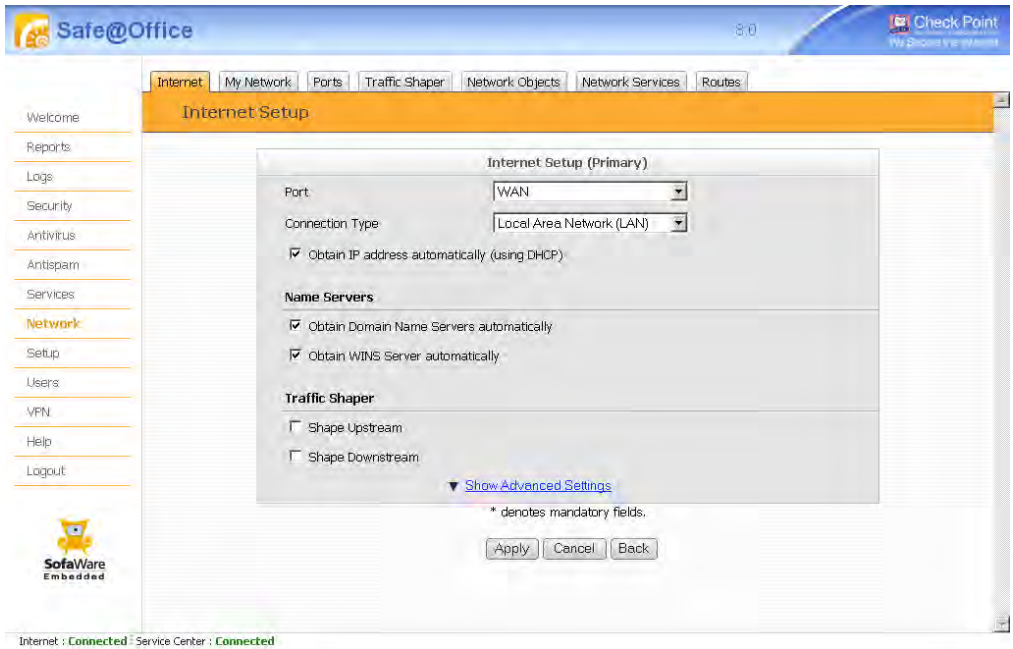
1. Click Network in the main menu, and click the Internet tab.

The **Internet** page appears.



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

The **Internet Setup** page appears.



3. Do one of the following:

- To configure an ADSL connection using the internal ADSL modem, continue at ***Configuring a Direct ADSL Connection*** on page 105.

  This option is available in ADSL models only.

- To configure an Ethernet-based connection, continue at ***Configuring an Ethernet-Based Connection*** on page 114.

- To configure a Dialup connection, continue at ***Configuring a Dialup Connection*** on page 125.

- To configure no connection, continue at ***Using No Connection*** on page 127.

Configuring a Direct ADSL Connection

ADSL

1. In the Port drop-down list, select ADSL.
2. Do one of the following:

   - To automatically fill in the supported ADSL settings for your ISP, do the following:

     1) Click Search by country and ISP.

        The ADSL Configuration Assistant opens.

     2) In the Country drop-down list, select your country.

     3) In the ISP / Telco drop-down list, select your ISP or telephone company.

        The ADSL Configuration Assistant closes. The Connection Type drop-down list and the ADSL Link Settings fields are filled in with the correct values for your ISP.

   - To manually fill in the supported ADSL settings for your ISP, in the Connection Type drop-down list, select the Internet connection type you intend to use.

   The display changes according to the selected connection type.

   For PPPoA, continue at ***Using a PPPoA Connection*** on page 106.

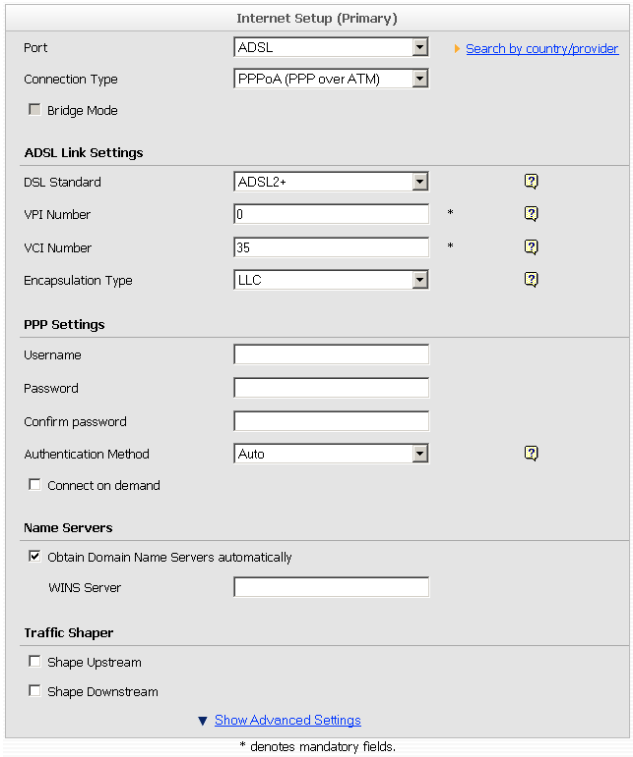
   For EoA, continue at ***Using an EoA Connection*** on page 108.

   For PPPoE, continue at ***Using a PPPoE Connection*** on page 110.

   For IPoA, continue at ***Using an IPoA (IP over ATM) Connection*** on page 112.

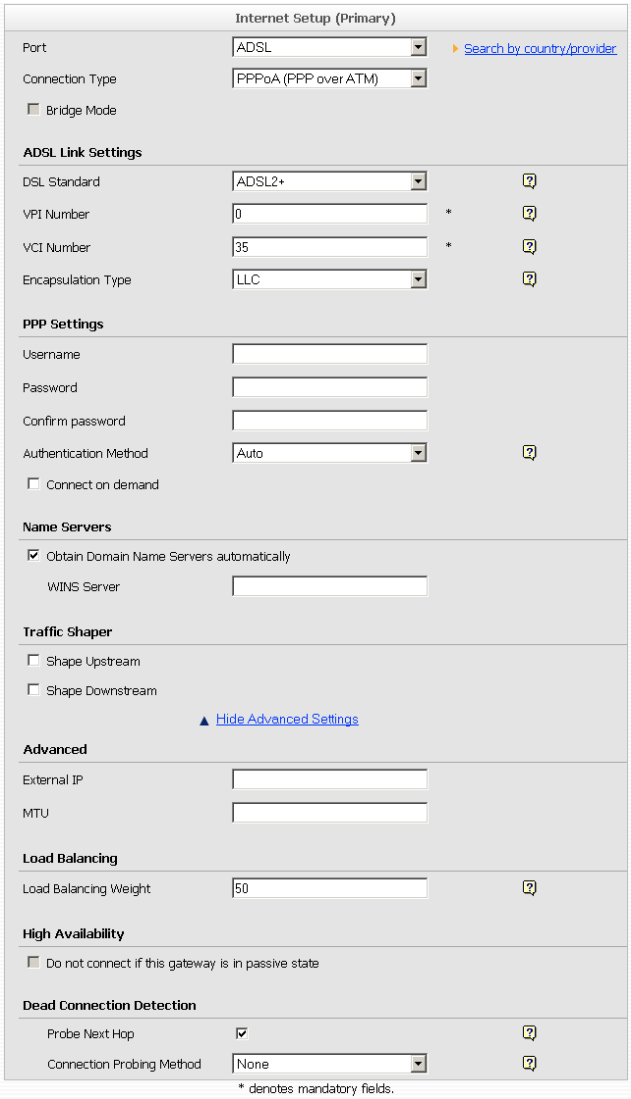
   For information on configuring bridged connections, see ***Adding Internet Connections to Bridges*** on page 233.

Using a PPPoA (PPP over ATM) Connection



1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 127.

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

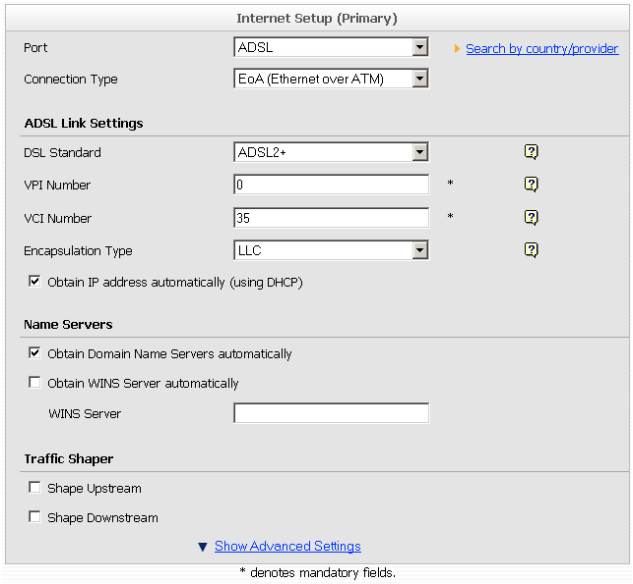


2. Click **Apply**.

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

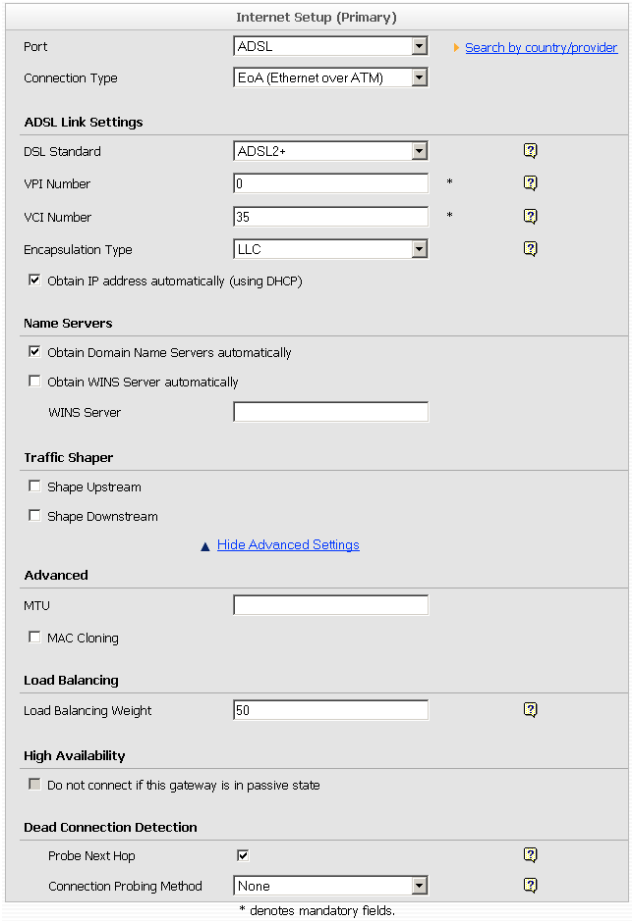
Once the connection is made, the Status Bar displays the Internet status “Connected”.

Using an EoA (Ethernet over ATM) Connection



1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 127.

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

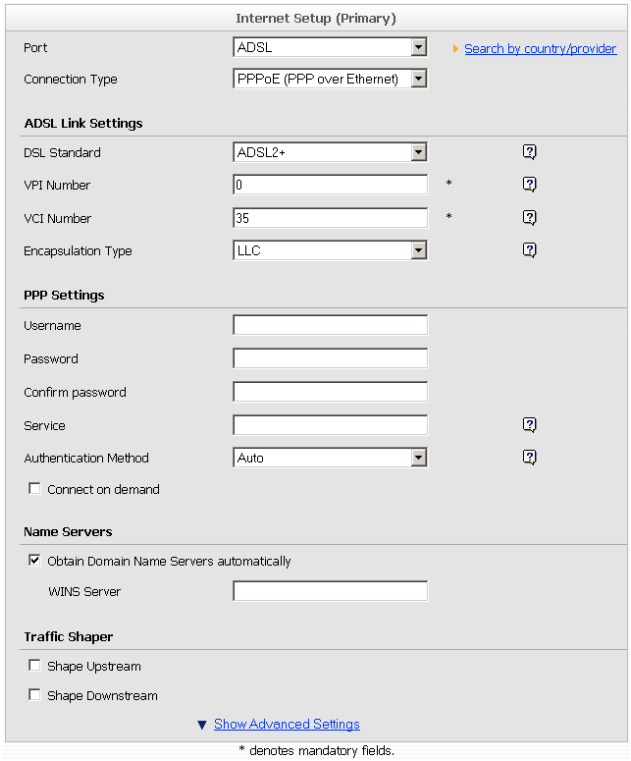


2. Click **Apply**.

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

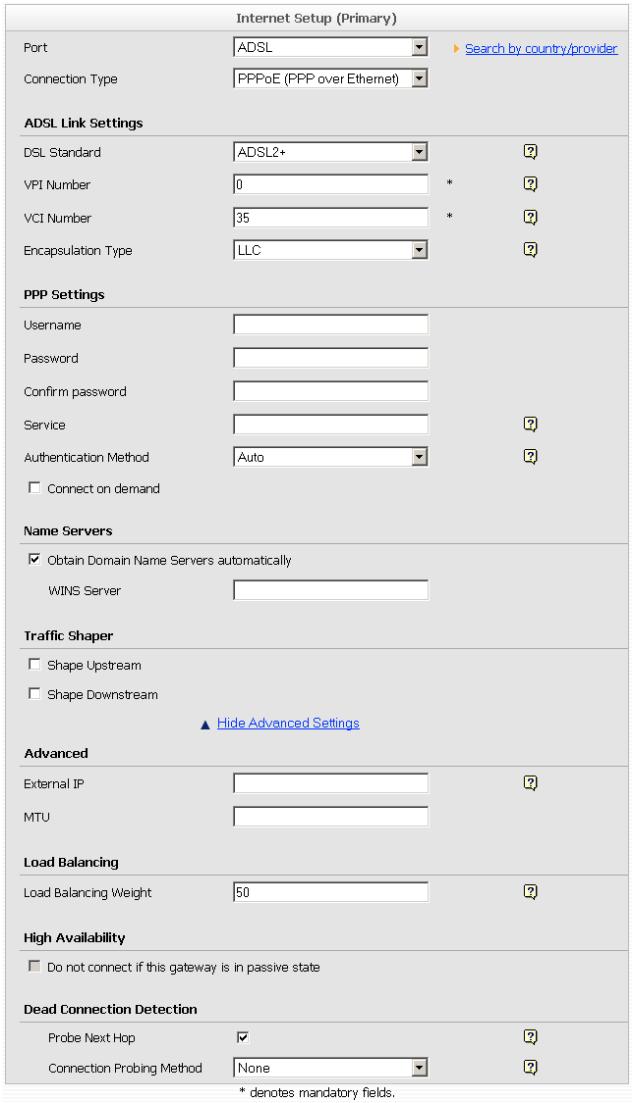
   Once the connection is made, the Status Bar displays the Internet status “Connected”.

Using a PPPoE (PPP over Ethernet) Connection



1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 127.

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

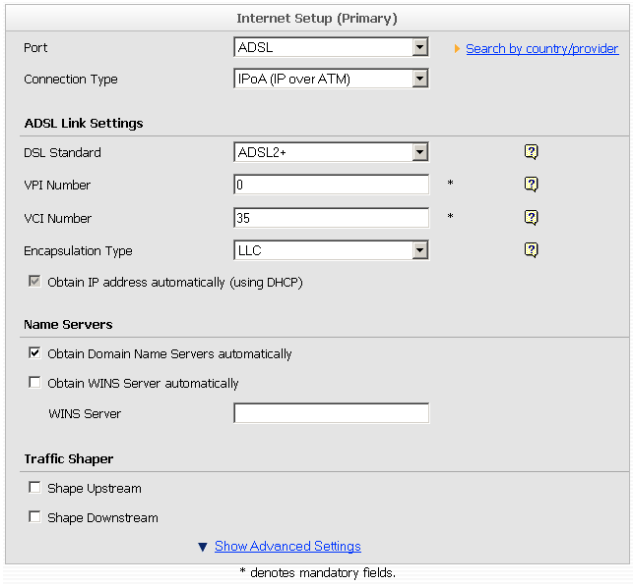


2. Click **Apply**.

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

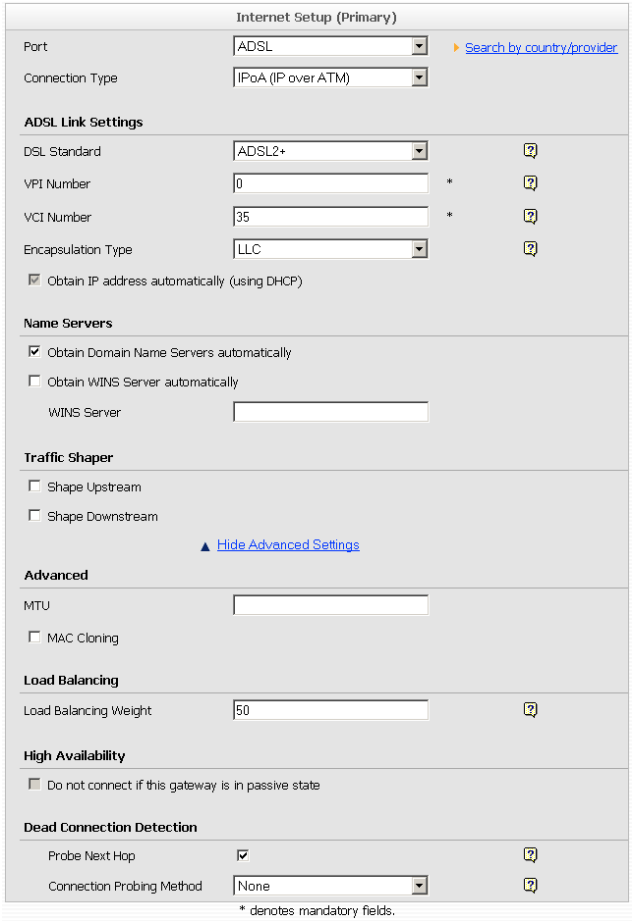
Once the connection is made, the Status Bar displays the Internet status “Connected”.

Using an IPoA (IP over ATM) Connection



1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 127.

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”.

Configuring an Ethernet-Based Connection

500

1. In the Port drop-down list, do one of the following:

   - To configure an Ethernet-based connection through the WAN port, select WAN.
   - To configure an Ethernet-based connection through the DMZ/WAN2 port, select WAN2.

     This option is available in non-ADSL models only.
   - To configure an Ethernet-based connection through a LAN port, select the desired LAN port.

     This option is available with the Power Pack license only.

   The selected port is automatically configured for use with an Internet connection. For information on viewing a port's status, see ***Viewing Port Statuses.*** on page 206

2. In the Connection Type drop-down list, select the Internet connection type you intend to use.

   The display changes according to the connection type you selected.

   If you chose LAN, continue at ***Using a LAN Connection*** on page 115.

   If you chose Cable Modem, continue at ***Using a Cable Modem Connection*** on page 117.

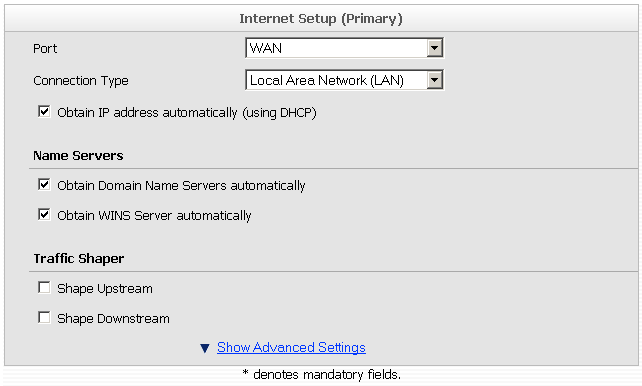
   If you chose PPPoE, continue at ***Using a PPPoE Connection*** on page 119.

   If you chose PPTP, continue at ***Using a PPTP Connection*** on page 121.

   If you chose Telstra, continue at ***Using a Telstra (BPA) Connection*** on page 123.

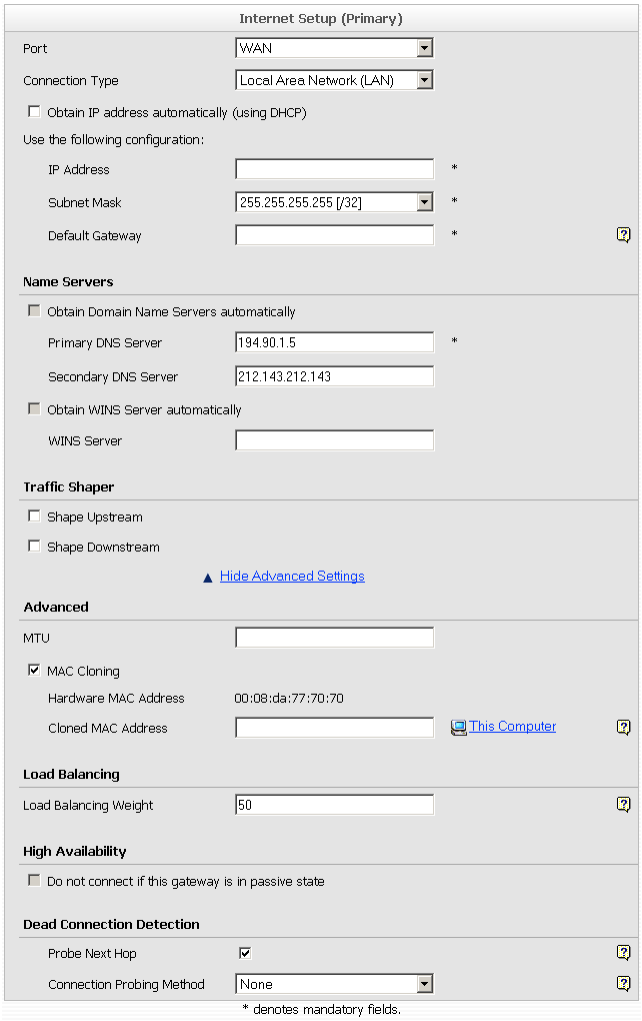
   For information on configuring bridged connections, see ***Adding Internet Connections to Bridges*** on page 233.

Using a LAN Connection



1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 127.

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

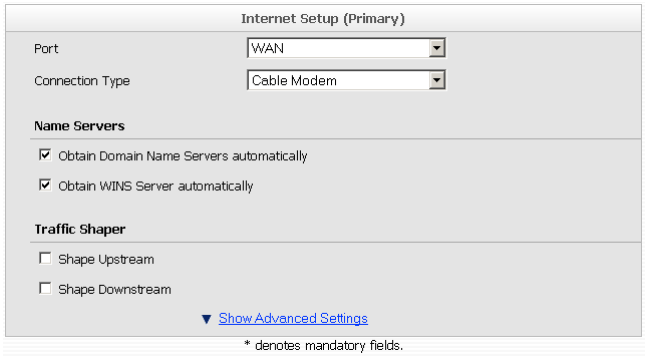


2. Click **Apply**.

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

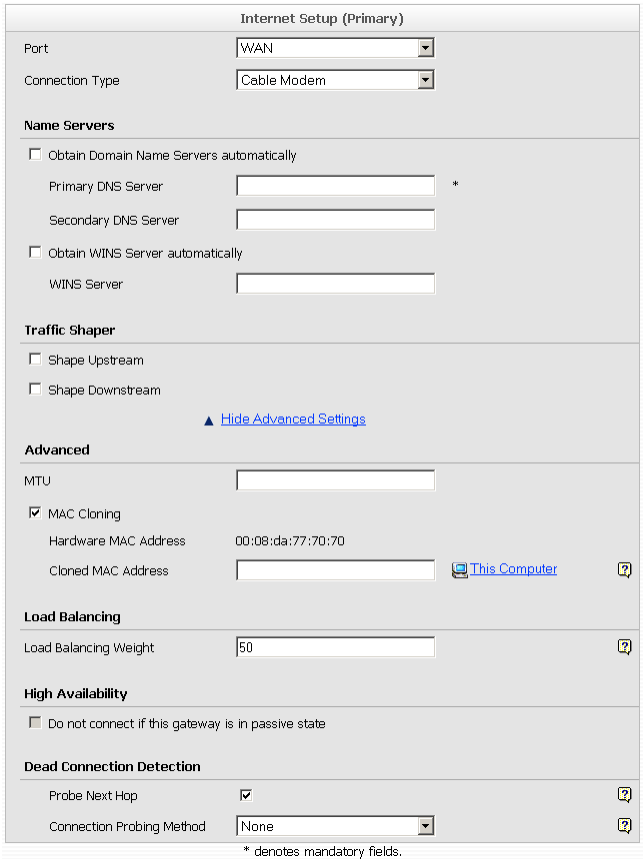
   Once the connection is made, the Status Bar displays the Internet status “Connected”.

Using a Cable Modem Connection



1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 127.

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

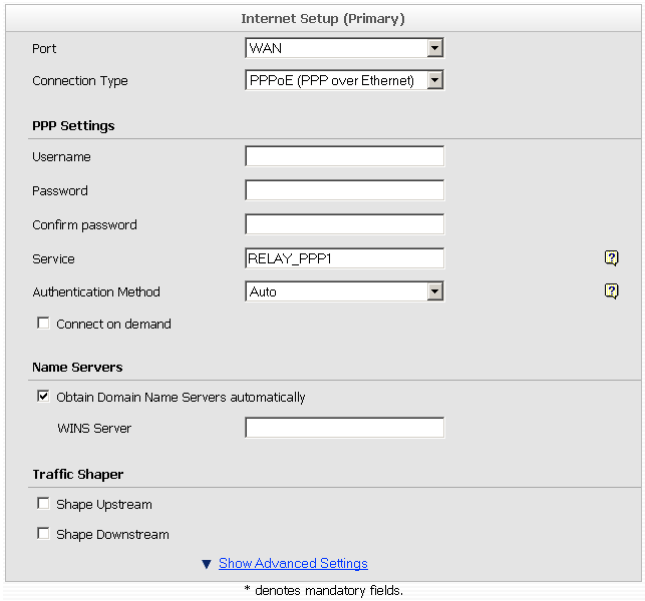


2. Click **Apply**.

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

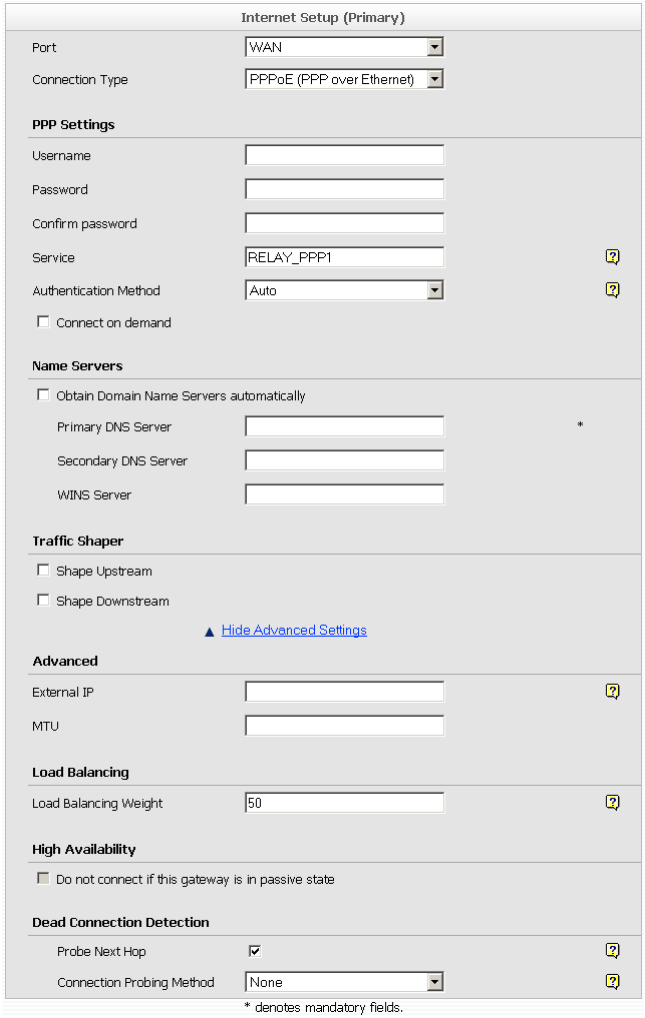
   Once the connection is made, the Status Bar displays the Internet status “Connected”.

Using a PPPoE Connection



1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 127.

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

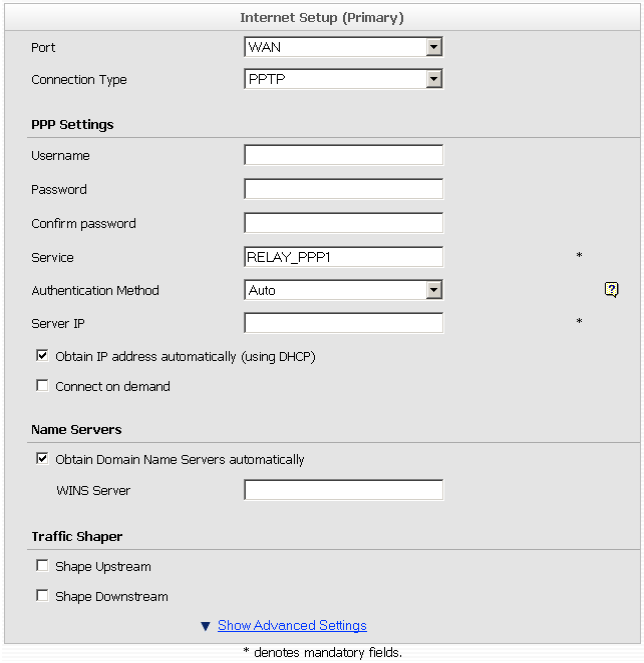


2. Click **Apply**.

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

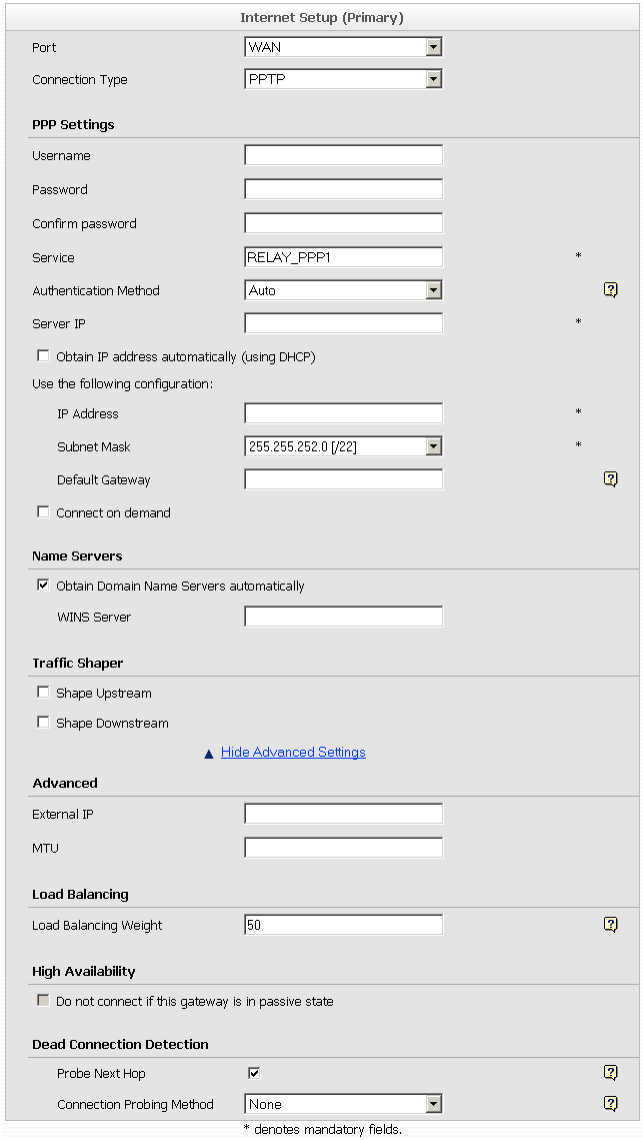
   Once the connection is made, the Status Bar displays the Internet status “Connected”.

Using a PPTP Connection



1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 127.

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



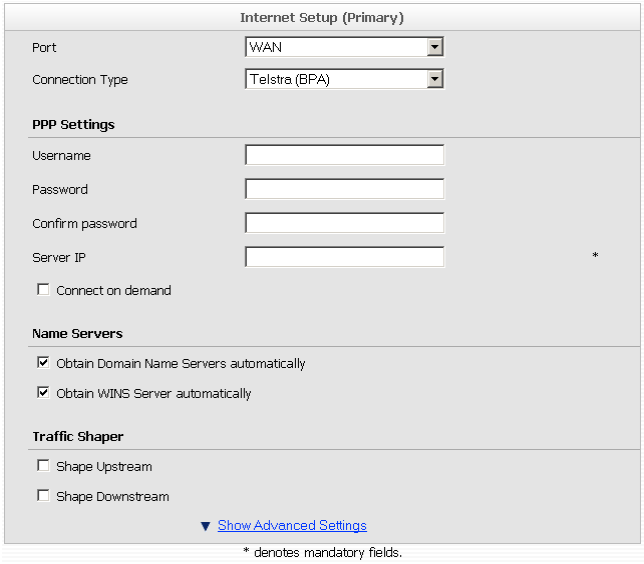
2. Click **Apply**.

   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”.

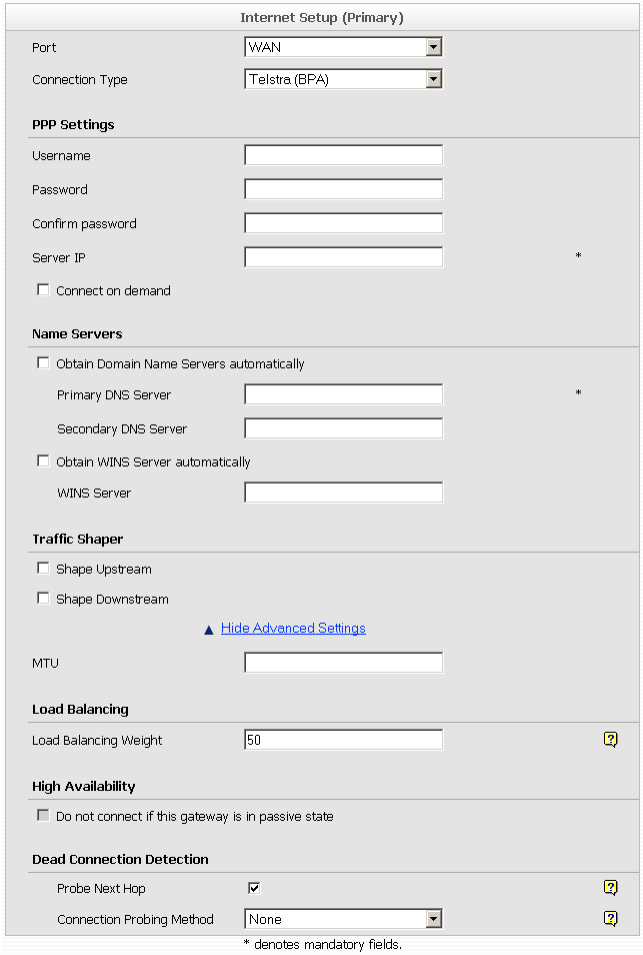
Using a Telstra (BPA) Connection

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 127.

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”.

Configuring a Dialup Connection

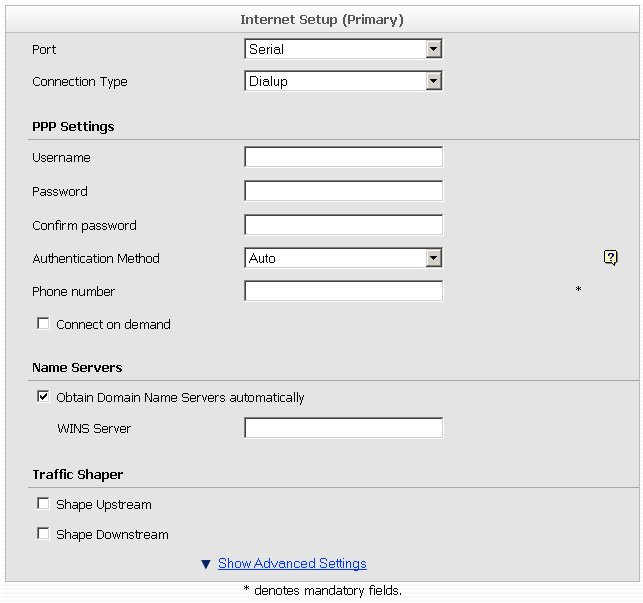
500

Note: To use this connection type, you must first set up the dialup modem. For information, see ***Setting Up Modems*** on page 136.

1. In the Port drop-down list, do one of the following:

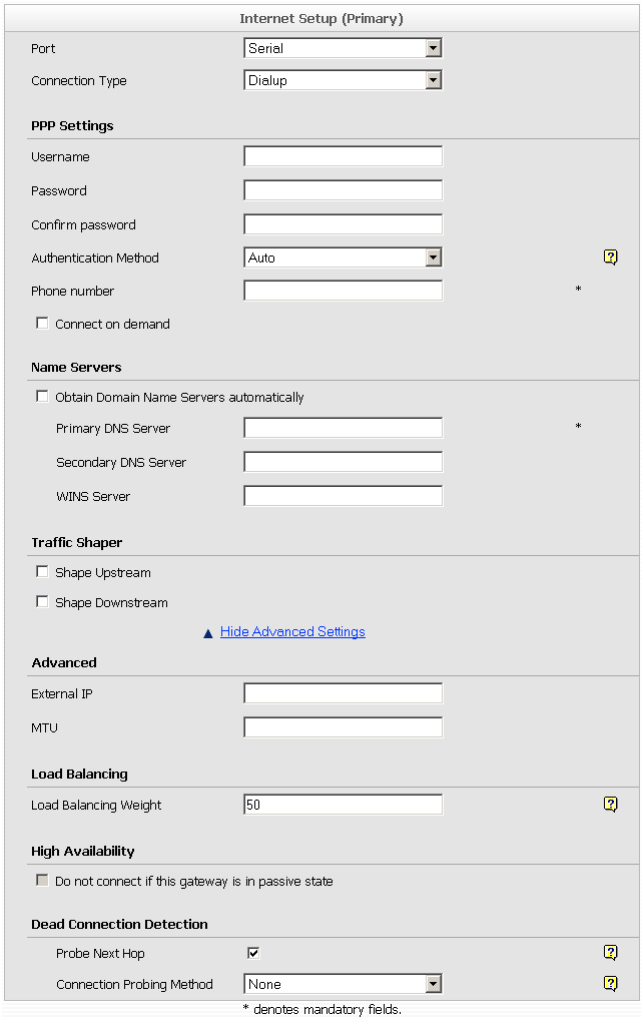
   - To configure a Dialup connection on the Serial port (using a connected RS232 modem), select Serial.
   - To configure a Dialup connection on a USB port (using a connected USB modem), select USBModem1.

   The Connection Type field displays Dialup.



2. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 127.

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



3. 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.

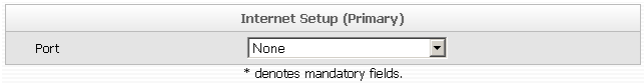
   Once the connection is made, the Status Bar displays the Internet status “Connected”.

Configuring No Connection

500

1. In the Port drop-down list, select None.

   The fields disappear.



2. Click Apply.

Table 23: Internet Setup Fields

In this field…	Do this…
ADSL Link Settings	
DSL Standard	Select the standard to support for the DSL line, as specified by your ISP.
VPI Number	Type the VPI number to use for the ATM virtual path, as specified by your ISP.
VCI Number	Type the VCI number to use for the ATM virtual circuit, as specified by your ISP.
Encapsulation Type	Select the encapsulation type to use for the DSL line, as specified by your ISP.
PPP Settings	
Username	Type your user name.
Password	Type your password.
Confirm password	Type your password.

In this field…	Do this…
Service	Type your service name. If your ISP has not provided you with a service name, leave this field empty.
Authentication Method	Specify the authentication method to use for PPP connections, by selecting one of the following: • Auto. If possible, use CHAP; otherwise, use PAP. This is the default. • PAP • CHAP
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.
Connect on demand	Select this option if you do not want the appliance to be constantly connected to the Internet. The appliance will establish a connection only under certain conditions. This option is useful when configuring a backup connection. For information, see ***Configuring a Backup Internet Connection*** on page 149.

In this field…	Do this…
When no higher priority connection is available	Select this option to specify that the appliance should only establish a connection in the following cases: • When no other connection exists, and the Safe@Office appliance is not acting as a Backup appliance. If another connection opens, the appliance will disconnect. For information on configuring the appliance as a Backup or Master, see ***Configuring High Availability*** on page 239. • When there is interesting traffic (that is, traffic for which no static route is defined).
On outgoing activity	Select this option to specify that the appliance should only establish 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 appliance 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 appliance will disconnect. The default value is 1.
Delay before connecting	Type the amount of time (in seconds) that the appliance should wait to re-connect to the Internet, if the connection goes down. If you have an unstable Internet connection that tends to go down and then return almost immediately, this setting allows you to avoid unnecessary and costly dialing during outage periods, by deferring re-connection for a few seconds. The default value is 0.
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.

In this field…	Do this…
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.
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 IP address of your ISP's primary DNS server.
Secondary DNS Server	Type the IP address of your ISP's secondary DNS server.
WINS Server	Type the IP address of your ISP's WINS server.

In this field...	Do this...
Traffic Shaper	
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 251.
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 251.

In this field…	Do this…
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.
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 205.
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.

In this field…	Do this…
Load Balancing	
Load Balancing Weight	If you are using WAN load balancing, type a value indicating the amount of traffic that should be routed though this connection relative to the other connection. For example, if you assign the primary connection a weight of 100, and you assign the secondary connection a weight of 50, twice as much traffic will be routed through the primary connection as through the secondary connection. To ensure full utilization of both Internet connections, the ratio between the connections' load balancing weights should reflect the ratio between the connections' bandwidths. The default value is 50. For information on WAN load balancing, see ***Configuring WAN Load Balancing*** on page 150.
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 is called WAN HA. This field is only enabled if HA is configured. For information on HA, see ***Configuring High Availability*** on page 239.

In this field...	Do this...
Dead Connection Detection	
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 Dialup Modems

500

You can use a connected 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 backup connection, see ***Configuring a Backup Internet Connection*** on page 149.

The Safe@Office appliance supports the connecting following modems:

- RS232 dialup modem (regular or ISDN)

  You can connect one RS232 to the appliance's Serial port.

  See ***Setting Up an RS232 Modem*** on page 137.

- USB-based modems, including dialup (PSTN/ISDN) and cellular (GPRS/EVDO) modems

  You can connect up to two USB-based modems to the appliance's USB port.

  See ***Setting Up a USB Modem*** on page 141.

Setting Up an RS232 Modem

500

Note: Your RS232 dialup modem and your Safe@Office appliance's Serial port must be configured for the same speed.

By default, the appliance's Serial port's speed is 57600 bps. For information on changing the Serial port's speed, refer to the *Embedded NGX CLI Reference Guide*.

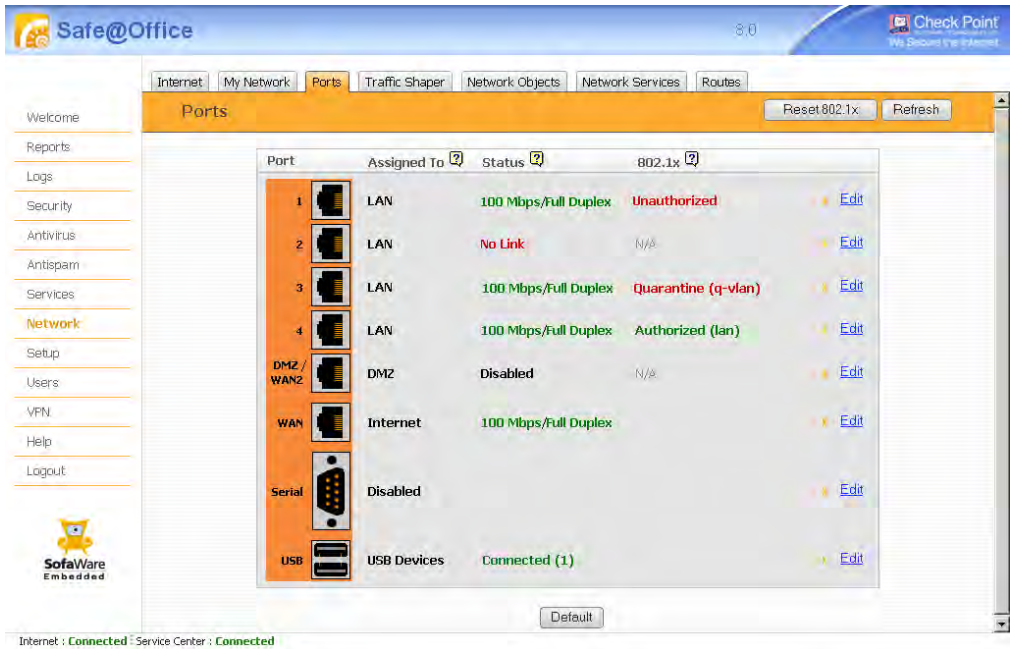
To set up an RS232 dialup modem

1. Connect an RS232 dialup modem to your Safe@Office appliance's serial port.

   For information on locating the serial port, see ***Introduction*** on page 1.

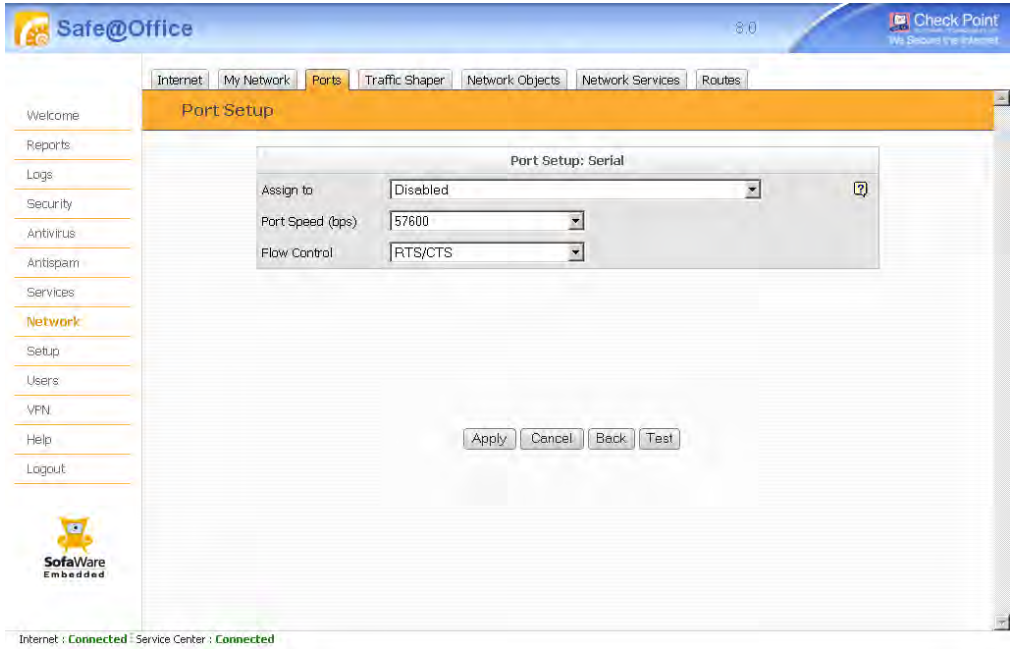
2. Click Network in the main menu, and click the Ports tab.

   The Ports page appears.



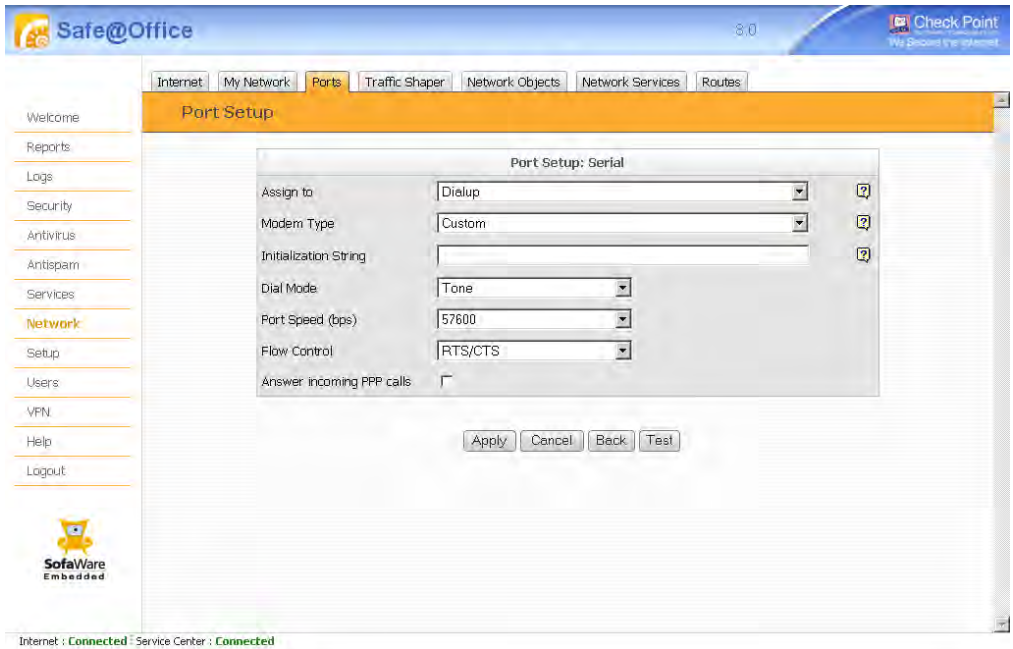
3. Next to **Serial**, click **Edit**.

   The **Port Setup** page appears.



4. In the **Assign to Network** drop-down list, select **Dialup**.

New fields appear.



5. Complete the fields using the information in ***Dialup Fields*** on page 140.
6. Click Apply.
7. To check that that the values you entered are correct, click Test.

   The page displays a message indicating whether the test succeeded.
8. Configure a Dialup Internet connection on the Serial port.

   See ***Using Internet Setup*** on page 102.

Table 24: RS232 Dialup Fields

In this field...	Do this...
Modem Type	Select the modem type. You can select one of the predefined modem types or Custom. 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.
Dial Mode	Select the dial mode the modem uses.
Port Speed	Select the Serial port's speed (in bits per second). The Serial port's speed must match that of the attached dialup modem. The default value is 57600.
Flow Control	Select the method of flow control supported by the attached device: • RTS/CTS. Hardware-based flow control, using the Serial port's RTS/CTS lines. • XON/XOFF. Software-based flow control, using XON/XOFF characters.
Answer incoming PPP calls	Select this option to specify that the modem should answer incoming PPP calls. This allows accessing the appliance out of band for maintenance purposes, in case the primary Internet connection fails. The client is assigned an IP address from the OfficeMode network; therefore, the OfficeMode network must be enabled. For information on enabling the OfficeMode network, see ***Configuring the OfficeMode Network*** on page 172.

Setting Up a USB Modem

USB

Warning: Before attaching a USB modem, ensure that the total power drawn by all connected USB devices does not exceed 2.5W per port (0.5A at 5V). If the total current consumed by a port exceeds 0.5A, a powered USB hub must be used, to avoid damage to the gateway.

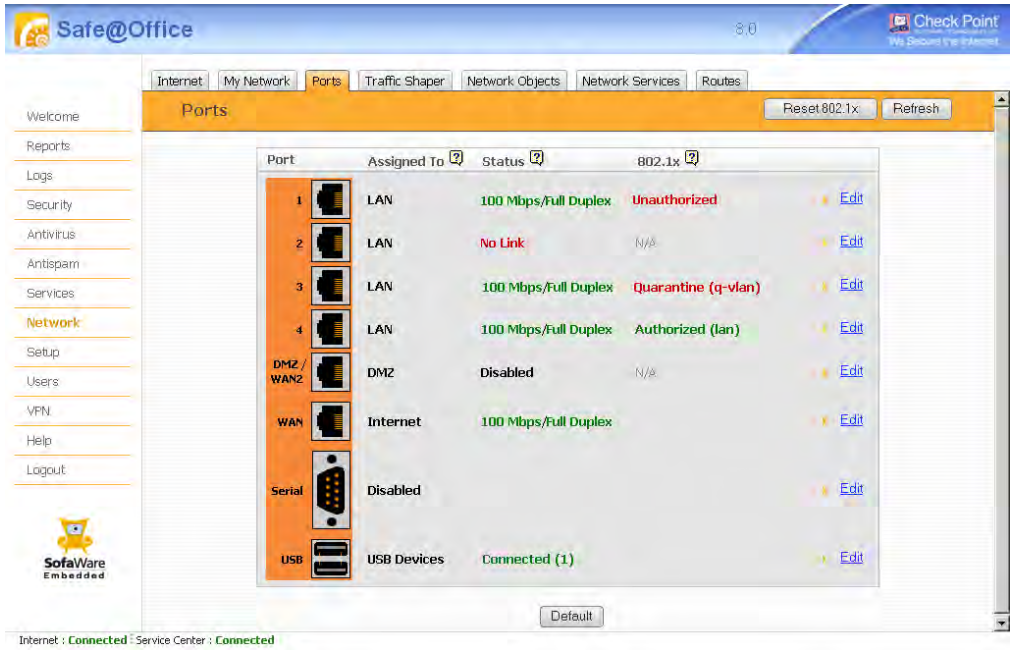
To set up a USB modem

1. Connect a USB-based modem to one of your Safe@Office appliance's USB ports.

   For information on locating the USB ports, see ***Introduction*** on page 1.

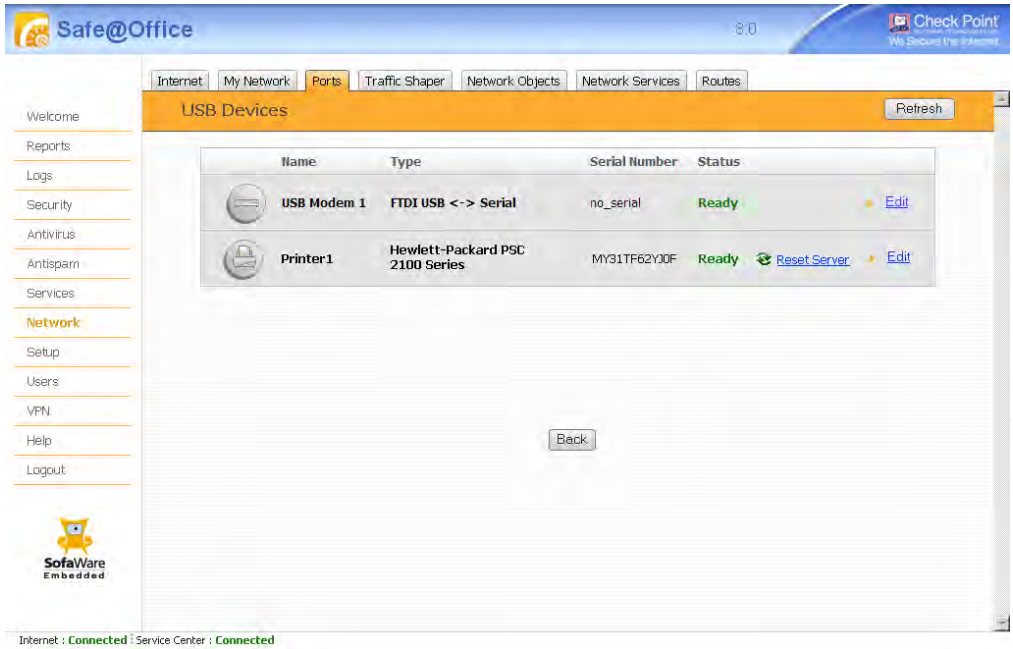
2. Click Network in the main menu, and click the Ports tab.

   The Ports page appears.



3. Next to USB, click Edit.

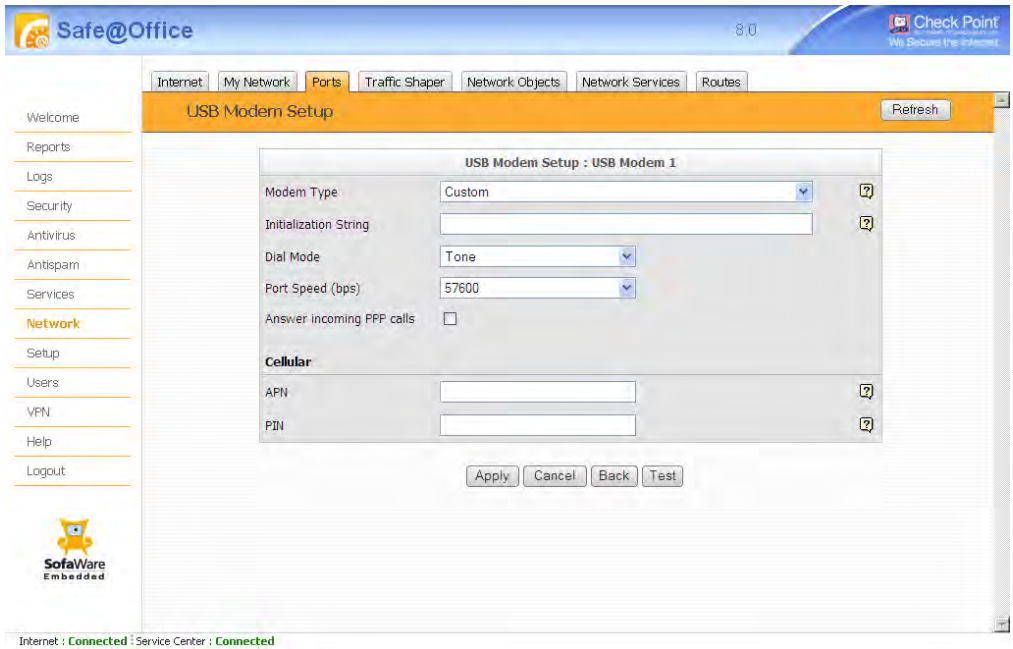
   The USB Devices page appears. If the Safe@Office appliance detected the modem, the modem is listed on the page.



   If the modem is not listed, check that you connected the modem correctly, then click Refresh to refresh the page.

4. Next to the modem, click Edit.

The USB Modem Setup page appears.



5. Complete the fields using the information in ***USB Dialup Fields*** on page 144.
6. Click Apply.
7. To check that that the values you entered are correct, click Test.

   The page displays a message indicating whether the test succeeded.
8. Configure a Dialup Internet connection on the USB port.

   See ***Using Internet Setup*** on page 102.

Table 25: USB Dialup Fields

In this field...	Do this...
Modem Type	Select the modem type. You can select one of the predefined modem types or Custom. 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.
Dial Mode	Select the dial mode the modem uses.
Port Speed	Select the modem's port speed (in bits per second).
Answer incoming PPP calls	Select this option to specify that the modem should answer incoming PPP calls. This allows accessing the appliance out of band for maintenance purposes, in case the primary Internet connection fails. The client is assigned an IP address from the OfficeMode network; therefore, the OfficeMode network must be enabled. For information on enabling the OfficeMode network, see ***Configuring the OfficeMode Network*** on page 172.
Cellular	
APN	Type your Access Point Name (APN) as given by your cellular provider. If your cellular provider has not provided you with an APN, leave this field empty.

In this field…	Do this…
PIN	Type the Personal Identification Number (PIN) code that you received with your cellular SIM card, if required by your modem. The PIN code is usually 4 digits long. Warning: Entering an incorrect PIN code may cause your SIM card to be blocked.

Viewing Internet Connection Information

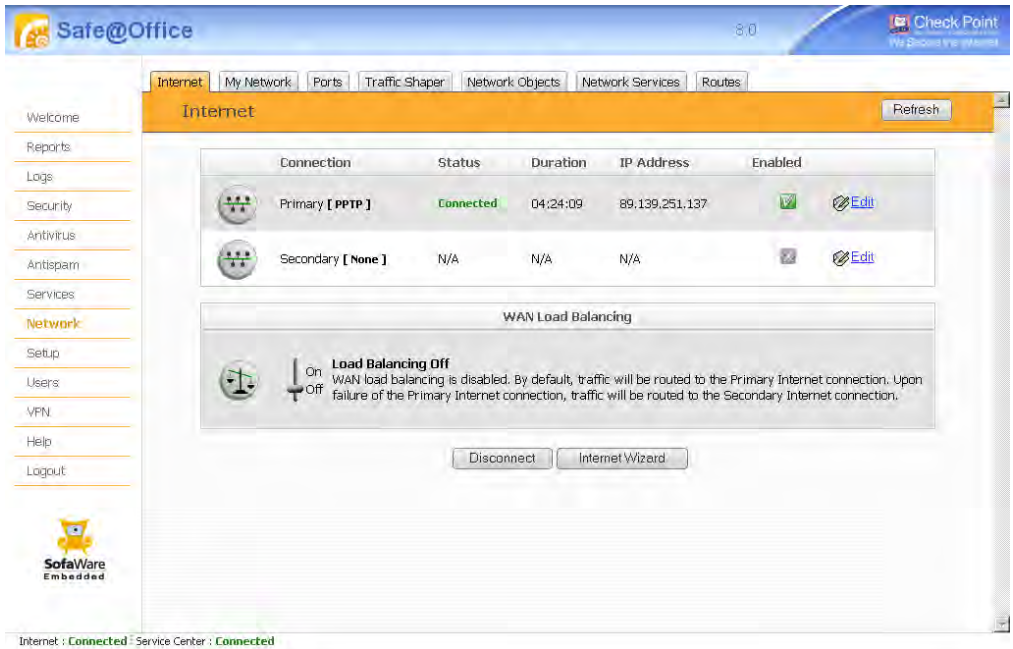
500

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 following table.

2. To view activity information for a connection, mouse-over the information icon next to the desired connection.

   A tooltip displays the number of bytes sent and received bytes through the connection.

3. To refresh the information on this page, click **Refresh**.

Table 26: 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 148

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 148.

Configuring a Backup Internet Connection

500

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.

You have full flexibility in deciding which port to use for each Internet connection. You can assign the primary connection to use any of the following ports:

- WAN port (on Non-ADSL models)
- DSL port (on ADSL models)
- Serial port (for use with an RS232 modem)
- DMZ/WAN2 port
- USB ports (for use with a USB modem)

You can assign the secondary connection to use any of the above ports that is not being used by the primary connection.

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.

Configuring WAN Load Balancing

500

If your network is prone to congestion, for example in large offices which include multiple active clients and/or servers, you can increase the amount of available bandwidth by configuring WAN load balancing. By default, the Safe@Office appliance routes all traffic to the primary Internet connection, and the secondary Internet connection is used only when the primary connection is down, or when a routing rule specifically states that traffic should be sent through the secondary connection. WAN load balancing automatically distributes traffic between the primary and secondary connections, allowing you to use both connections in parallel.

When one IP address sends packets to another IP address, the Safe@Office appliance examines each Internet connection's recent bandwidth utilization in kilobits per second to determine its load. The Safe@Office appliance then enters the source-destination pair in a load balancing table and specifies the least-loaded Internet connection as the connection to use for traffic between this pair. To prevent disruption of stateful protocols, the Safe@Office appliance will route *all* traffic between this pair to the specified Internet connection, so long as the pair remains in the load balancing table.

Note: By default, load balancing is performed when the amount of bandwidth utilization exceeds a threshold of 64 kilobits per second. You can change this threshold via the CLI. For information, refer to the Embedded NGX CLI Guide.

Note: By default, a source-destination pair is removed from the load balancing table after 1 hour of inactivity. You can change the default value via the CLI. For information, refer to the *Embedded NGX CLI Guide*.

Note: In order for WAN load balancing to be effective, there must be more than one active source-destination pair.

By default, the load distribution between Internet connections is symmetric; however, you can configure non-symmetric load balancing by assigning a different load balancing weight to each Internet connection. For example, if you assign the primary connection a weight of 100, and you assign the secondary connection a weight of 50, the Safe@Office appliance will only route traffic to the secondary connection if the primary connection's current load is more than twice the secondary connection's current load. Therefore, to

ensure full utilization of both Internet connections, the ratio between the connections' load balancing weights should reflect the ratio between the connections' bandwidths.

Note: To ensure continuous Internet connectivity, if one of the Internet connections fails, all traffic will be routed to the other connection.

To configure WAN load balancing

1. Configure the desired load balancing weight for both the primary and secondary Internet connections.

   For further information, see the Load Balancing Weight field in ***Using Internet Setup*** on page 102.

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

   The Internet page appears.

3. In the WAN Load Balancing area, drag the load balancing lever to On.

   WAN load balancing is enabled. Traffic will be distributed automatically across the defined Internet connections, according to the configured load balancing weights.

Note: You can view the effect of WAN load balancing in the Traffic Monitor.

Chapter 6

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

Note: If you accidentally change the network settings to incorrect values and are unable to connect to the my.firewall Web portal, you can connect to the appliance through the serial console and correct the error (see ***Using a Console*** on page 676). Alternatively, you can reset the Safe@Office appliance to its default settings (see ***Resetting the Safe@Office appliance to Defaults*** on page 728).

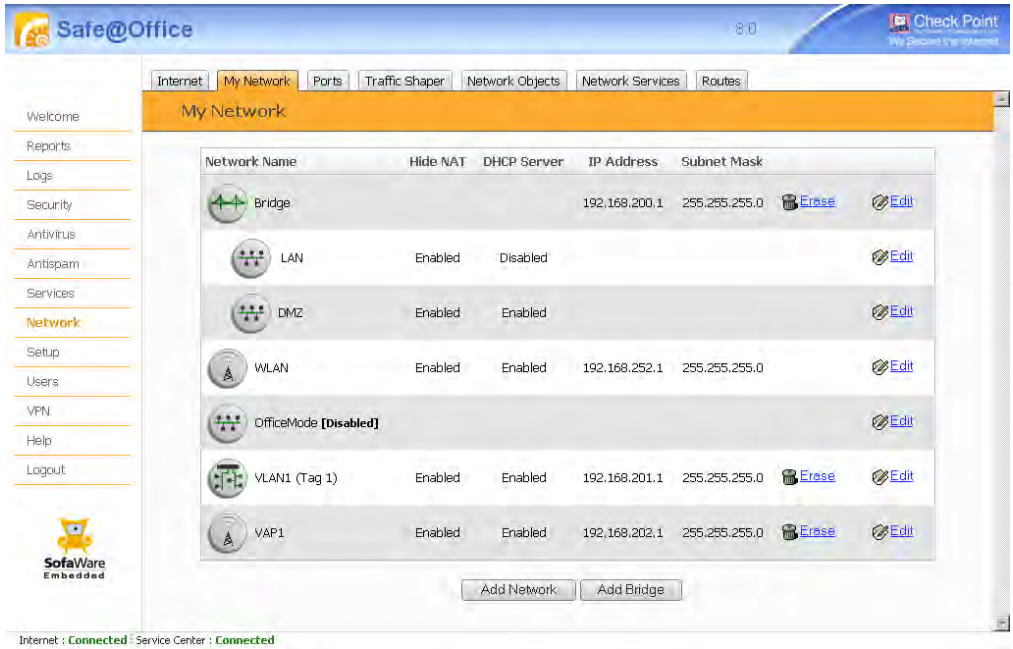
Configuring the LAN Network

500

To configure the LAN network

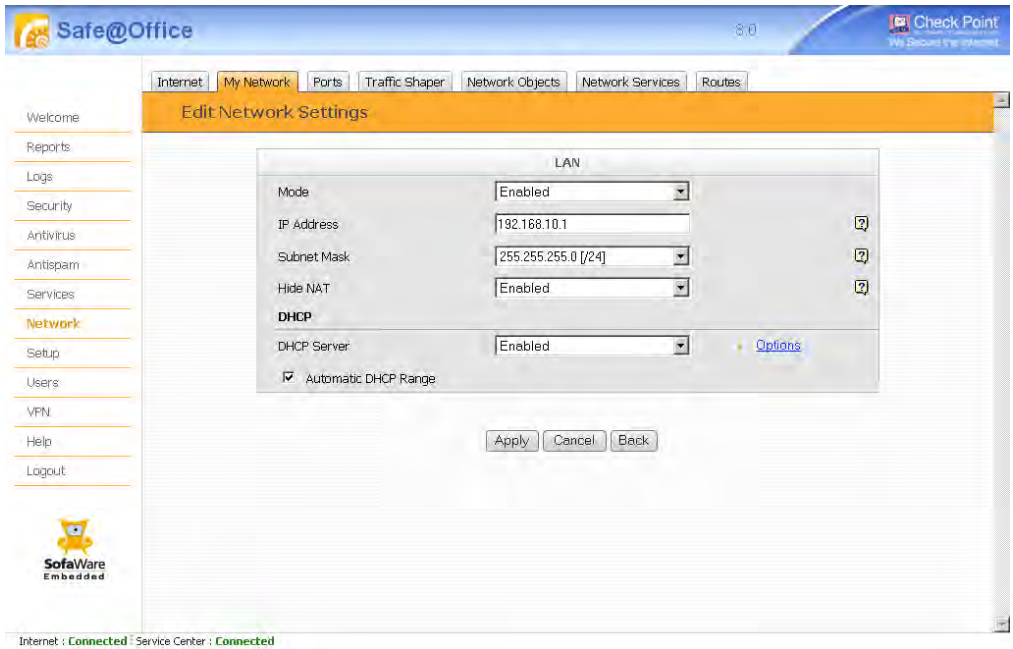
1. Click **Network** in the main menu, and click the **My Network** tab.

   The **My Network** page appears.



2. Click **Edit** in the LAN network's row.

The Edit Network Settings page for the LAN network appears.



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

   The fields are enabled.

4. If desired, change your Safe@Office appliance's internal IP address.

   See ***Changing IP Addresses*** on page 156.

5. If desired, enable or disable Hide NAT.

   See ***Enabling/Disabling Hide NAT*** on page 157.

6. If desired, configure a DHCP server.

   See ***Configuring a DHCP Server*** on page 158.

7. Click Apply.

   A warning message appears.

8. Click OK.

   A success message appears.

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.

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 desired 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.

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 54.

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, Hide NAT, and custom NAT rules 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 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. However, if you do assign the computer an IP address within the DHCP address range, the DHCP server will detect this and 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 185.

Note: The following DHCP server configurations are not available for the OfficeMode network:

- Enabling and disabling the Safe@Office DHCP Server
- Setting the DHCP range manually
- Configuring DHCP relay

Enabling/Disabling the Safe@Office DHCP Server

500

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

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.

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.

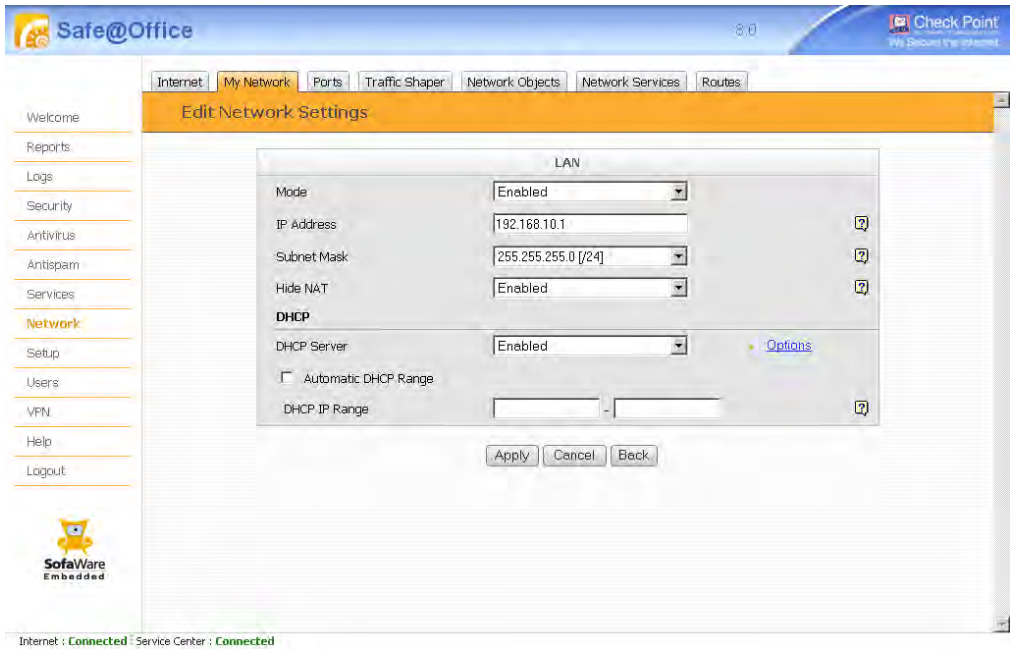
   The Edit Network Settings page appears.

3. Do one of the following:

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

     1) Clear the Automatic DHCP range check box.

The DHCP IP range fields appear.



2) In the DHCP IP range fields, type the desired DHCP range.

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.

   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.

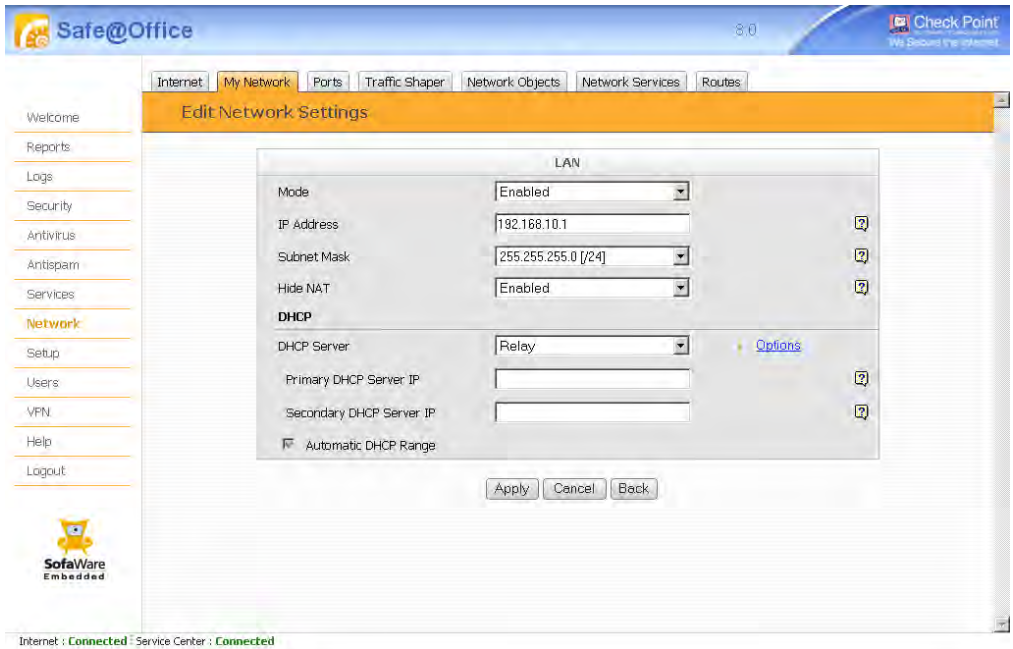
To configure DHCP relay

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 new fields appear.



4. In the Primary DHCP Server IP field, type the IP address of the primary DHCP server.
5. In the Secondary DHCP Server IP field, type the IP address of the DHCP server to use if the primary DHCP server fails.
6. Click Apply.

   A warning message appears.
7. Click OK.

   A success message appears
8. 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
- Default gateway
- NTP servers
- VoIP call managers
- TFTP server and boot filename
- Avaya, Nortel, and Thomson IP phone configuration strings

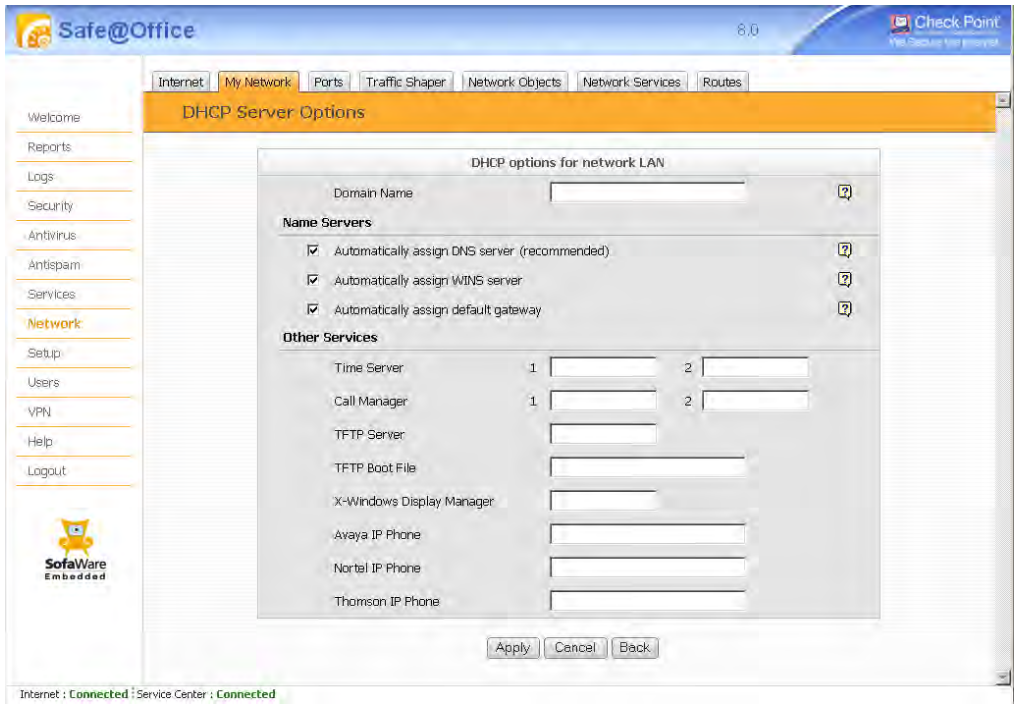
To configure DHCP options

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.

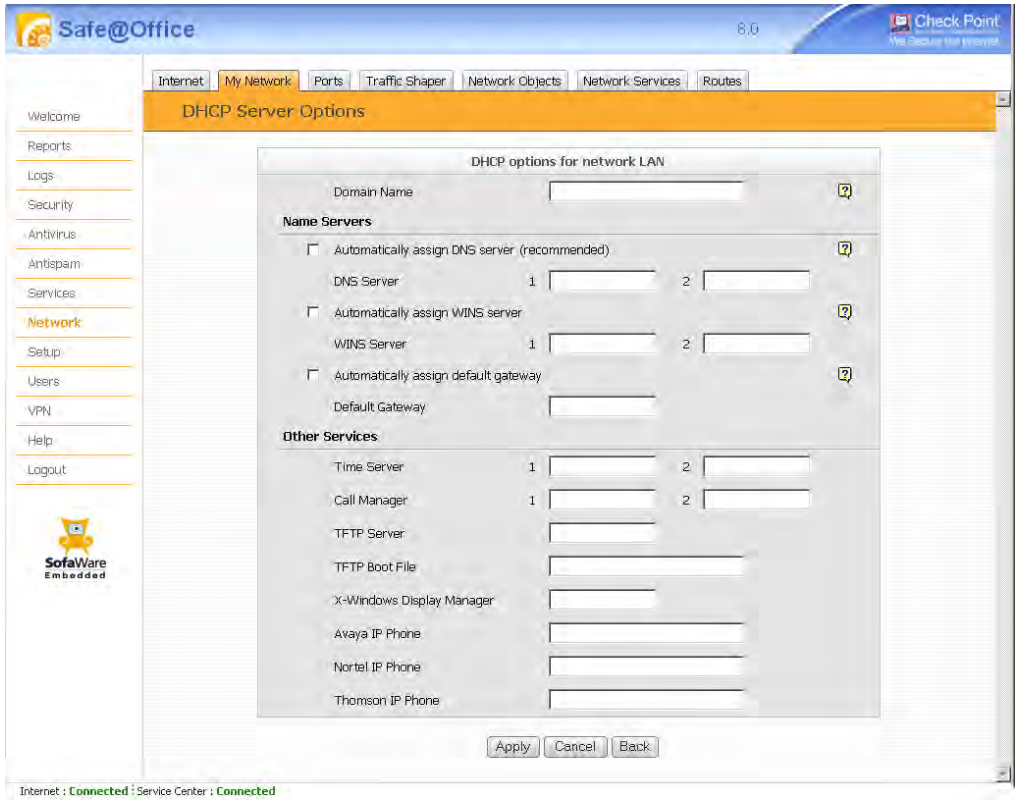
   The Edit Network Settings page appears.
3. In the DHCP area, click Options.

The DHCP Server Options page appears.



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

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 27: 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”.
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.

In this field...	Do this...
Automatically assign default gateway	Clear this option if you do not want the DHCP server to pass the current gateway IP address to DHCP clients as the default gateway's IP address. Normally, it is recommended to leave this option selected. The Default Gateway field is enabled.
Default Gateway	Type the IP address to pass to DHCP clients as the default gateway, instead of the current gateway IP address.
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 IP phones, type the IP address of the Primary and Secondary VoIP servers.
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.
X-Windows Display Manager	To assign X-Windows terminals the appropriate X-Windows Display Manager when booting via DHCP, type the XDM server's IP address.
Avaya IP Phone	To enable Avaya IP phones to receive their configuration, type the phone's configuration string.

In this field...	Do this...
Nortel IP Phone	To enable Nortel IP phones to receive their configuration, type the phone's configuration string.
Thomson IP Phone	To enable Thomson IP phones to receive their configuration, type the phone's configuration string.

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 353.

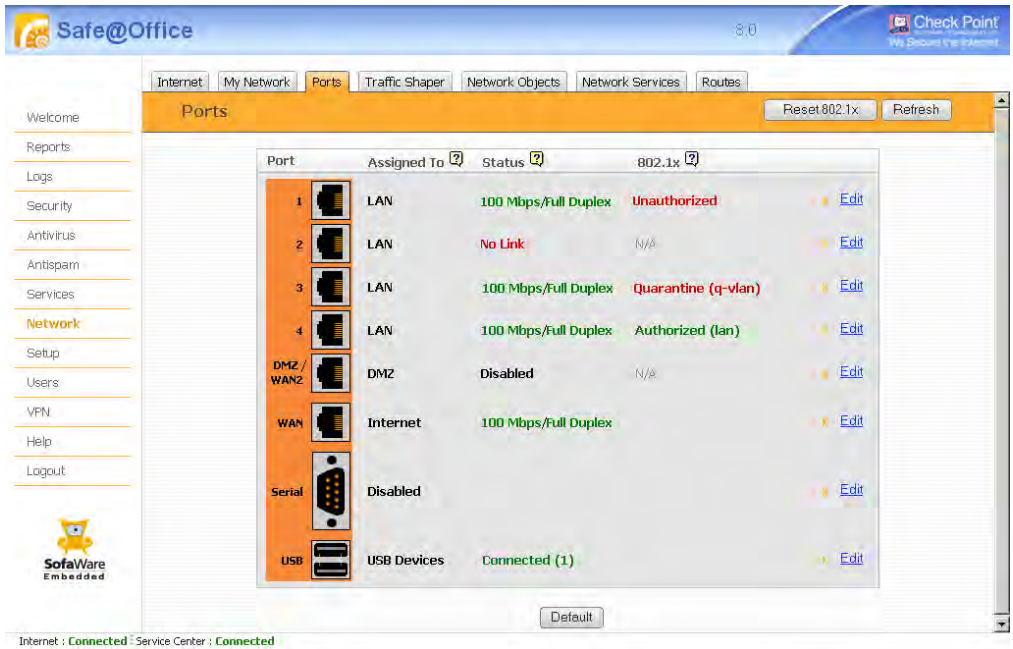
To configure a DMZ network

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.

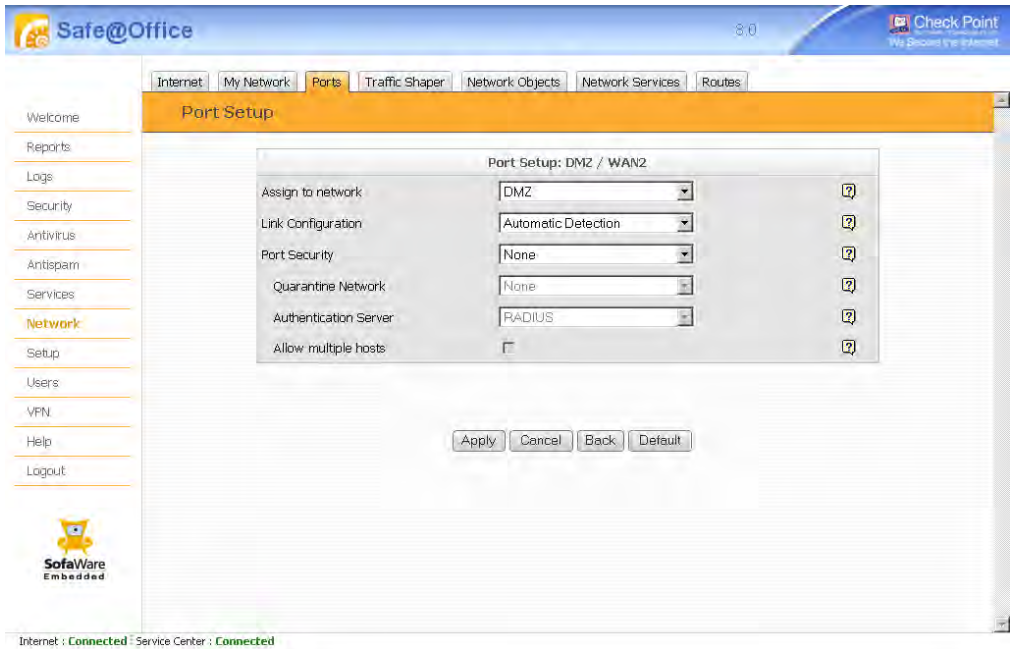
2. Click Network in the main menu, and click the Ports tab.

The **Ports** page appears.



3. Next to the **DMZ/WAN2** port, click **Edit**.

The Port Setup page appears.



4. In the Assign to network drop-down list, select DMZ.
5. Click Apply.

   A warning message appears.
6. Click OK.
7. Click Network in the main menu, and click the My Network tab.

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

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

   The fields are enabled.
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 drop-down list, select the DMZ's internal network range.
12. If desired, enable or disable Hide NAT.

    See ***Enabling/Disabling Hide NAT*** on page 157.
13. If desired, configure a DHCP server.

    See ***Configuring a DHCP Server*** on page 158.
14. Click Apply.

    A warning message appears.
15. 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 either Check Point SecureClient or an L2TP client 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 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 157.

7. If desired, configure DHCP options.

   See ***Configuring DHCP Server Options*** on page 164.

8. Click Apply.

   A warning message appears.

9. Click OK.

   A success message appears.

Configuring VLANs

Power Pack

Your Safe@Office appliance allows you to 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.

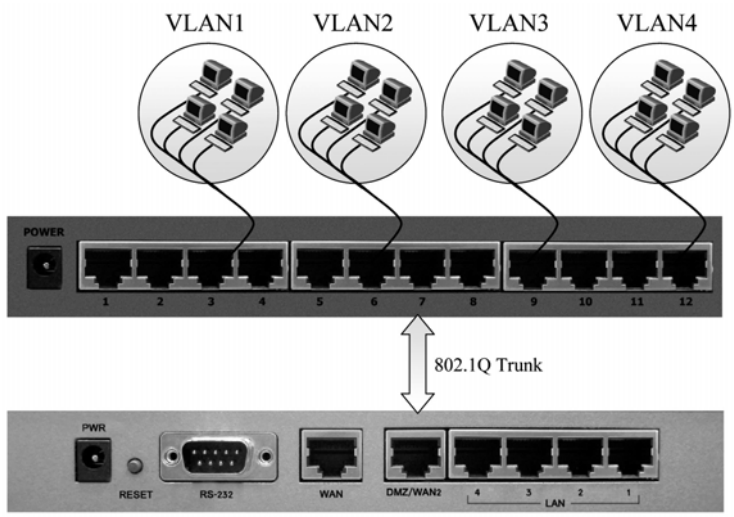


Figure 17: Tag-Based VLAN

- 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.

  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 by the number of appliance LAN ports.

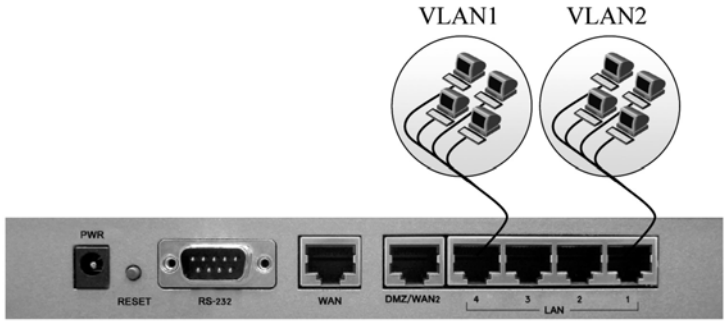


Figure 18: Port-Based VLAN

- Virtual access point (VAP)

  In wireless Safe@Office models, you can partition the primary WLAN network into wireless VLANs called virtual access points (VAPs). You can use VAPs to grant different permissions to groups of wireless users, by configuring each VAP with the desired security policy and network settings, and then assigning each group of wireless users to the relevant VAP. For example, you could assign different permissions to employees and guests on the company's wireless network, by configuring two VAPs called “Guest” and “Employee” with the desired set of permissions.

  To use VAPs, you must enable the primary WLAN network.

  For more information on VAPs, see ***Overview*** on page 263.

- Wireless Distribution System (WDS) links

  In wireless Safe@Office models, you can extend the primary WLAN's coverage area, by creating a Wireless Distribution System (WDS). A WDS is a system of access points that communicate with each other wirelessly, without any need for a wired backbone. WDS is usually used together with bridge mode to connect the networks behind the access points.

  To create a WDS, you must add WDS links between the desired access points. For example, if your business extends across a large area, and a single access point does not provide sufficient coverage, then you can add a second access point and create a WDS link between the two access points.

  To use WDS links, you must enable the primary WLAN network.

  For more information on WDS links, see ***Overview*** on page 263.

In Safe@Office models with unlimited nodes, you can define up to 32 VLAN networks (port-based, tag-based, VAP, and WDS links combined), while in other models, you can define up to ten VLAN networks. In wireless models, up to three of the VLAN networks can be VAPs, and up to seven of the VLAN networks can be WDS links. For information on counting VAPs and WDS links, see ***Configuring a Wireless Network*** on page 263.

For information on the default security policy for VLANs, see ***Default Security Policy*** on page 353.

Adding and Editing VLANs

Power Pack

For information on adding and editing port-based VLANs, see ***Adding and Editing Port-Based VLANs*** on page 178.

For information on adding and editing tag-based VLANs, see ***Adding and Editing Tag-Based VLANs*** on page 180.

For information on adding and editing VAPs, see ***Configuring Virtual Access Points*** on page 294.

For information on adding and editing WDS links, see ***Configuring WDS Links*** on page 298.

Adding and Editing Port-Based VLANs

Power Pack

To add or edit a port-based VLAN

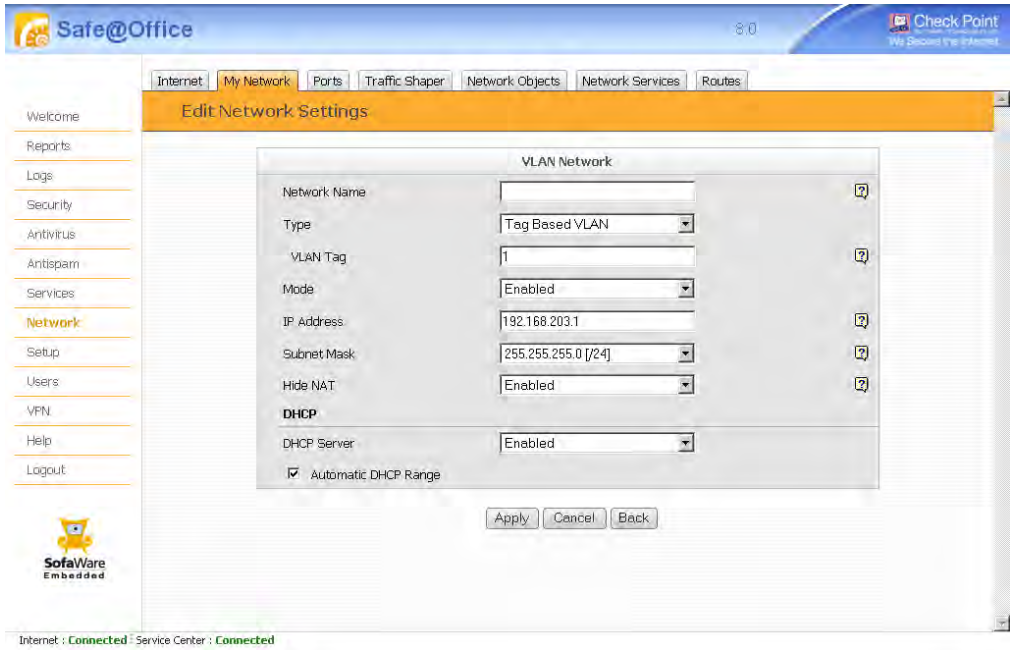
1. Click Network in the main menu, and click the My Network tab.

   The My Network page appears.

2. Do one of the following:

   - To add a VLAN, click Add Network.
   - To edit a VLAN, 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 Mode drop-down list, select Enabled.

   The fields are enabled.

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 157.

9. If desired, configure a DHCP server.

   See ***Configuring a DHCP Server*** on page 158.

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. Next to the LAN port you want to assign, click Edit.

    The Port Setup page appears.

14. In the Assign to network drop-down list, select the VLAN network's name.

    You can assign more than one port to the VLAN.

15. 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, click Add Network.
   - To edit a VLAN, 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 Mode drop-down list, select Enabled.

   The fields are enabled.

7. 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.

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

   See ***Enabling/Disabling Hide NAT*** on page 157.

10. If desired, configure a DHCP server.

    See ***Configuring a DHCP Server*** on page 158.

11. Click Apply.

    A warning message appears.

12. Click OK.

    A success message appears.

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

    The Ports page appears.

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

15. Click Apply.

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

16. 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.

17. 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. Delete any firewall rules or VStream Antivirus rules that use this VLAN.

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

    The My Network page appears.

4. In the desired VLAN's row, click Erase.

   A confirmation message appears.

5. Click OK.

   The VLAN is deleted.

Using the Internal DNS Server

500

The Safe@Office appliance includes an internal DNS server, which can resolve DNS names for hosts defined as network objects. Each host is assigned a DNS name in the format `<networkobjectname>.<domainsuffix>`, where `<networkobjectname>` is the name of the network object representing the host, and `<domainsuffix>` is the domain name suffix configured for the internal DNS server. The internal DNS server will reply to all DNS requests for the host's DNS name with the host's IP address.

In addition to resolving network objects, the internal DNS server also resolves requests for the current gateway. If a gateway hostname is defined, the DNS server will reply to DNS requests in the format `<hostname>.<domainsuffix>` with the gateway's internal IP address. For information on configuring the gateway's hostname, see ***Configuring a Gateway Hostname*** on page 687.

Note: The internal DNS server responds to DNS requests from internal network hosts only. It does not respond to requests from the Internet.

Example

If a computer with the IP address 192.188.22.1 is represented by a network object called "server1", and the internal DNS server is configured with the domain suffix "mycompany.com", then the computer's DNS name will be "server1.mycompany.com", and the internal DNS server will reply to all DNS requests for "server1.mycompany.com" with the IP address 192.188.22.1.

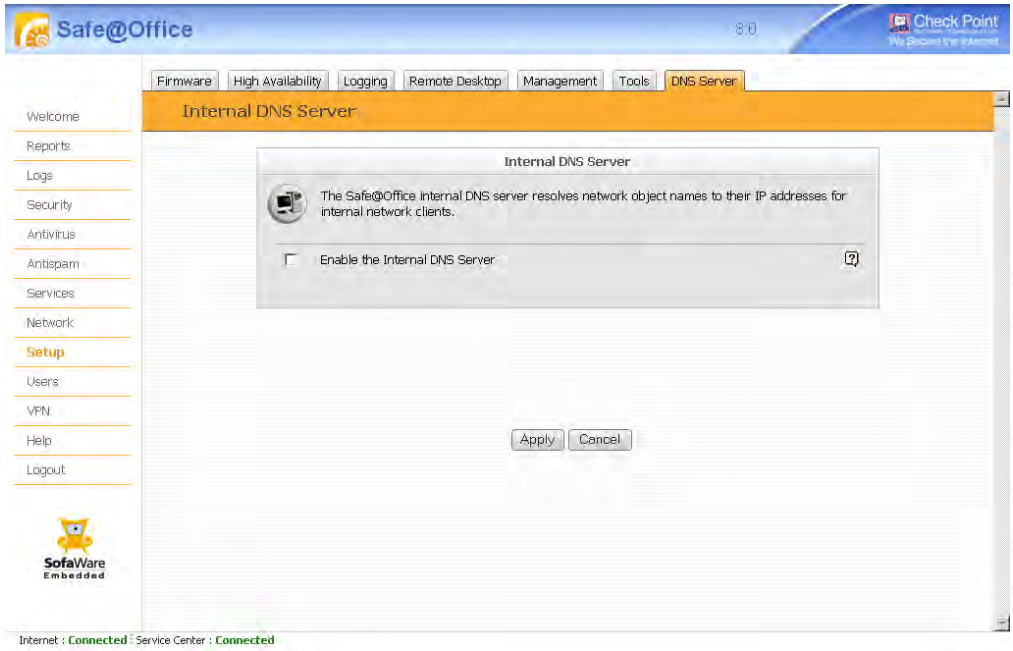
In addition, if the gateway is configured with the hostname "mygateway", the DNS server will reply to all DNS requests for "mygateway.mycompany.com" with the gateway's internal IP address.

Enabling the Internal DNS Server

To enable the internal DNS server

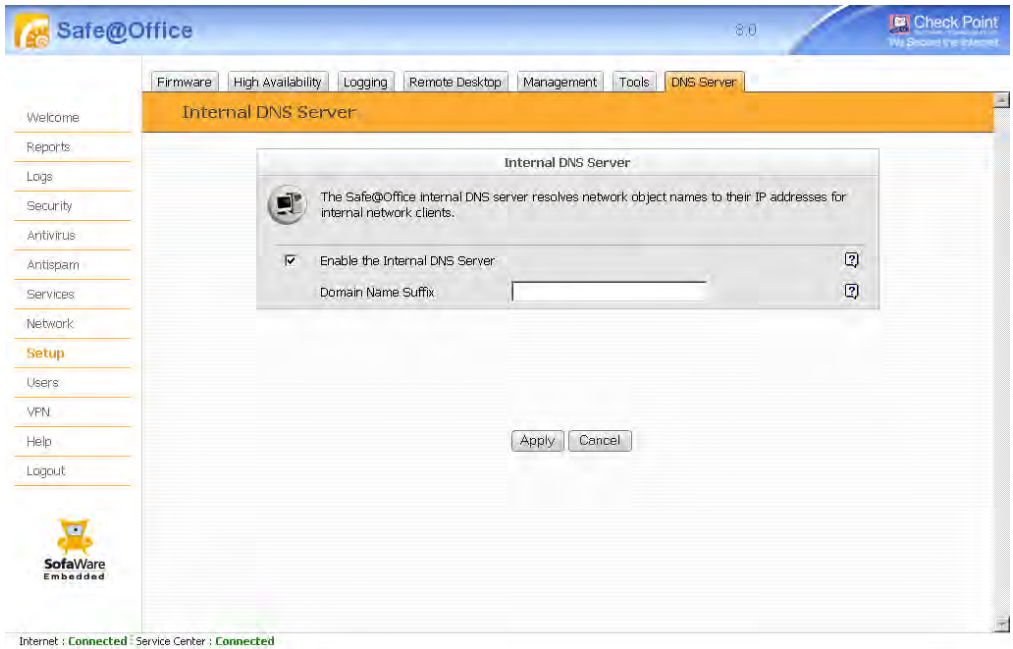
1. Click **Setup** in the main menu, and click the **DNS Server** tab.

   The **DNS Server** page appears.



2. Select the **Enable the Internal DNS Server** check box.

The **Domain Name Suffix** field appears.



3. In the **Domain Name Suffix** field, type the desired domain name suffix.

Using Network Objects

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 360.

Note: Static NAT, Hide NAT, and custom NAT rules 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.

- Web Filtering enforcement

  You can specify whether or not to enforce the Web Filtering service and Web rules for the network object. Network objects that are excluded from such enforcement will be able to access the Internet without restriction. For information on Web Filtering, see ***Web Filtering*** on page 537. For information on Web rules, see ***Using Web Rules*** on page 529.

- 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. Furthermore, users on HotSpot networks will be able to access the excluded network object without viewing the My HotSpot page. For information on Secure HotSpot, see ***Configuring Secure HotSpot*** on page 380.

- 802.1x port-based security enforcement

  In Safe@Office 500 with Power Pack, when DHCP reservation is used, you can specify whether or not to exclude a computer from 802.1x port-based security enforcement. Excluded computers will be able to connect to the Safe@Office appliance's ports and access the network without authenticating. For information on 802.1x port-based security, see ***Using Port-Based Security*** on page 374.

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.

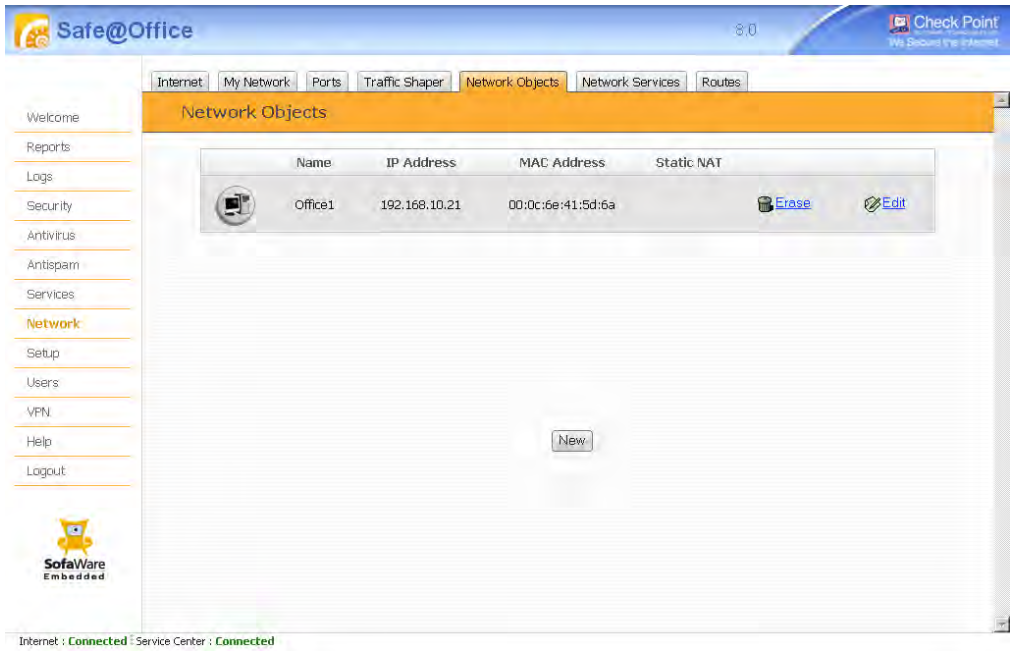
- The My Computers page

  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 the Edit icon 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**.

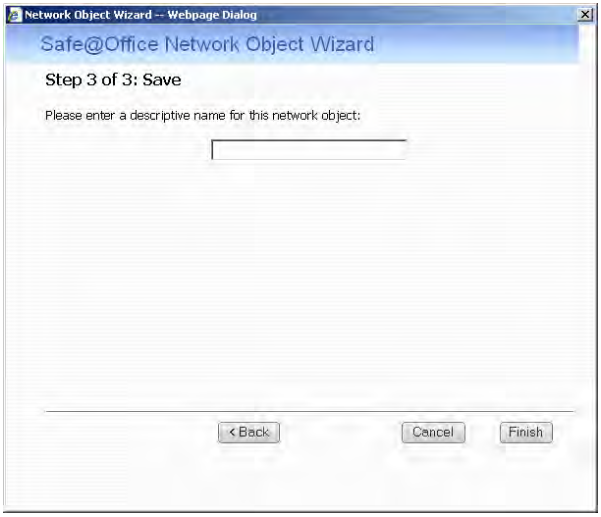
4. Click **Next**.

The **Step 2: Computer Details** dialog box appears. If you chose **Single Computer**, the dialog box includes the **Reserve a fixed IP address for this computer** 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.

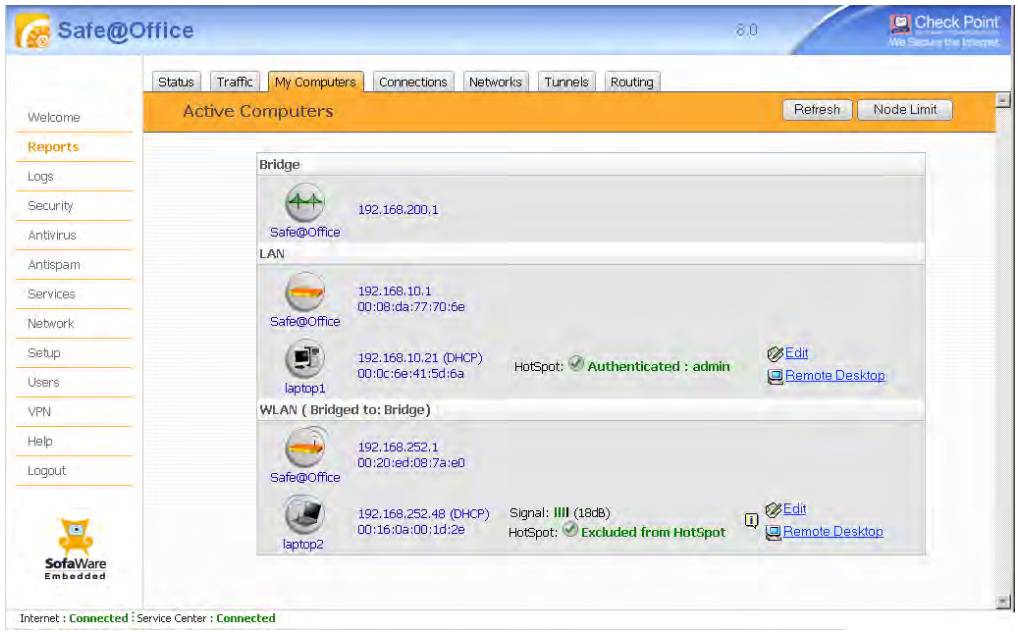


7. Type a name for the network object in the field.
8. Click Finish.

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

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

The My 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 28: 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 and Allow this computer to connect when MAC filtering is enabled	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 263. The MAC Address and Exclude this computer from 802.1x Port Security fields are enabled.
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.

In this field...	Do this...
Exclude this computer from 802.1x Port Security	Select this option to exclude this computer from 802.1x port-based security enforcement. The computer will be able to connect to a Safe@Office appliance ports and access the network without authenticating.
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 this computer from Secure HotSpot enforcement. This computer will be able to access the network without viewing the My HotSpot page. Furthermore, users on HotSpot networks will be able to access this computer without viewing the My HotSpot page.
Exclude this computer from Web Filtering	Select this option to exclude this computer from the Web Filtering service and Web rule enforcement.

Table 29: 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 Secure HotSpot enforcement. Computers on the excluded network will be able to access your network without viewing the My HotSpot page. Furthermore, users on HotSpot networks will be able to access computers on the excluded network without viewing the My HotSpot page.
Exclude this network from Web Filtering	Select this option to exclude this network from the Web Filtering service and Web rules.

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 Erase.

      A confirmation message appears.

   b. Click OK.

      The network object is deleted.

Configuring Network Service Objects

500

You can add custom services as network service objects. This enables you to configure firewall rules, VStream Antivirus rules, custom NAT rules, and static routes for the services represented by the network service objects.

Defining network service objects can make your policies easier to understand and maintain. When a network service object is modified, the change automatically takes effect in all rules and settings that reference the network service object.

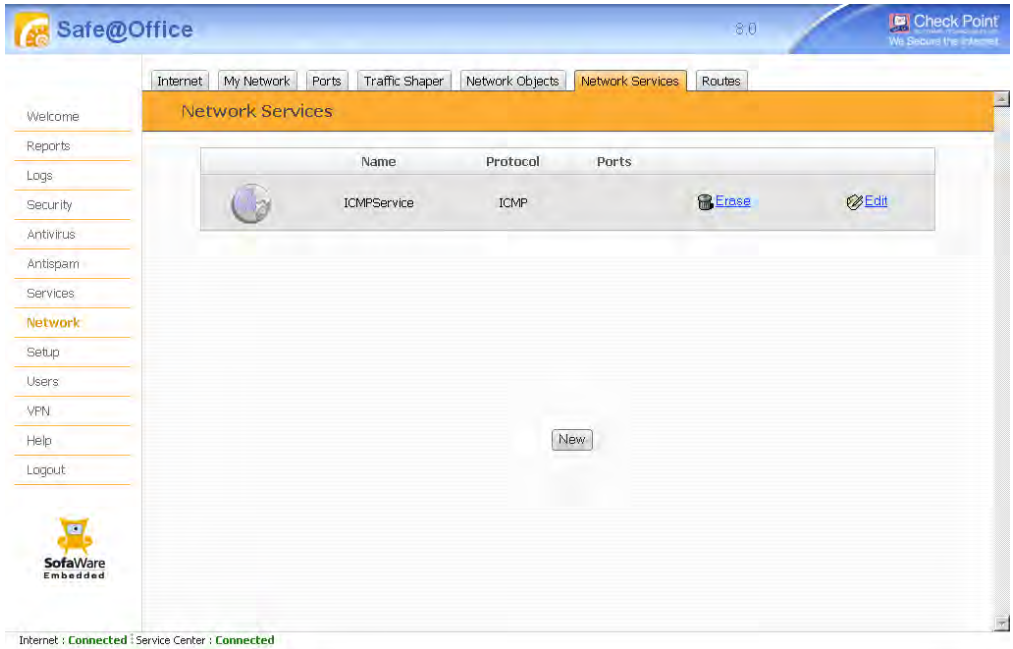
Adding and Editing Network Service Objects

500

To add or edit a network service object

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

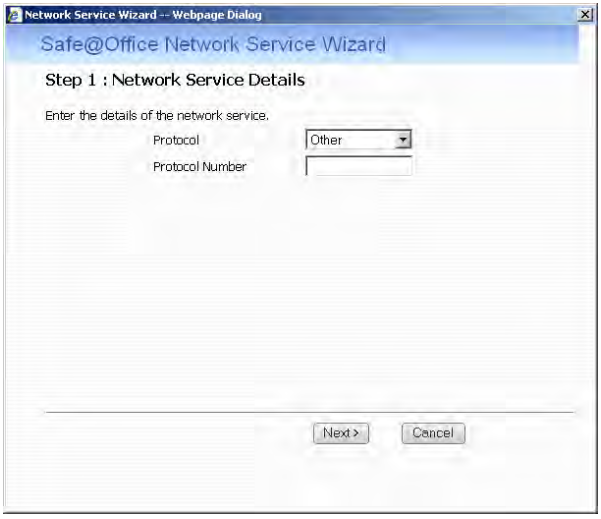
   The Network Services page appears with a list of network service objects.



2. Do one of the following:

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

The **Safe@Office Network Service Wizard** opens, with the **Step 1: Network Service Details** dialog box displayed.



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

   The **Step 2: Network Service Name** dialog box appears.

5. Type a name for the network service object in the field.

6. Click Finish.

Table 30: Network Service Fields

In this field…	Do this…
Protocol	Select the network service's IP protocol. If you select Other, the Protocol Number field appears. If you select TCP or UDP, the Port Ranges field appears.
Protocol Number	Type the number of the network service's IP protocol.
Port Ranges	Type the network service's port or port ranges. Multiple ports or port ranges must be separated by commas. For example: "1000-1003,2000-2001,2005".

Viewing and Deleting Network Service Objects

500

To view or delete a network service object

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

   The Network Services page appears with a list of network service objects.
2. To delete a network service object, do the following:
   a. In the desired network service object's row, click Erase.

      A confirmation message appears.
   b. Click OK.

      The network service object is deleted.

Using Static Routes

500

A static route is a setting that explicitly specifies the route to use for packets, according to *one* of the following criteria:

- The packet's source IP address and/or destination IP address
- The network service used to send the packet

Packets that match the criteria for a specific static route are sent to the route's defined destination, or *next hop*, which can be a specific gateway's IP address or an Internet connection. Specifying an Internet connection as the static route's next hop is useful in cases where the ISP's default gateway IP address is dynamically assigned to the gateway, as this approach allows you to route traffic to the Internet connection by specifying its name, instead of a static IP address.

Note: If the static route's next hop is an Internet connection that is currently unavailable, the Safe@Office appliance sends matching traffic through the static route with the next-lowest metric.

Packets with a source, destination, or network service that do not match any defined static route are routed to the default gateway. To modify the default gateway, see ***Using a LAN Connection*** on page 115.

When a static route is based on the packet's source, it is called a *source route*. Source routing can be used, for example, for load balancing between two Internet connections. For instance, 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.

A static route that is based on the network service used to send the packet is called a *service route*. Service routing is useful for directing all traffic of a particular type to a specific Internet connection. For example, you can choose to route all HTTP traffic to the secondary Internet connection, while routing all other traffic to the primary Internet connection. Service routes can be defined for network service objects, enabling you to create routes for custom protocols and port ranges.

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

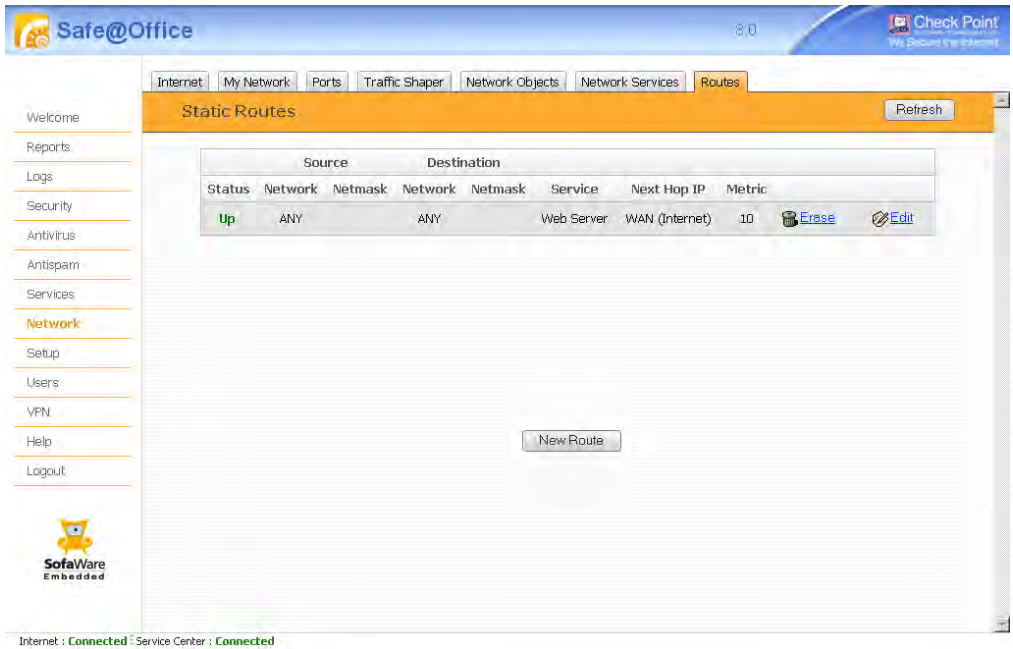
Adding and Editing Static Routes

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.



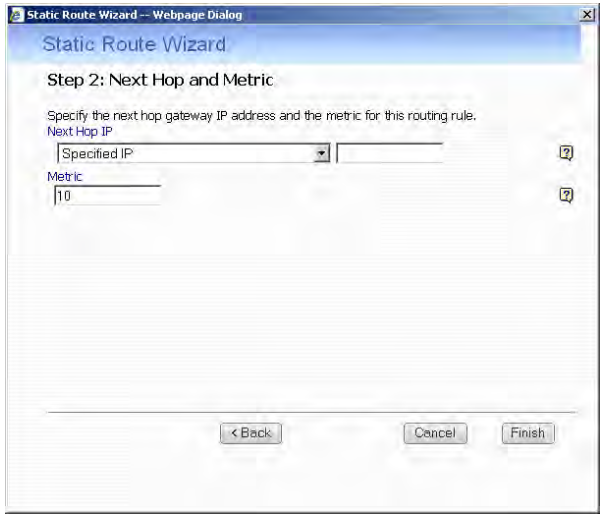
2. Do one of the following:

   - 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. Complete the fields using the relevant information in the following table.
4. Click **Next.**

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



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

6. Click **Next**.

   The new static route is saved.

Table 31: Static Route Fields

In this field…	Do this…
Source	Specify the source network (source routing). This can be either of the following: • ANY. This route applies to packets originating in any network. • Specified Network. This route applies to packet originating in a specific network. The Network and Netmask fields appear.
Source - Network	Type the source network's IP address.
Source - Netmask	Select the source network's subnet mask.
Destination	Specify the destination network. This can be either of the following: • ANY. This route applies to packets sent to any network. • Specified Network. This route applies to packets sent to a specific network. The Network and Netmask fields appear.
Destination - Network	Type the destination network's IP address.
Destination - Netmask	Select the destination network's subnet mask.

In this field…	Do this…
Service	Specify the service used to send packets (service routing). This can be either of the following: • ANY. This route applies to packets sent using any service. • A specific service or network service object. Note: When defining a static route for a specific service, the Source and Destination fields must be set to ANY.
Next Hop IP	Specify the next hop to which packets should be sent. This can be any of the following: • Specified IP. Traffic matching this static route's criteria will be routed to a specific gateway. Type the IP address of the desired gateway (next hop router) in the field provided. • WAN (Internet). Traffic matching this static route's criteria will be routed to the Internet connection on the WAN1 interface. • WAN2 (Internet). Traffic matching this static route's criteria will be routed to the Internet connection on the WAN2 interface.
Metric	Type the static route's metric. When a packet matches multiple static routes' criteria, the gateway sends the packet to the matching route with the lowest metric. The default value is 10.

Viewing and Deleting Static Routes

500

To view or 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. To refresh the view, click Refresh.
3. To delete a route, do the following:

   a. In the desired route's row, click Erase.

      A confirmation message appears.

   b. 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 following table. If desired, you can also disable ports.

Table 32: Ports and Assignments

You can assign this port...	To these uses...
LAN 1-4	LAN network
	A WAN Internet connection
	A port-based VLAN
	A VLAN that is dynamically assigned by a RADIUS server, as part of an 802.1x port-based security scheme
DMZ/WAN2	DMZ network
	A WAN Internet connection
	VLAN trunk
	A port-based VLAN
	A VLAN that is dynamically assigned by a RADIUS server, as part of an 802.1x port-based security scheme
WAN	A WAN Internet connection
Serial	RS232 modem
	Serial console

You can assign this port...	To these uses...
USB	Printers
	USB-based modems

The Safe@Office appliance also allows you to restrict each port to a specific link speed and duplex setting and to configure its security scheme. For information on port-based security, see ***Using Port-Based Security*** on page 374.

Viewing Port Statuses

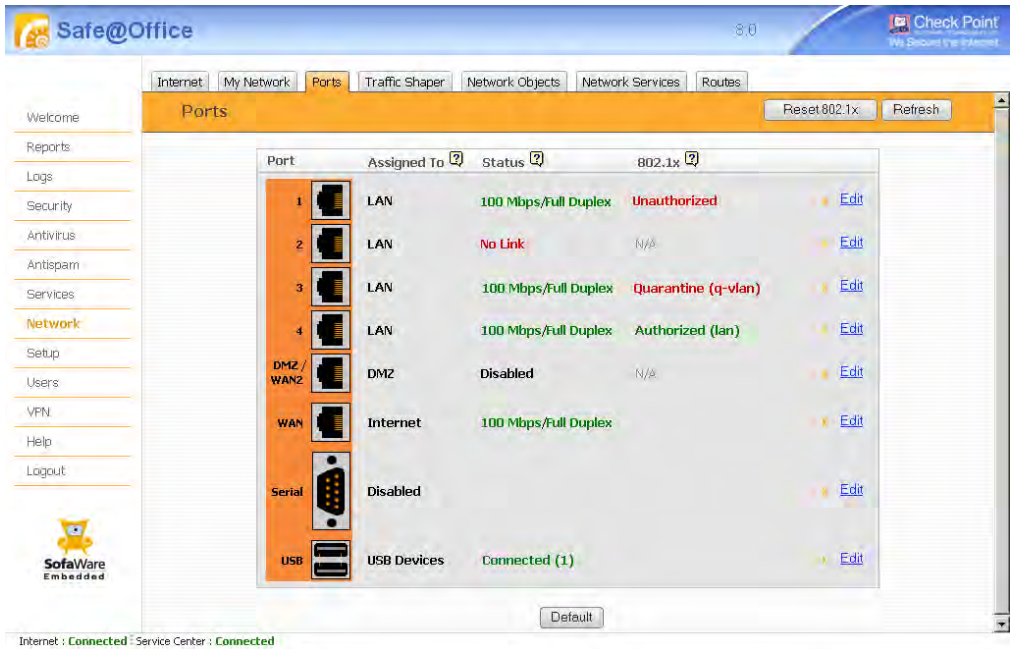
500

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.

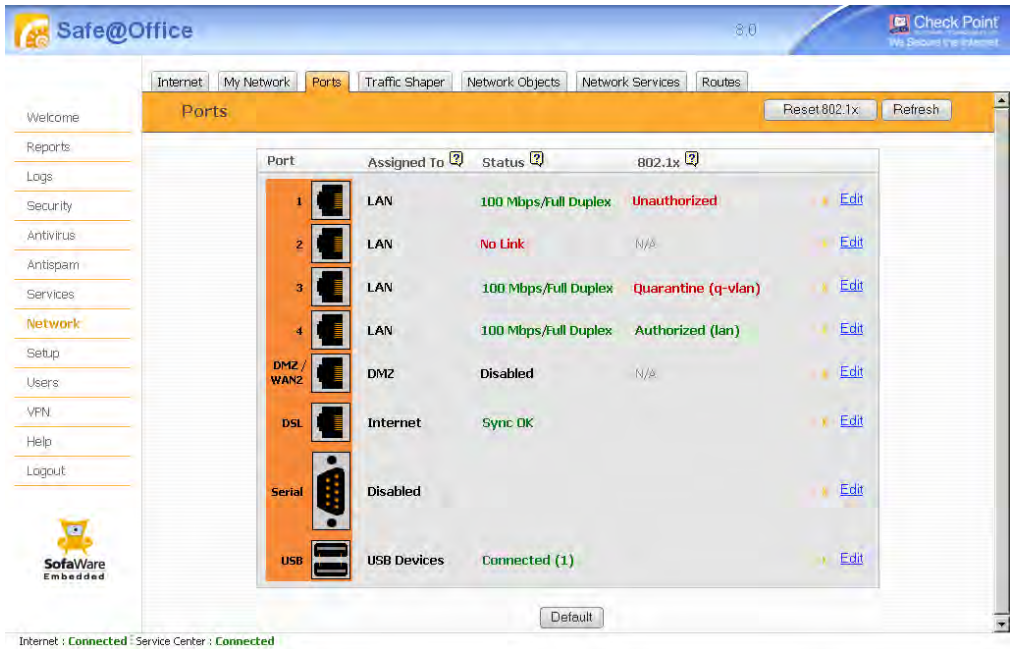
To view port statuses

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

The **Ports** page appears. In non-ADSL models, this page appears as follows:



In ADSL models, this page appears as follows:



The page displays the information for each port, as described in the following table.

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

Table 33: Ports Fields

This field…	Displays…
Assign To	The port's current assignment. For example, if the DMZ/WAN2 port is currently used for the DMZ, the field displays "DMZ".

This field...	Displays...
Status	The port's current status. Ethernet ports can have the following statuses:

Status	Description
The detected link speed and duplex (Full Duplex or Half Duplex)	The port is in use.
No Link	The appliance does not detect anything connected to the port.
Disabled	The port is disabled. For example, the DMZ/WAN2 port's status will be "Disabled" if the port is assigned to "None", or if it assigned to "DMZ" and the DMZ is disabled.

This field...	Displays...
	The ADSL port can have the following statuses:

Status	Description
Sync OK	The ADSL modem synchronized with the ADSL service provider.
No Sync	The ADSL modem failed to synchronize with the ADSL service provider. Check that a micro-filter is properly connected, and check that your DSL Standard setting is compatible with your service provider. You can view this setting in the Network > Internet Setup page.

The USB port can have the following statuses:

Status	Description
Connected (number)	USB devices (printers or modem) are connected to the USB ports. The number of connected devices appears in parentheses.
Not Connected	No USB devices are connected to the USB ports.

This field...	Displays...
802.1x	The port's security scheme. This can be any of the following:

Scheme	Description
N/A	No security scheme is defined for the port.
Unauthorized	An 802.1x security scheme is defined for the port. Users have not yet connected to the port and attempted to authenticate, *or* a user failed to authenticate and no Quarantine network is configured.
Authorized (network)	An 802.1x security scheme is defined for the port. A user connected to the port, authenticated successfully, and was assigned to a network. The name of the assigned network appears in parentheses.
Quarantine (network)	An 802.1x security scheme is defined for the port. A user connected to the port, failed to authenticate, and was assigned to the Quarantine network. The name of the Quarantine network appears in parentheses.

For information on configuring 802.1x port-based security, see ***Using Port-Based Security*** on page 374.

Modifying Port Assignments

500

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

Table 34: Modifying Port Assignments

To assign a port to...	See...
No network	The procedure below. This disables the port.
LAN	The procedure below
VLAN or VLAN Trunk	***Configuring VLANs*** on page 174
A WAN Internet connection	The procedure below. Note: When you configure an Ethernet-based Internet connection on a port, the port is automatically assigned to Internet use. For information on configuring an Internet connection, see ***Using Internet Setup*** on page 102.
DMZ	Configuring a DMZ Network
Console	***Using a Console*** on page 676
A VLAN network, dynamically assigned by a RADIUS server	***Configuring Port-Based Security*** on page 375
A printer	***Setting Up Network Printers*** on page 734
An RS232 Modem	***Setting Up an RS232 Modem*** on page 137

To assign a port to...	See...
A USB-based modem	***Setting Up a USB Modem*** on page 141

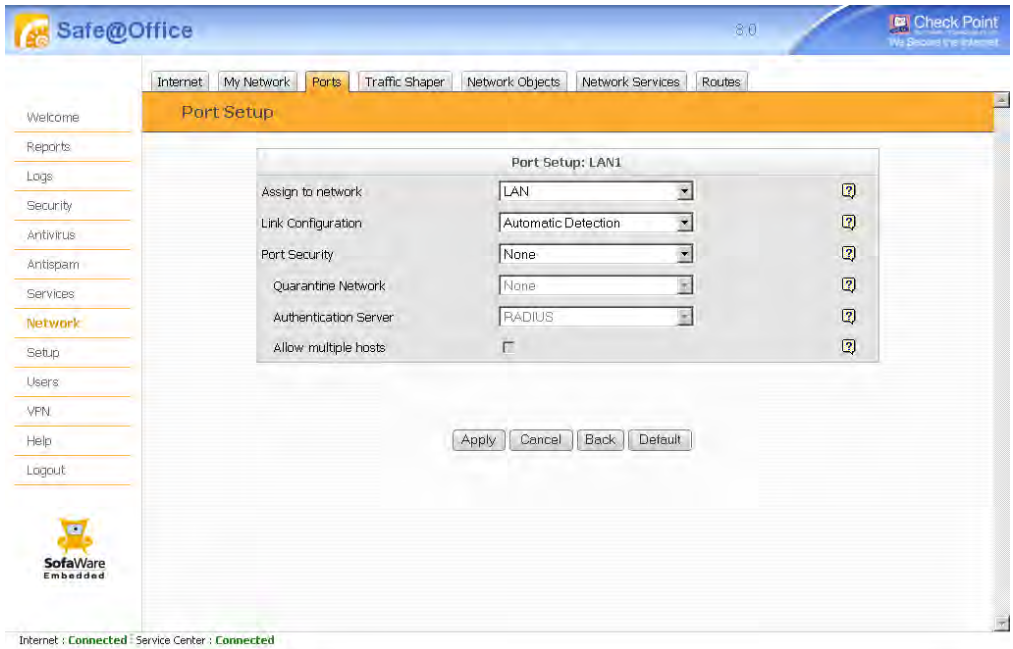
To modify a port assignment

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

   The Ports page appears.

2. Next to the desired port, click Edit.

   The Port Setup page appears.



3. In the Assign to Network drop-down list, do one of the following:

   - To assign a network port to the LAN, select LAN.
   - To configure a network port for use with a WAN Internet connection, select Internet.

- To disable a network port, select None.
- To disable the Serial port, select Disabled.

4. Click Apply.

   A warning message appears.

5. Click OK.

   The port is reassigned to the specified network or purpose.

Modifying Link Configurations

500

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

To modify a port's link configuration

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

   The Ports page appears.

2. Next to the desired port, click Edit.

   The Port Setup page appears.

3. In the Link Configuration drop-down list, 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.

4. Click Apply.

   A warning message appears.

5. Click OK.

   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 following table).

Table 35: Default Port Assignments

Port	Default Assignment
LAN 1-4	LAN
DMZ / WAN2	DMZ
WAN	This port is always assigned to the WAN.
ADSL	This port is always assigned to the WAN.
Serial	Console

Note: Resetting ports to their defaults may result in the loss of your Internet connection. Therefore, it is recommended to be particularly careful when performing this procedure remotely.

Resetting All Ports to Defaults

500

To reset all 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.

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

Resetting Individual Ports to Defaults

500

To reset a port to defaults

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

   The Ports page appears.

2. Next to the desired port, click Edit.

   The Port Setup page appears.

3. Click Default.

   A confirmation message appears.

4. Click OK.

   The port is reset to its default assignment and to "Automatic Detection" link configuration.

Chapter 7

Using Bridges

This chapter describes how to connect multiple network segments at the data-link layer, using a bridge.

This chapter includes the following topics:

Overview

The Safe@Office appliance enables you to connect multiple network segments at the data-link layer, by configuring a bridge. Bridges offer the following advantages:

- Easy network segmentation

  Bridges can be used to compartmentalize an existing network into several security zones, without changing the IP addressing scheme or the routers' configuration.

  Ordinarily, if you need to deploy a firewall within an internal network, you can divide the existing subnet into two networks and configure a new routing scheme. However, in some deployments, the amount of network reconfiguration required prohibits such a solution. Adding a bridge not only allows you to segment your network quickly and easily, but it allows you to choose whether to enable the firewall between network segments.

  If you enable the firewall between bridged network segments, the gateway operates as a regular firewall between network segments, inspecting traffic and dropping or blocking unauthorized or unsafe traffic. In contrast, if you disable the firewall between bridged network segments, all network interfaces assigned to the bridge are connected

directly, with no firewall filtering the traffic between them. The network interfaces operate as if they were connected by a hub or switch.

Figure 19: Bridge with Four VLANs

For example, if you assign the LAN and primary WLAN networks to a bridge and disable the bridge's internal firewall, the two networks will act as a single, seamless network, and only traffic from the LAN and primary WLAN networks to other networks (for example, the Internet) will be inspected by the firewall. If you enable the internal firewall, it will enforce security rules and inspect traffic between the LAN and primary WLAN networks.

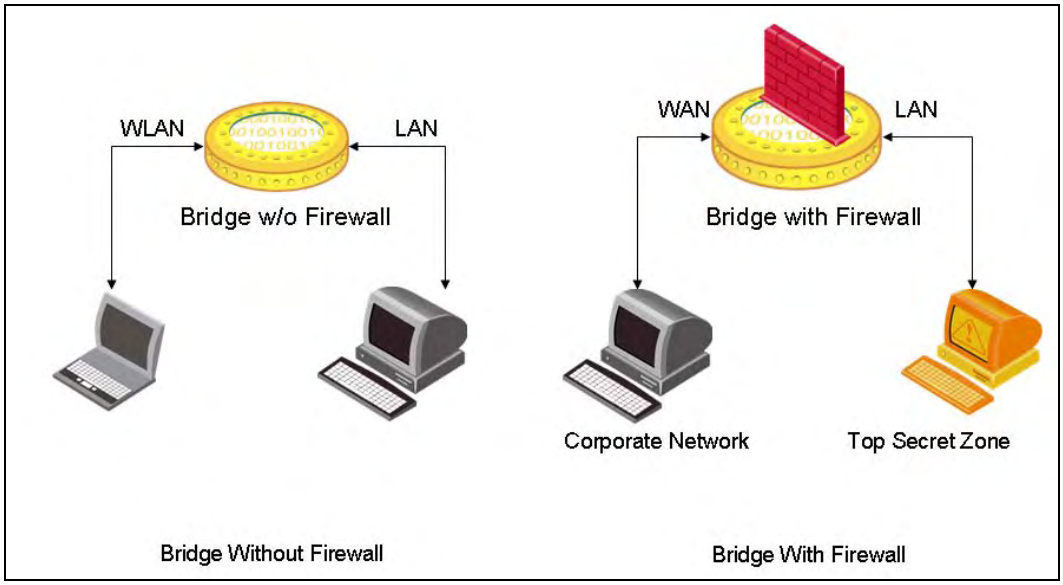


Figure 20: Bridge Firewalling

- Transparent roaming

  In a routed network, if a host is physically moved from one network area to another, then the host must be configured with a new IP address. However, in a bridged network, there is no need to reconfigure the host, and work can continue with minimal interruption.

The Safe@Office appliance allows you to configure anti-spoofing for bridged network segments. When anti-spoofing is configured for a segment, only IP addresses within a specific IP address range can be sent from that network segment. For example, if you configure anti-spoofing for the “Marketing” network segment, the following things happens:

- If a host with an IP address *outside of the allowed IP address range* tries to connect from a port or VLAN that belongs to the “Marketing” network segment, the connection will be blocked and logged as “Spoofed IP”.
- If a host with an IP address within the bridge IP address range tries to connect from a port or VLAN that belongs to a network segment *other than the “Marketing” segment*, the connection will be blocked and logged as “Spoofed IP”.

Note: The following Safe@Office models do not support using bridge mode with port-based VLAN:

- SBX166-LHGE-2
- SBX166-LHGE-3

Note: If the Safe@Office 500 Power Pack upgrade is not installed, you can configure only one bridge.

How Does Bridge Mode Work?

Bridges operate at layer 2 of the OSI model, therefore adding a bridge to an existing network is completely transparent and does not require any changes to the network's structure.

Each bridge maintains a forwarding table, which consists of `<MAC Address, Port>` associations. When a packet is received on one of the bridge ports, the forwarding table is automatically updated to map the source MAC address to the network port from which the packet originated, and the gateway processes the received packet according to the packet's type.

When a bridge receives an IP packet, the gateway processes the packet as follows:

1. The destination MAC address is looked up in the bridge's forwarding table.
2. If the destination MAC address is found in the forwarding table, the packet is forwarded to the corresponding port.
3. If the destination MAC address is not found in the forwarding table, the destination IP address is searched for in all the defined bridge IP address ranges.
4. If the destination IP address is found in the bridge IP address range of exactly one port, the IP address is transmitted to that port.
5. If the IP address is found in the bridge IP address range of more than one port, the packet is dropped. The gateway then sends an ARP query to each of the relevant ports.
6. If a host responds to the ARP request packet with an ARP reply, the forwarding table is updated with the correct `<MAC Address, Port>` association. Subsequent packets will be forwarded using the forwarding table.

If a bridge receives a non-IP packet, and the bridge is configured to forward non-IP protocol Layer-2 traffic, the gateway processes the packet as follows:

1. The destination MAC address is looked up in the bridge's forwarding table.
2. If the destination MAC address is found in the forwarding table, the packet is forwarded to the corresponding port.
3. If the destination MAC address is not found in the forwarding table, the packet is flooded to all the ports on the bridge.

Multiple Bridges and Spanning Tree Protocol

When using multiple bridges, you can enable fault tolerance and optimal packet routing, by configuring Spanning Tree Protocol (STP - IEEE 802.1d). When STP is enabled, each bridge communicates with its neighboring bridges or switches to discover how they are interconnected. This information is then used to eliminate loops, while providing optimal routing of packets. STP also uses this information to provide fault tolerance, by re-computing the topology in the event that a bridge or a network link fails.

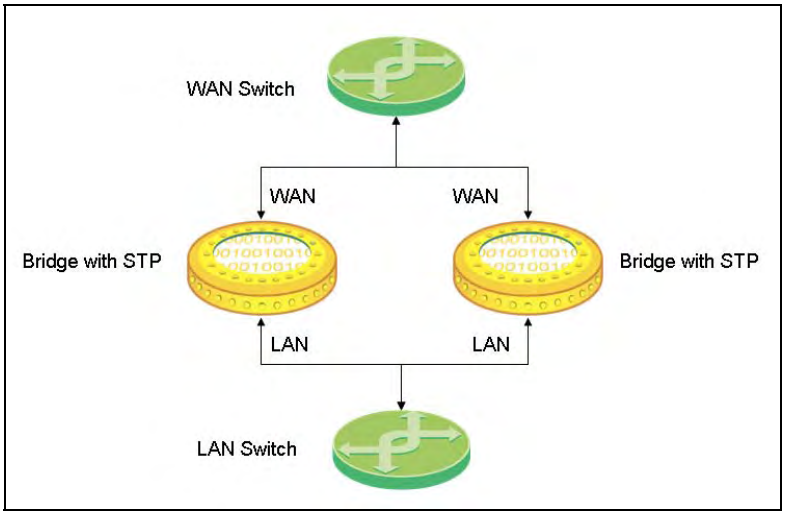


Figure 21: Dual Redundant Bridges with STP

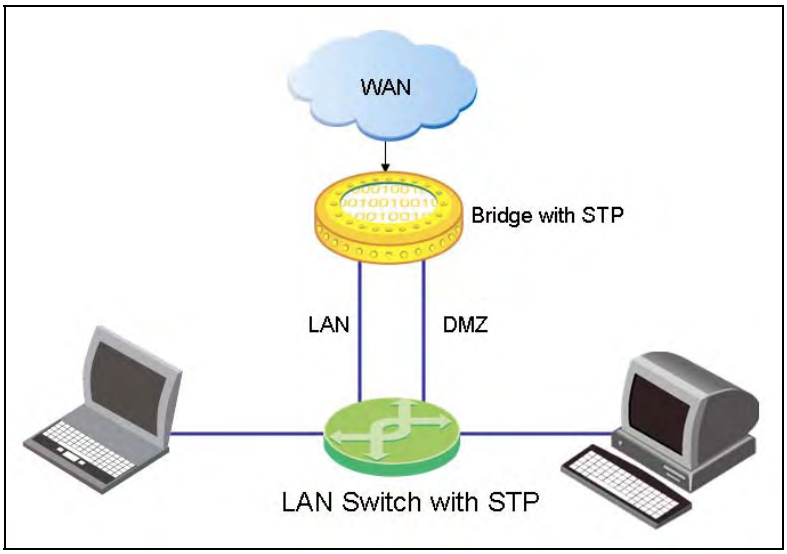


Figure 22: Link Redundancy with STP

Workflow

500

To use a bridge

1. Add a bridge.

   See ***Adding and Editing Bridges*** on page 224.

2. Add the desired internal networks to the bridge.

   See ***Adding Internal Networks to Bridges*** on page 228.

3. Add the desired Internet connections to the bridge.

   See ***Adding Internet Connections to Bridges*** on page 233.

4. If you enabled the firewall between networks on this bridge, add security rules and VStream Antivirus rules as needed.

For information on adding security rules, see ***Adding and Editing Rules*** on page 364. For information on adding VStream Antivirus rules, see ***Adding and Editing Vstream Antivirus Rules*** on page 473.

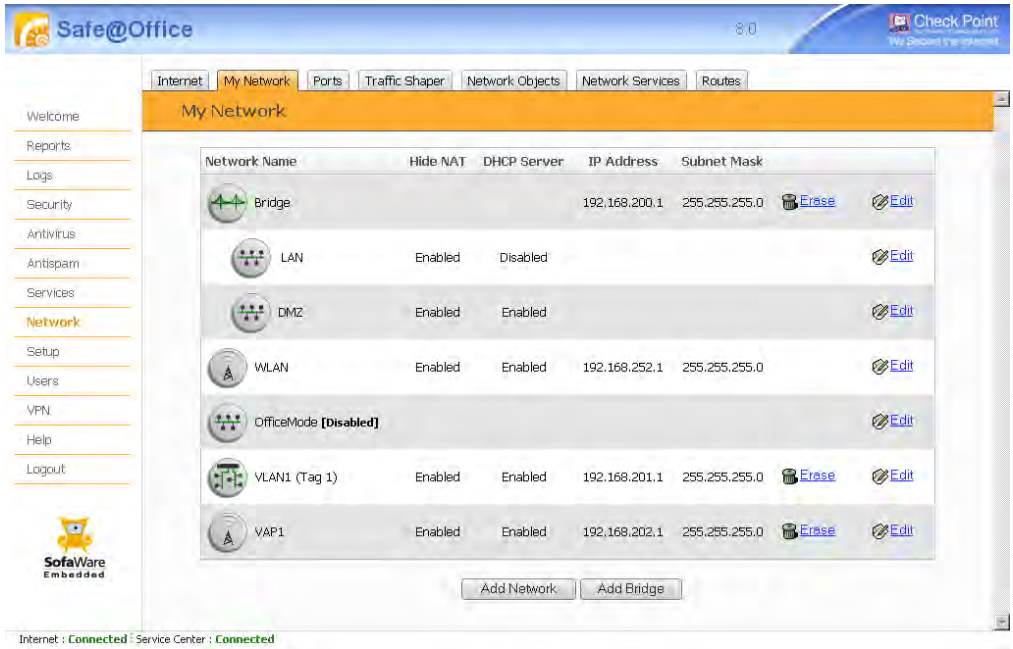
Adding and Editing Bridges

500

To add or edit a bridge

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

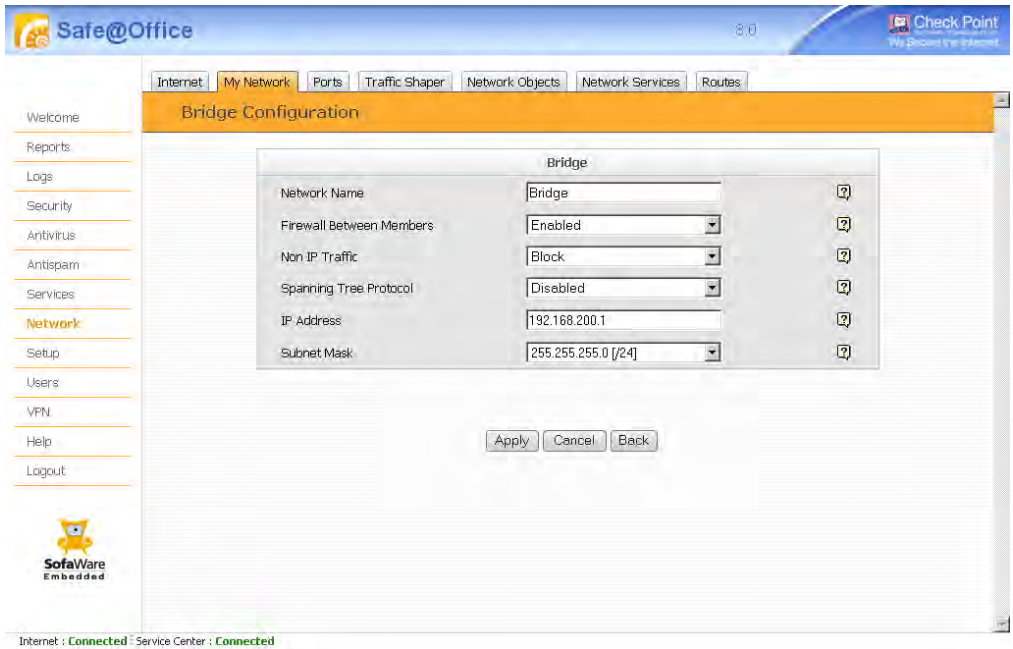
   The My Network page appears.



2. Do one of the following:

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

The **Bridge Configuration** page appears.



3. Complete the fields using the following table.
4. Click **Apply**.

   A success message appears.

Table 36: Bridge Configuration Fields

In this field…	Do this…
Network Name	Type a name for the bridge.
Firewall Between Members	Specify whether the firewall should be enabled between networks on this bridge, by selecting one of the following: • Enabled. The firewall is enabled, and it will inspect traffic between networks on the bridge, enforcing firewall rules and SmartDefense protections. This is the default value. • Disabled. The firewall is disabled between networks on the bridge.
Non IP Traffic	Specify how the firewall should handle non-IP protocol traffic between networks on this bridge, by selecting one of the following: • Block. The firewall will block all non-IP protocol traffic on the bridge. This is the default value. • Pass. The firewall will allow all non-IP protocol traffic on the bridge and process it as described in ***Using Bridges*** on page 217.
Spanning Tree Protocol	Specify whether to enable STP for this bridge, by selecting one of the following: • Enabled. STP is enabled. • Disabled. STP is disabled. This is the default value. If you selected Enabled, the Bridge Priority field appears.

In this field…	Do this…
Bridge Priority	Select this bridge's priority. The bridge's priority is combined with a bridged network's MAC address to create the bridge's ID. The bridge with the lowest ID is elected as the root bridge. The other bridges in the tree calculate the shortest distance to the root bridge, in order to eliminate loops in the topology and provide fault tolerance. To increase the chance of this bridge being elected as the root bridge, select a lower priority. Note: If you select the same priority for all bridges, the root bridge will be elected based on MAC address. The default value is 32768. This field only appears if STP is enabled.
IP Address	Type the IP address to use for this gateway on this bridge. Note: The bridge must not overlap other networks.
Subnet Mask	Select this bridge's subnet mask.

Adding Internal Networks to Bridges

500

Note: In order to add a VLAN of any type (port-based, tag-based, VAP, or WDS link) to the bridge, you must first create the desired VLAN.

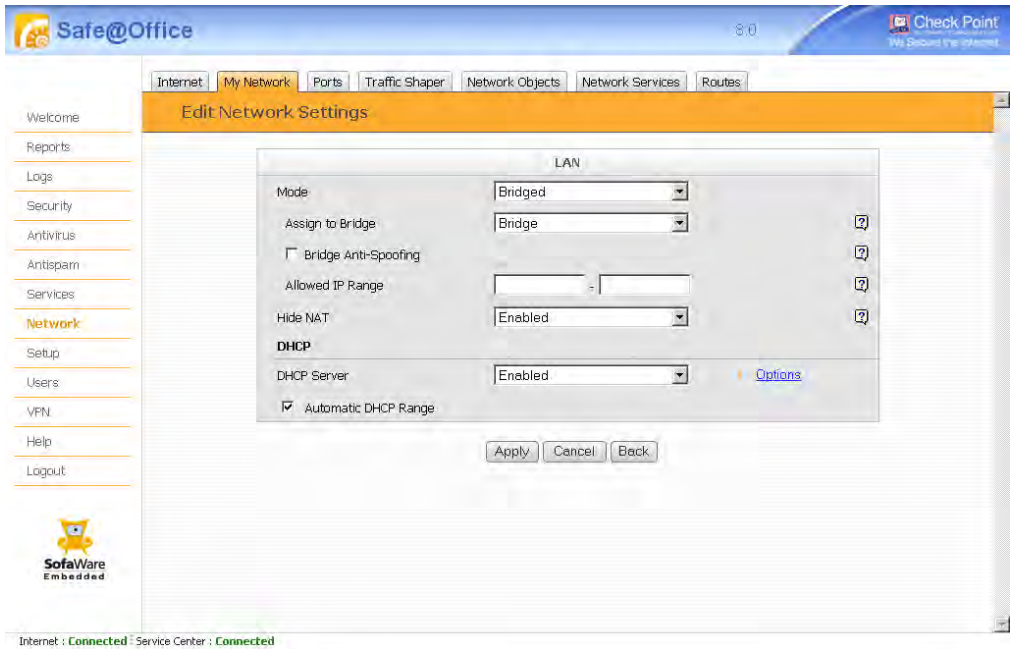
For information on adding port-based VLANs, see ***Adding and Editing Port-Based VLANs*** on page 178. For information on adding tag-based VLANs, see ***Adding and Editing Tag-Based VLANs*** on page 180.For information on adding VAPs, see ***Configuring Virtual Access Points*** on page 294. For information on adding WDS links, see ***Configuring WDS Links*** on page 298.

To add an internal network to a bridge

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

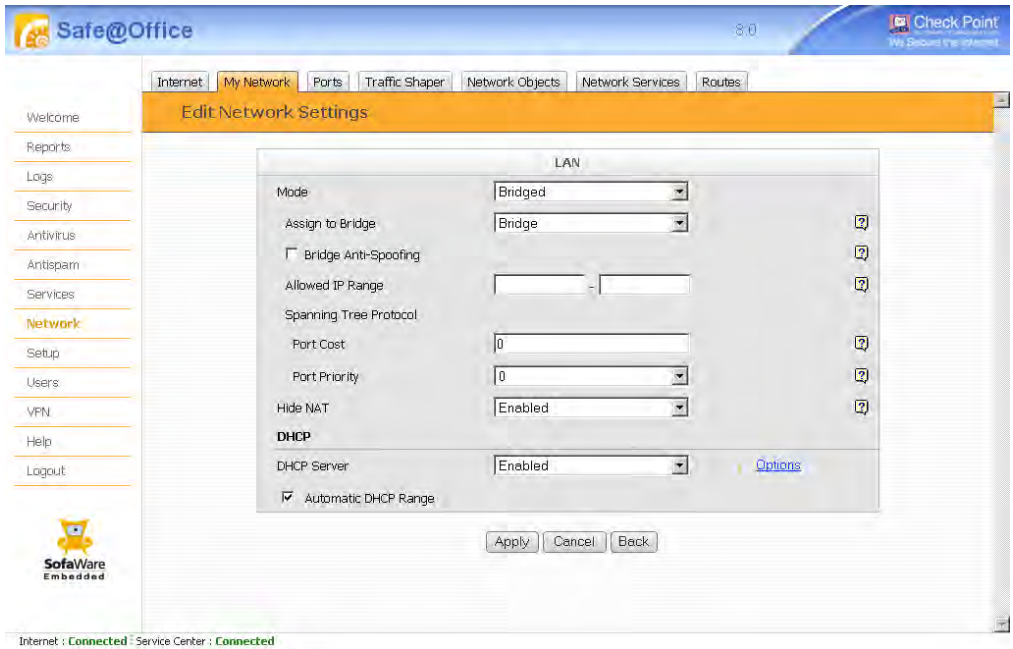
   The My Network page appears.
2. Click Edit in the desired network's row.
3. In the Mode drop-down list, select Bridged.

New fields appear.



4. Complete these fields as described below.

If the assigned bridge uses STP, additional fields appear.



5. Click **Apply**.

   A warning message appears.

6. Click **OK**.

   A success message appears.

   In the **My Network** page, the internal network appears indented under the bridge.

Table 37: Bridged Network Fields

In this field...	Do this...
Assign to Bridge	Select the bridge to which the connection should be assigned.
Bridge Anti-Spoofing	Select this option to enable anti-spoofing. If anti-spoofing is enabled, only IP addresses within the Allowed IP Range can be source IP addresses for packets on this network.
Allowed IP Range	Type the range of IP addresses that should be allowed on this network. Note: When assigning IP addresses to machines in a bridged network segment, the Safe@Office DHCP server allocates only addresses within the allowed IP address range. To enable clients to move between bridged networks without changing IP addresses, configure identical IP address ranges for the desired networks, thus allowing the IP addresses to be used on either of the bridged networks. Note: Configuring overlapping or identical allowed IP address ranges will decrease the effectiveness of anti-spoofing between the bridged networks.
Spanning Tree Protocol - Port Cost	Type the port's cost. STP uses the available port with the lowest cost to forward frames to the root port. All other ports are blocked. It is recommended to set a lower value for faster links. This field only appears if the bridge uses STP.

In this field...	Do this...
Spanning Tree Protocol - Port Priority	Select the port's priority. The port's priority is combined with the port's logical number to create the port's ID. The port with the lowest ID is elected as the root port, which forwards frames out of the bridge. The other ports in the bridge calculate the least-cost path to the root port, in order to eliminate loops in the topology and provide fault tolerance. To increase the chance of this port being elected as the root port, select a lower priority. Note: If you select the same priority for all ports, the root port will be elected based on the port's logical number. The default value is 128. This field only appears if the bridge uses STP.

Adding Internet Connections to Bridges

500

To add an Internet connection to a bridge

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

   The Internet page appears.

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

   The Internet Setup page appears.

3. In the Port drop-down list, specify the port that the Internet connection should use, by doing one of the following:

   - To use the ADSL port, select ADSL.

     This option is available in ADSL models only.

   - To use the WAN port, select WAN.

     This option is available in non-ADSL models only.

   - To use the DMZ/WAN2 port, select WAN2.

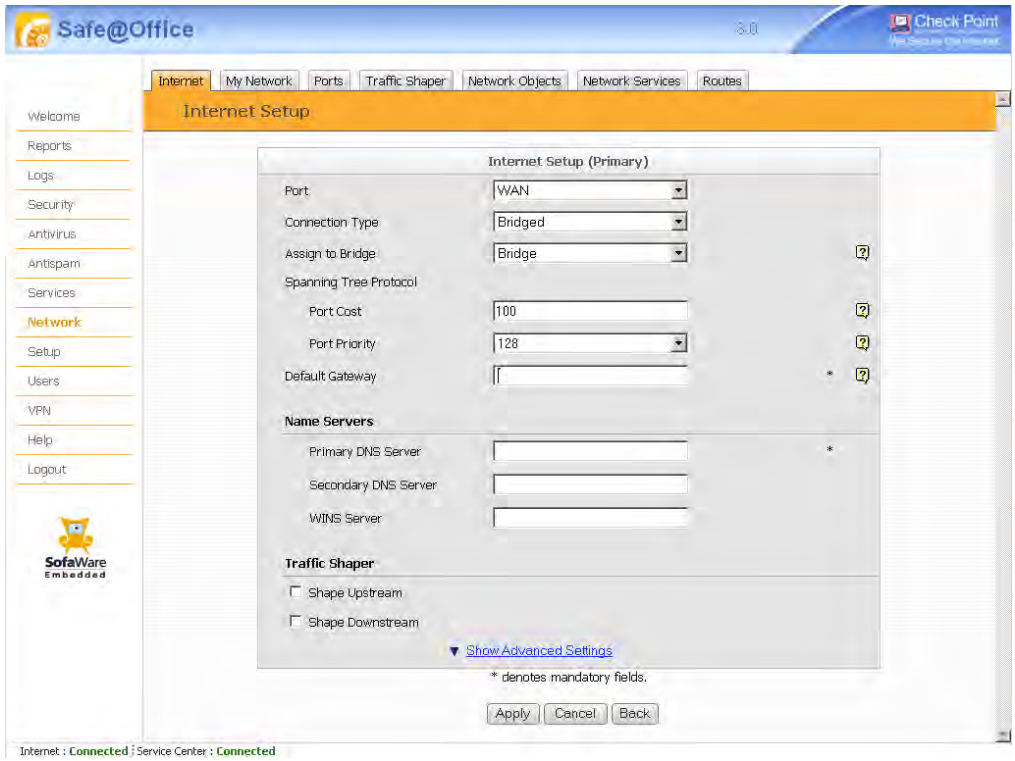
4. Do one of the following:

   - To configure a Bridged PPPoA connection, in the Connection Type field, select PPPoA.

     This option is available in ADSL models only.

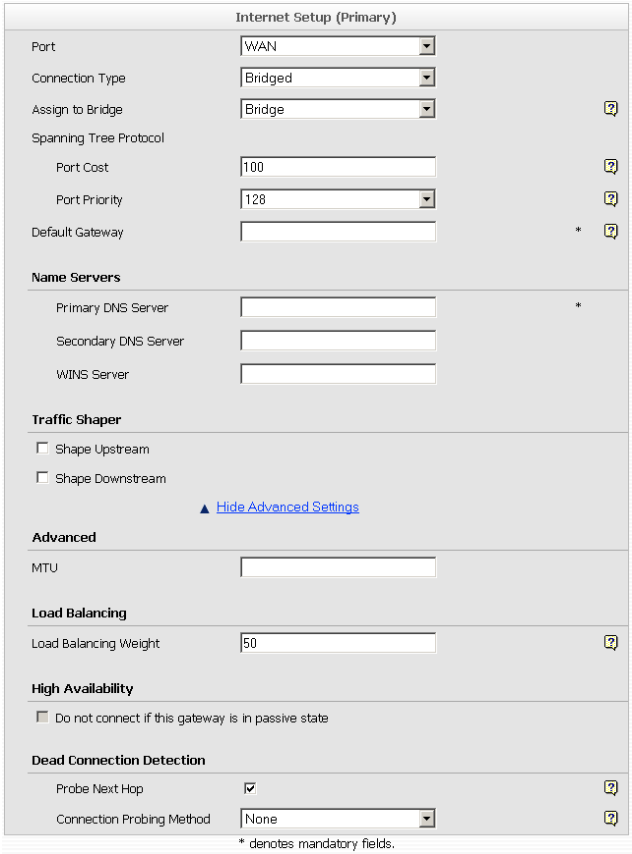
   - Otherwise, in the Connection Type field, select Bridged.

New fields appear.



5. Complete the fields specified in the table below.
6. Complete the rest of the fields using the relevant information in ***Internet Setup Fields*** on page 127.

New fields appear, depending on the selected options, and whether the selected bridge uses STP.



7. 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”.

Table 38: Bridged Connection Fields

In this field…	Do this…
Bridge Mode	Select this option to configure a Bridged PPPoA connection. The **Bridge To** field appears. This field is relevant for Bridged PPPoA connections only.
Bridge To	Select the bridge to which you want to add the PPPoA connection. This field is relevant for Bridged PPPoA connections only.
Assign to Bridge	Select the bridge to which the connection should be assigned. This field is relevant for regular bridged connections only.
Spanning Tree Protocol - Port Cost	Type the port's cost. STP uses the available port with the lowest cost to forward frames to the root port. All other ports are blocked. It is recommended to set a lower value for faster links. This field only appears if the selected bridge uses STP. It is relevant for regular bridged connections only.

In this field...	Do this...
Spanning Tree Protocol - Port Priority	Select the port's priority. The port's priority is combined with the port's logical number to create the port's ID. The port with the lowest ID is elected as the root port, which forwards frames out of the bridge. The other ports in the bridge calculate the least-cost path to the root port, in order to eliminate loops in the topology and provide fault tolerance. To increase the chance of this port being elected as the root port, select a lower priority. Note: If you select the same priority for all ports, the root port will be elected based on the port's logical number. The default value is 128. This field only appears if the selected bridge uses STP. It is relevant for regular bridged connections only.

Deleting Bridges

500

To delete a bridge

1. Remove all internal networks from the bridge, by doing the following for each network:
   a. Click Network in the main menu, and click the My Network tab.

      The My Network page appears.
   b. Click Edit in the desired network's row.
   c. In the Mode drop-down list, select Enabled.
   d. Click Apply.
2. Remove all Internet connections from the bridge, by doing the following for each connection:
   a. Click Network in the main menu, and click the Internet tab.

      The Internet page appears.
   b. Next to the desired Internet connection, click Edit.
   c. The Internet Setup page appears.
   d. In the Connection Type field, select the desired connection type (not Bridged).
   e. Click Apply.
3. Click Network in the main menu, and click the My Network tab.

   The My Network page appears.
4. In the desired bridge’s row, click Erase.

   A confirmation message appears.
5. Click OK.

   The bridge is deleted.

Chapter 8

Configuring High Availability

This chapter describes how to configure High Availability (HA) for two or more Safe@Office appliances.

This chapter includes the following topics:

Overview

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 or bridge existing on both gateways, except the WAN interface and the primary 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 appliances 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.

On the other hand, you might prefer to keep Passive Gateways connected to the Internet at all times, so that they can download updates from the Service Center and be accessible for remote management, even when not acting as the Active Gateway. In this case, you must assign a virtual IP address to the WAN interface. Each Passive Gateway will remain constantly connected to the Internet using its WAN interface's primary IP address, while remaining on standby to take over the WAN virtual IP address, in the event that the Active Gateway fails. If desired, you can configure a WAN virtual IP address for the WAN2 interface, as well.

Note: To use a WAN virtual IP address, the Internet connection method must be "Static IP". PPP-based connections and dynamic IP connections are not supported.

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 and bridges 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 or bridge.

You can configure HA for the WAN interface, for any bridge, and for any internal network except wireless networks and 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 primary WLAN network:

- A passive appliance's wireless transmitter will be disabled until the gateway becomes active.
- The two primary WLAN networks can share the same SSID and wireless frequency.
- Wireless interfaces 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.

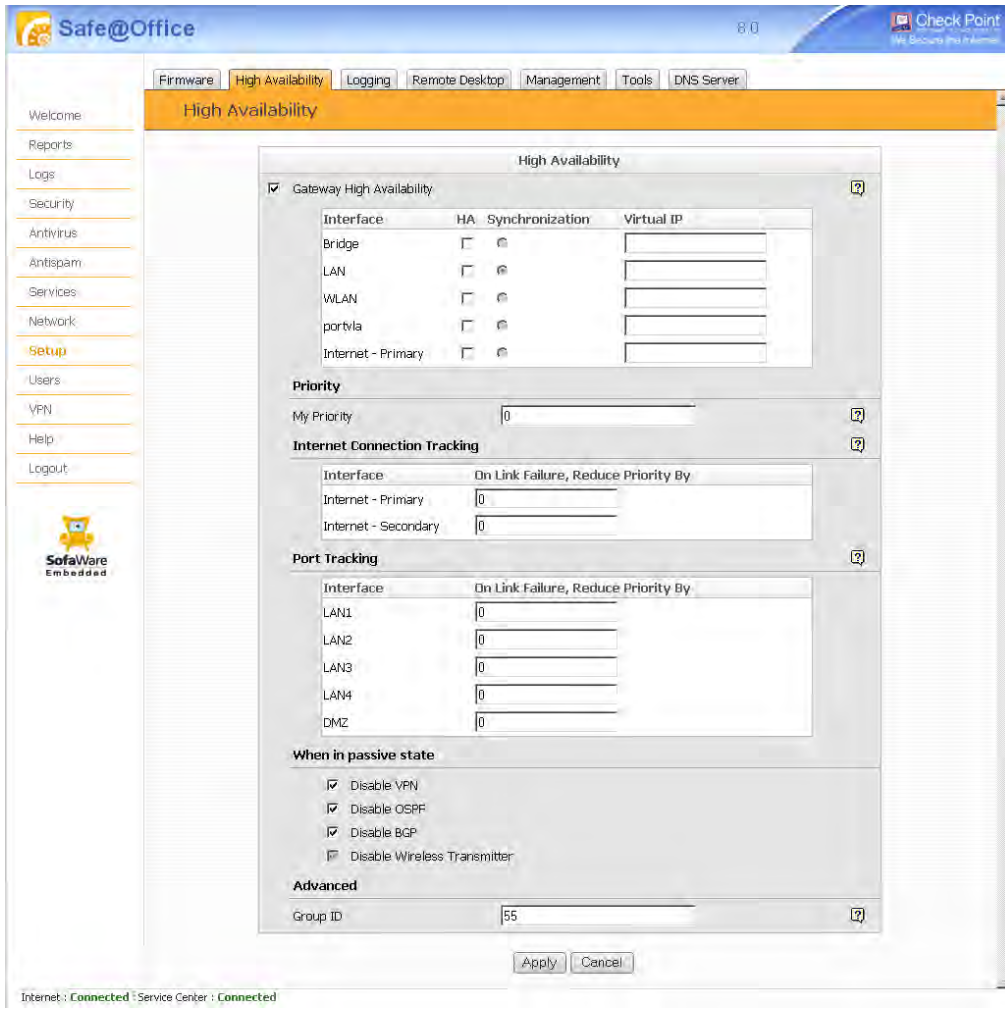
   See ***Changing IP Addresses*** on page 156.

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.

   The Internet-Primary field represents the WAN interface, and the Internet-Secondary field represents the WAN2 interface.

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.

You can assign a virtual IP address to any internal interface, as well as to "LAN Static IP" Internet connections (that is, LAN connections for which the Obtain IP address automatically (using DHCP) check box is cleared).

6. Click the Synchronization radio button next to the network you want to use as the synchronization interface.

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.

The synchronization interface cannot be an Internet connection or a wireless interface.

7. Complete the fields using the information the following table.
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 the Do not connect if this gateway is in passive state field in ***Using Internet Setup*** on page 102.
10. If you configured a virtual IP address for the WAN or WAN2 interface, configure the Internet connection to use the "Static IP" connection method.

    See ***Using Internet Setup*** on page 102.

Table 39: 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.
Internet Connection 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.
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 149.
Port Tracking	
LAN1-4	Type the amount to reduce the gateway's priority if the LAN port's Ethernet link is lost. This must be an integer between 0 and 255.

In this field...	Do this...
DMZ	Type the amount to reduce the gateway's priority if the DMZ / WAN2 port's Ethernet link is lost. This must be an integer between 0 and 255.
When in passive state	
Disable VPN	Select this option to specify that VPN connectivity should be disabled when the gateway is a Passive Gateway.
Disable OSPF	Select this option to specify that Open Shortest Path First (OSPF) dynamic routing should be disabled when the gateway is a Passive Gateway.
Disable BGP	Select this option to specify that Border Gateway Protocol (BGP) dynamic routing should be disabled when the gateway is a Passive Gateway.
Disable Wireless Transmitter	Indicates that the appliance's wireless transmitter will be disabled when the gateway is a Passive Gateway. This option only appears for wireless appliances, and it cannot be cleared.
Advanced	Select this option to specify that VPN connectivity should be disabled when the gateway is a Passive Gateway.
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 40: 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 156.

   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 156.

   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.

Chapter 9

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 desired wireless network. See ***Manually Configuring a Wireless Network*** on page 280.

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 102.

   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 256.

   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 364.

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 360.

Table 41: 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. Note that the weight (amount of bandwidth) allocated to this class is less than the weight allocated to the “Important” class. The "Urgent" class is ideal for delay-sensitive traffic that does not demand a high amount of bandwidth.
Important	20	Medium (Normal Traffic)	Important traffic that requires a high allocation of bandwidth, but which is not exceptionally sensitive to delays. For example, you can prioritize the HTTP traffic of a company's executive officers over other types of traffic, by assigning it to the “Important” class.
Low Priority	5	Low (Bulk Traffic)	Traffic that is not sensitive to long delays, and which does not require a high guaranteed bandwidth. For example, SMTP traffic (outgoing email).

Note: In Simplified Traffic Shaper, these classes cannot be changed.

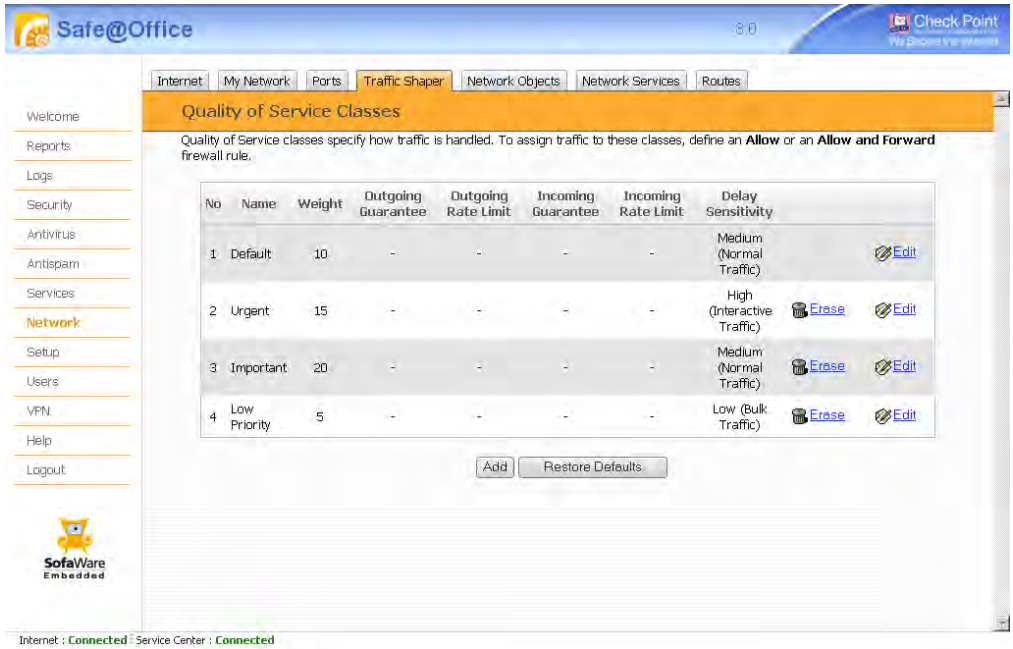
Adding and Editing Classes

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 following table.
4. Click **Next**.

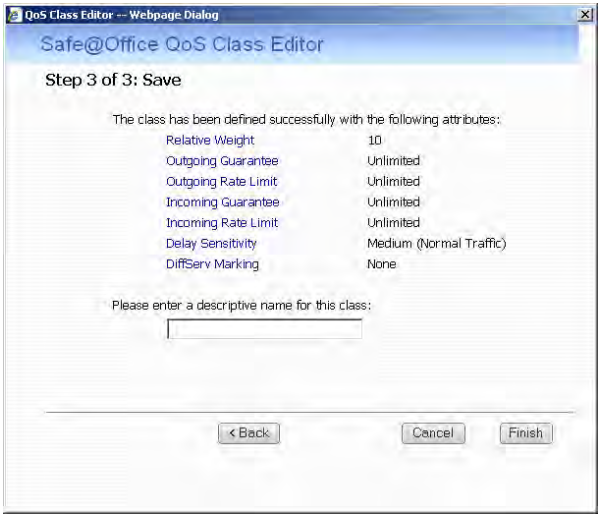
   The **Step 2 of 3: Advanced Options** dialog box appears.

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

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 102.

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 42: 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.

Viewing and 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 view or 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 with a list of all defined QoS classes.
2. To delete a QoS class, do the following:

   a. In the desired class's row, click Erase.

      A confirmation message appears.

   b. 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 254.

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 10

Working with Wireless Networks

This chapter describes how to configure wireless internal networks.

This chapter includes the following topics:

Overview

500W

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

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

Safe@Office wireless appliances transmit in 2.4GHz range, using dual diversity antennas to increase the range. In addition, Safe@Office appliances support 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 105 dBm, 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).

The Primary WLAN

500W

In addition to the LAN and DMZ networks, you can define a wireless internal network called the primary WLAN (wireless LAN) network. The primary WLAN is the main wireless network, and it controls all other wireless network's statuses: wireless networks can be enabled only if the primary WLAN is enabled, and disabling the primary WLAN automatically disables all other wireless network. In addition, all wireless networks inherit certain settings from the primary WLAN.

You can configure the primary WLAN in either of the following ways:

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

  See ***Using the Wireless Configuration Wizard*** on page 273.

- Manual configuration. Offers advanced setup options for the primary WLAN.

  See ***Manually Configuring a WLAN*** on page 280.

Note: If the Safe@Office 500 Power Pack upgrade is not installed, the primary WLAN is the only wireless network.

Virtual Access Points

500W | Power Pack

The Safe@Office appliance enables you to partition the primary WLAN into virtual access points (VAPs). A VAP is a logical wireless network behind the Safe@Office appliance and is a type of VLAN (see ***Configuring VLANs*** on page 174). Like other types of VLANs, VAPs are isolated from each other and can have separate security policies, IP network segments, and Traffic Shaper settings. This enables you to configure separate policies for different groups of wireless users.

For example, you could assign different permissions to employees and guests using your company's wireless network, by defining two VAPs called “Guest” and “Employee”. The Guest VAP would use simple WPA-Personal encryption, and the security policy would mandate that stations connected to this network can access the Internet, but not sensitive

company resources. You could configure Traffic Shaper bandwidth management to give stations in the Guest network a low priority, and by enabling Secure HotSpot on this network, you could define terms of use that the guest users must accept before accessing the Internet. In contrast, the Employee VAP would use the more secure WPA2-Enterprise (802.11i) encryption standard and allow employees to access company resources such as the intranet.

You can configure up to three VAPs, in addition to the primary WLAN. For information on configuring VAPs, see ***Configuring VAPs*** on page 294.

Wireless Distribution System Links

500W | Power Pack

The Safe@Office appliance enables you to extend the primary WLAN's coverage area, by creating a Wireless Distribution System (WDS). A WDS is a system of access points that communicate with each other wirelessly via WDS links, without any need for a wired backbone. For example, if your business has expanded across two buildings, and a single access point no longer provides sufficient coverage, you can add another access point that acts as a repeater. If it is impractical or costly to run wires between the access points, you can connect them by configuring a WDS that includes both access points.

WDS is usually used together with bridge mode to connect the networks behind the access points. For example, if you have two network segments, each of which is served by a different access point, you can bridge the two network segments over WDS links. The network segments will communicate with each other wirelessly via their access points and act as a single network. For information on bridge mode, see ***Using Bridges*** on page 217.

WDS links are considered a type of VLAN (see ***Configuring VLANs*** on page 174). Therefore, they can have separate security policies, IP network segments, and Traffic Shaper settings.

You can use WDS links to create loop-free topologies, such as a star or tree of access points.

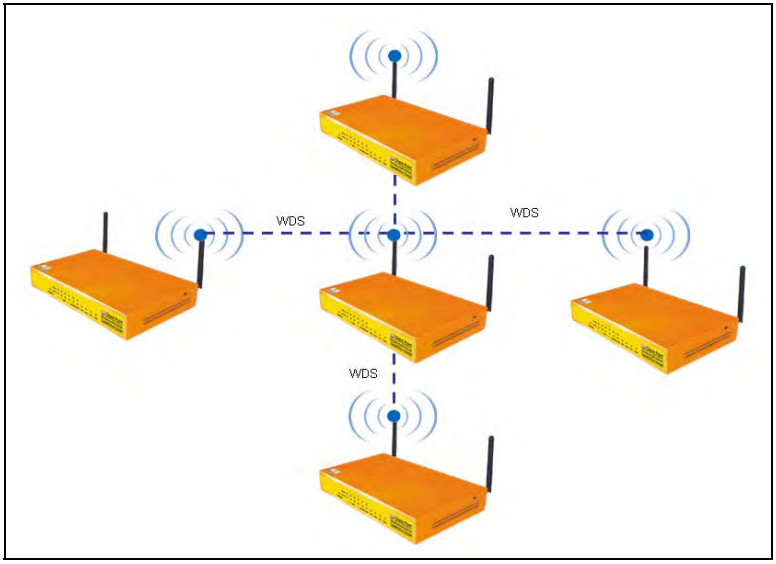


Figure 23: WDS Star of Wireless Access Points

When used together with bridge mode and Spanning Tree Protocol (STP), you can use WDS links to create redundant topologies, such as a loop or mesh of linked access points.

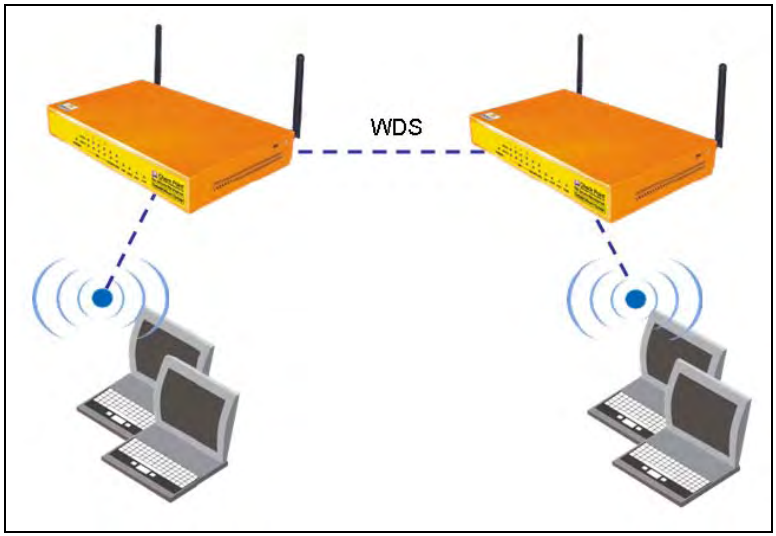


Figure 24: Two Access Points Linked by a WDS Bridge

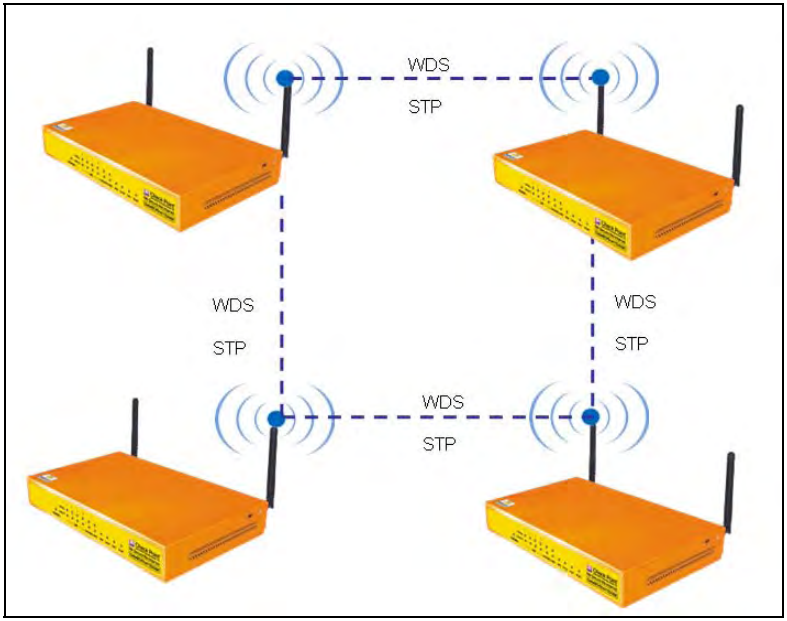


Figure 25: Redundant Loop of Access Points Linked by WDS and STP

You can configure up to seven WDS links, in addition to the primary WLAN. For information on configuring WDS links, see ***Configuring WDS Links*** on page 298.

Note: All access points in a WDS must use the same radio channel for the WDS link and for communicating with wireless stations. Therefore, using WDS may have a negative impact on wireless throughput. In this case, it is recommended to use a traditional wired backbone to connect the access points, instead of WDS links.

Network Count Limitations

500W | Power Pack

You can configure a total of eight wireless objects, including any combination of the following:

- The primary WLAN
- Up to three virtual access points (VAPs)
- Up to seven WDS links

For example, if you configure the primary WLAN and two VAPs, then you can configure five WDS links, or one more VAP and four WDS links.

When Extended Range (XR) mode is enabled for a wireless object, then it is counted as two objects. For example, if you configure XR mode for the primary WLAN and one VAP, they are counted as four wireless objects.

For information on default security policy rules controlling traffic to and from the primary WLAN and VAPs, see ***Default Security Policy*** on page 353.

Wireless Security Protocols

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

Table 43: 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 wireless network, although you can still limit access from the wireless network by creating firewall rules. This method is suitable for creating public access points.

Security Protocol	Description
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, either by a RADIUS server (authentication server) which supports 802.1x, or by the Safe@Office appliance's built-in EAP authenticator. 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. This security method is not supported for WDS links. Note: To use this security method, you must first configure either a RADIUS server that supports 802.1x, or set up the network for use with the Safe@Office EAP authenticator. For information on configuring a RADIUS server, see ***Using RADIUS Authentication.*** on page 650 For information on using the Safe@Office EAP authenticator, see ***Using the Safe@Office EAP Authenticator*** on page 394.

Security Protocol	Description
WPA-Enterprise: RADIUS authentication, encryption	The WPA-Enterprise (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-Enterprise includes 802.1x and EAP authentication, based either on a central RADIUS authentication server, or on the Safe@Office appliance's built-in EAP authenticator. This method is recommended for situations where you want to authenticate wireless stations, and to encrypt the transmitted data. Note: To use this security method, you must first configure either a RADIUS server that supports 802.1x, or set up the network for use with the Safe@Office EAP authenticator. For information on configuring a RADIUS server, see ***Using RADIUS Authentication.*** on page 650 For information on using the Safe@Office EAP authenticator, see ***Using the Safe@Office EAP Authenticator*** on page 394.
WPA-Personal: password authentication, encryption	The WPA-Personal security method (also called WPA-PSK) is a variation of WPA-Enterprise that does not require an authentication server. WPA-Personal 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 or use the Safe@Office EAP authenticator. This security method is not supported for WDS links. Note: The appliance and the wireless stations must be configured with the same passphrase.

Security Protocol	Description
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-Enterprise or WPA-Personal security methods, the Safe@Office appliance enables you to restrict access to the wireless 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. This security method is not supported for WDS links.

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/SecureClient on each computer in the wireless network. This ensures that all connections from the wireless network to the LAN are encrypted and authenticated. For information, see ***Internal VPN Server*** on page 566 and ***Setting Up Your Safe@Office Appliance as a VPN Server*** on page 567.

Configuring Wireless Networks

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

Using the Wireless Configuration Wizard

500W

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

Note: You cannot configure WPA-Enterprise and 802.1x using this wizard. For information on configuring these modes, see ***Manually Configuring a Wireless Network*** on page 280.

To configure a WLAN using the Wireless Configuration Wizard

1. Prepare the appliance for a wireless connection as described in ***Preparing the Appliance for a Wireless Connection*** on page 62.
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 primary WLAN.

   The fields are enabled.

6. Complete the fields using the information in ***Basic WLAN Settings Fields*** on page 284.

7. Click **Next**.

8. The Wireless Security dialog box appears.

9. Do one of the following:

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

     WPA-Personal (also called WPA-PSK) uses a passphrase for authentication. This method is recommended for small, private wireless networks, which want to authenticate and encrypt wireless data, but do not want to install a RADIUS server or use the Safe@Office EAP authenticator. Both WPA and the newer, more secure WPA2 (802.11i) will be accepted. To allow only the more secure WPA2 and not WPA, see ***Manually Configuring a WLAN*** on page 280. For larger wireless networks with many users, configure the primary WLAN to use WPA-Enterprise, using the procedure ***Manually Configuring a WLAN*** on page 280.

   - 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.

10. Do one of the following:

- To bridge the LAN and WLAN networks so that they appear as a single unified network, click Bridge Mode.

  Traffic from the WLAN to the LAN will be allowed to pass freely, and the LAN and WLAN will share a single IP address range.

Note: This option creates a bridge called "default-bridge", which includes the WLAN and the LAN. If desired, you can later remove this bridge by running the Wireless Configuration Wizard again, and choosing Firewall Mode. For information on bridges, see ***Using Bridges*** on page 217.

- To isolate the LAN from the WLAN, click Firewall Mode.

  The WLAN and LAN will be assigned separate, isolated IP networks, and traffic from the WLAN to the LAN will be subjected to the defined firewall policy.

  By default, traffic from the WLAN to the LAN will be blocked, and traffic from the LAN to the WLAN will be allowed. To allow traffic from the WLAN to the LAN, you must create firewall rules. For information, see Using Firewall Rules.

11. Click Next.

WPA-Personal

If you chose WPA-Personal, the Wireless Configuration-WPA-Personal 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.

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.

No Security

The Wireless Security Complete dialog box appears.

- Click Finish.

  The wizard closes.

Manually Configuring a Wireless Network

500W

To manually configure a wireless network

1. If you intend to use the 802.1x or WPA-Enterprise security mode for the wireless network, do one of the following:

   - To use the Safe@Office EAP authenticator for authenticating wireless clients, follow the workflow ***Using the Safe@Office EAP Authenticator for Authentication of Wireless Clients*** on page 395.

     You will be referred back to this procedure at the appropriate stage in the workflow, at which point you can continue from the next step.

   - To use a RADIUS server for authenticating wireless clients, configure a RADIUS server.

     See ***Using RADIUS Authentication*** on page 650.

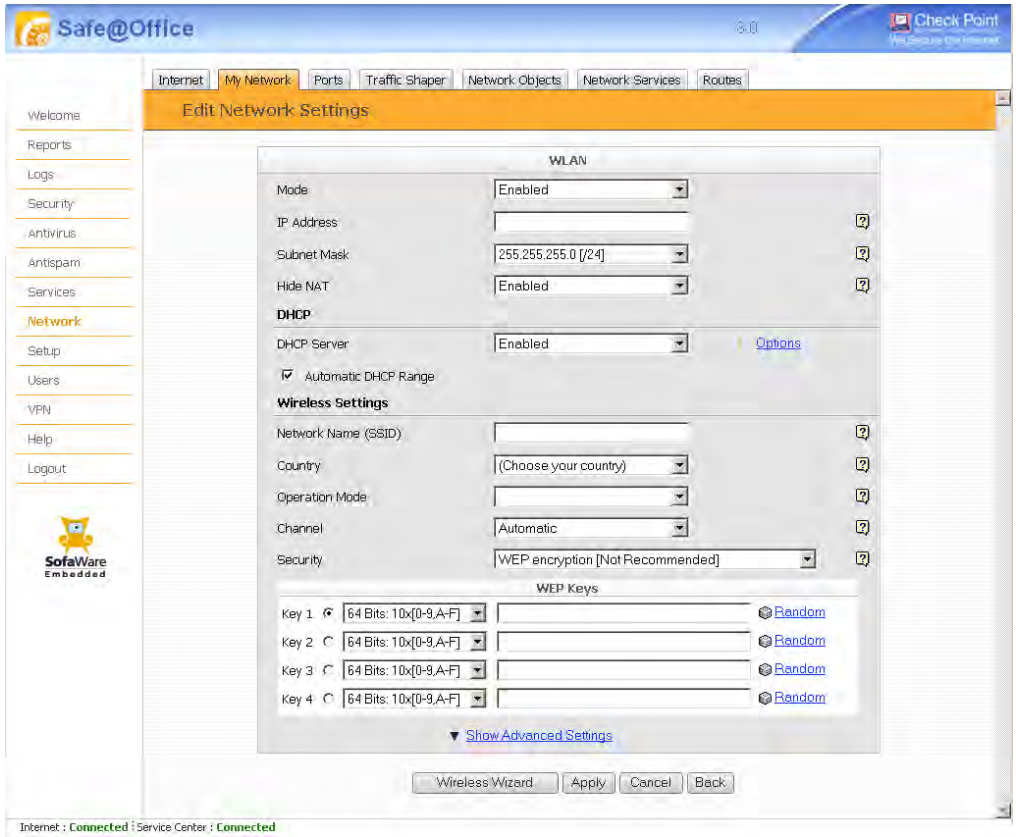
2. Prepare the appliance for a wireless connection as described in ***Preparing the Appliance for a Wireless Connection*** on page 62.

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

   The My Network page appears.

4. In the desired wireless 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. In the **IP Address** field, type the IP address of the wireless network network's default gateway.

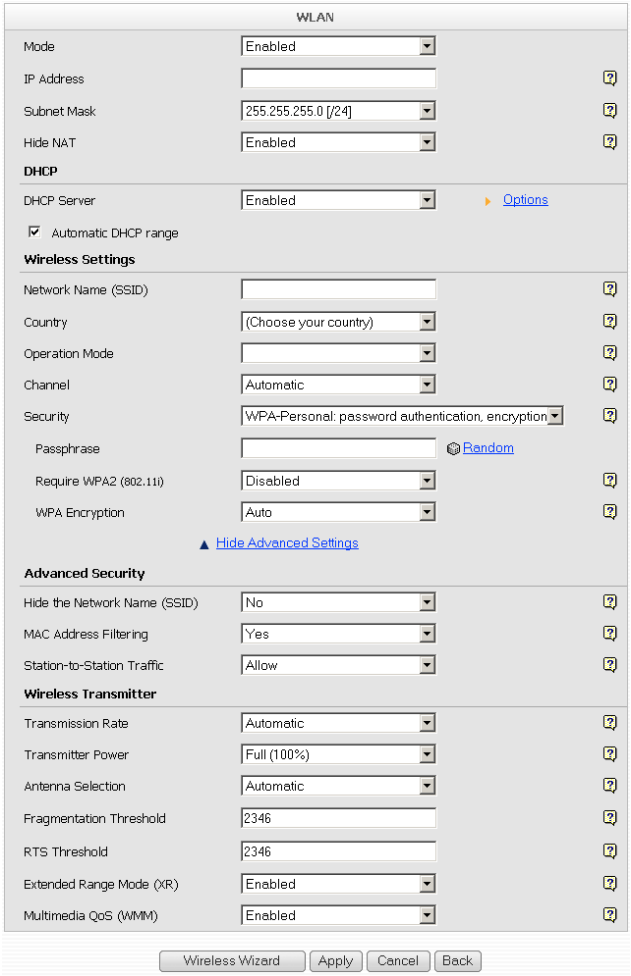
   The wireless network must not overlap other networks.

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

   See ***Enabling/Disabling Hide NAT*** on page 157.
9. If desired, configure a DHCP server.

   See ***Configuring a DHCP Server*** on page 158.
10. Complete the fields using the information in ***Basic Wireless Settings Fields*** on page 284.
11. To configure advanced settings, click Show Advanced Settings and complete the fields using the information in ***Advanced Wireless Settings Fields*** on page 290.

New fields appear.



12. Click **Apply**.

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

13. Click **OK**.

    A success message appears.

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

Table 44: Basic Wireless Settings Fields

In this field…	Do this…
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. This field only appears when configuring the primary WLAN, and it is inherited by all VAPs and WDS links.

In this field…	Do this…
Operation Mode	Select an operation mode: • 802.11b (11 Mbps). 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 (54/108 Mbps). Operates in the 2.4 GHz range, and offers a maximum theoretical rate of 108 Mbps. When using this mode, 802.1g stations and 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.

In this field…	Do this…
	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. This field only appears when configuring the primary WLAN, and it is inherited by all VAPs and WDS links.
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. This field only appears when configuring the primary WLAN, and it is inherited by all VAPs and WDS links.

In this field…	Do this…
Security	Select the security protocol to use. For information on the supported security protocols, see ***Wireless Security Protocols*** on page 269. If you select WEP encryption, the WEP Keys area opens. If you select 802.1x, the Authentication Server field appears. If you select WPA-Enterprise, the Authentication Server, Require WPA2 (802.11i), and WPA Encryption fields appear. If you select WPA-Personal, the Passphrase, Require WPA2 (802.11i), and WPA Encryption fields appear. Note: When configuring a WDS link, only None and WEP are supported.
Authentication Server	Specify which authentication server to use, by selecting one of the following: • RADIUS. A RADIUS server. • Internal User Database. The Safe@Office EAP authenticator.
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: • Enabled. Only wireless stations using WPA2 can access the wireless network. • Disabled. Wireless stations using either WPA or WPA2 can access the wireless network. This is the default.
WPA Encryption	Select the encryption method to use for authenticating and encrypting wireless data: • Auto. The Safe@Office appliance automatically selects the cipher used by the wireless client. This is the default. • AES. Advanced Encryption Standard • TKIP. Temporal Key Integrity Protocol Note: AES is more secure than TKIP; however, some devices do not support AES.
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.

In this field…	Do this…
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.
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 45: Advanced Wireless 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 and attempt to connect to your network. This is the default. Note: Hiding the SSID does not provide strong security, because a determined attacker can still discover your SSID. Therefore, it is not recommended to rely on this setting alone for security.
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 185. • 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.
Station-to-Station Traffic	Specify whether you want to allow wireless stations on this network to communicate with each other, by selecting one of the following: • Allow. Allow stations to communicate with each other. This is the default. • Block. Block traffic between wireless stations.

In this field…	Do this…
Wireless Transmitter	
Transmission Rate	Select the transmission rate: • Automatic. The Safe@Office appliance automatically selects a rate. This is the default. • A specific rate This field only appears when configuring the primary WLAN, and it is inherited by all VAPs and WDS links.
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. This field only appears when configuring the primary WLAN, and it is inherited by all VAPs and WDS links.

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. This field only appears when configuring the primary WLAN, and it is inherited by all VAPs and WDS links.
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 Wireless Appliance.
Multimedia QoS (WMM)	Specify whether to use the Wireless Multimedia (WMM) standard to prioritize traffic from WMM-compliant multimedia applications. This can have the following values: • **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.

Configuring Virtual Access Points

500W | Power Pack

You can partition the wireless network into wireless VLANs called virtual access points (VAPs). You can use VAPs to grant different permissions to groups of wireless users, by configuring each VAP with the desired security policy and network settings, and then assigning each group of wireless users to the relevant VAP. For more information on VAPs, see ***Overview*** on page 263.

Note: While virtual access points (VAPs) can have different security settings and network names, all VAPs inherit the following wireless settings from the primary WLAN:

- Country
- Operation Mode
- Channel
- Transmission Rate
- Transmitter Power
- Antenna Selection

For information on configuring these settings in the primary WLAN, see ***Manually Configuring a Wireless Network*** on page 280.

Note: To enable VAPs, you must first enable the primary WLAN network. If you disable the primary WLAN network, all VAPs are automatically disabled.

The procedure below explains how to add or edit a VAP. For information on deleting a VAP, see ***Deleting VLANs*** on page 181.

To add or edit a VAP

1. Configure and enable the primary WLAN.

   For information on configuring the primary WLAN manually, see ***Manually Configuring a Wireless Network*** on page 280.

   For information on using a wizard to configure the primary WLAN, see ***Using the Wireless Wizard*** on page 273.

2. If you intend to use the 802.1x or WPA-Enterprise security mode for the VAP, do one of the following:

   - To use the Safe@Office EAP authenticator for authenticating wireless clients, follow the workflow ***Using the Safe@Office EAP Authenticator for Authentication of Wireless Clients*** on page 395.

     You will be referred back to this procedure at the appropriate stage in the workflow, at which point you can continue from the next step.

   - To use a RADIUS server for authenticating wireless clients, configure a RADIUS server.

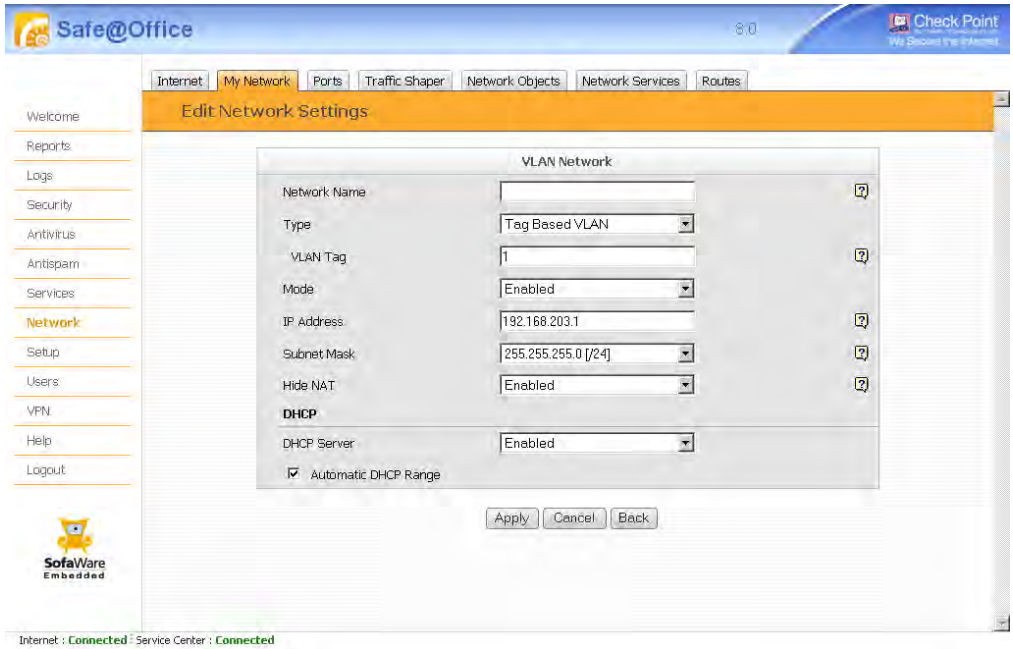
     See ***Using RADIUS Authentication*** on page 650.

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

   The My Network page appears.

4. Click Add Network.

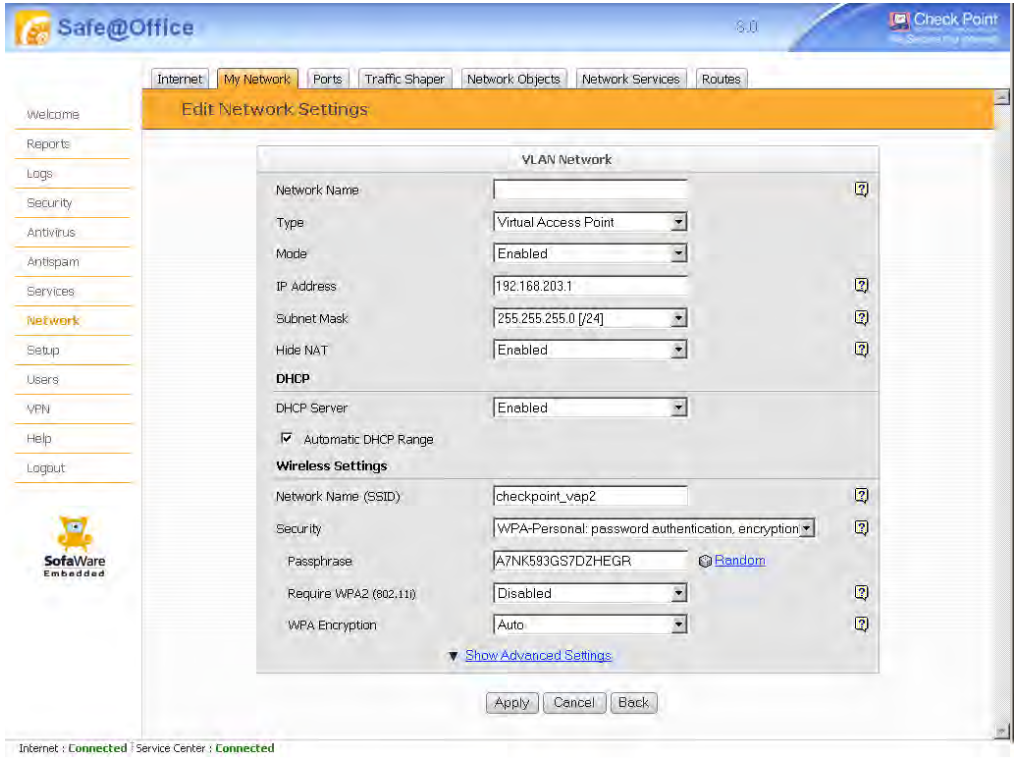
   The Edit Network Settings page appears.



5. In the Network Name field, type a name for the VAP.

6. In the **Type** drop-down list, select **Virtual Access Point**.

   New fields appear.



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

   The fields are enabled.

8. In the **IP Address** field, type the IP address of the VAP network's default gateway.

   The VAP network must not overlap other networks.

9. In the **Subnet Mask** field, type the VAP's internal network range.

10. If desired, enable or disable Hide NAT.

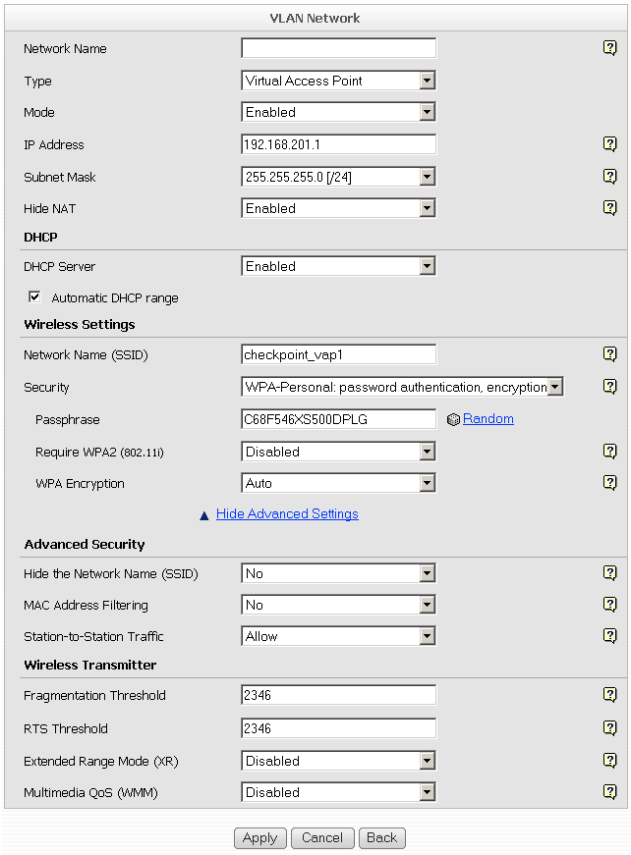
    See ***Enabling/Disabling Hide NAT*** on page 157.

11. If desired, configure a DHCP server.

See ***Configuring a DHCP Server*** on page 158.

12. Complete the fields using the information in ***Basic Wireless Settings Fields*** on page 284.
13. To configure advanced settings, click Show Advanced Settings and complete the fields using the information in ***Advanced Wireless Settings Fields*** on page 290.

    New fields appear.



14. Click Apply.

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

Configuring Wireless Distribution System Links

500W | Power Pack

You can extend the wireless network across multiple access points, or connect the networks behind different access points, by creating a Wireless Distribution System (WDS). To create a WDS, you must add WDS links between the desired access points.

For more information on WDS links, see ***Overview*** on page 263.

Note: While WDS links can have different security settings, all WDS links inherit the following wireless settings from the primary WLAN:

- Country
- Operation Mode
- Channel
- Transmission Rate
- Transmitter Power
- Antenna Selection

For information on configuring these settings in the primary WLAN, see ***Manually Configuring a Wireless Network*** on page 280.

Note: To enable WDS links, you must first enable the primary WLAN network. If you disable the primary WLAN network, all WDS links are automatically disabled.

The procedure below explains how to add or edit a WDS link. For information on deleting a WDS link, see ***Deleting VLANs*** on page 181.

To add or edit a WDS link

1. Configure and enable the primary WLAN.

   For information on configuring the primary WLAN manually, see ***Manually Configuring a Wireless Network*** on page 280.

For information on using a wizard to configure the primary WLAN, see ***Using the Wireless Wizard*** on page 273.

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

   The My Network page appears.

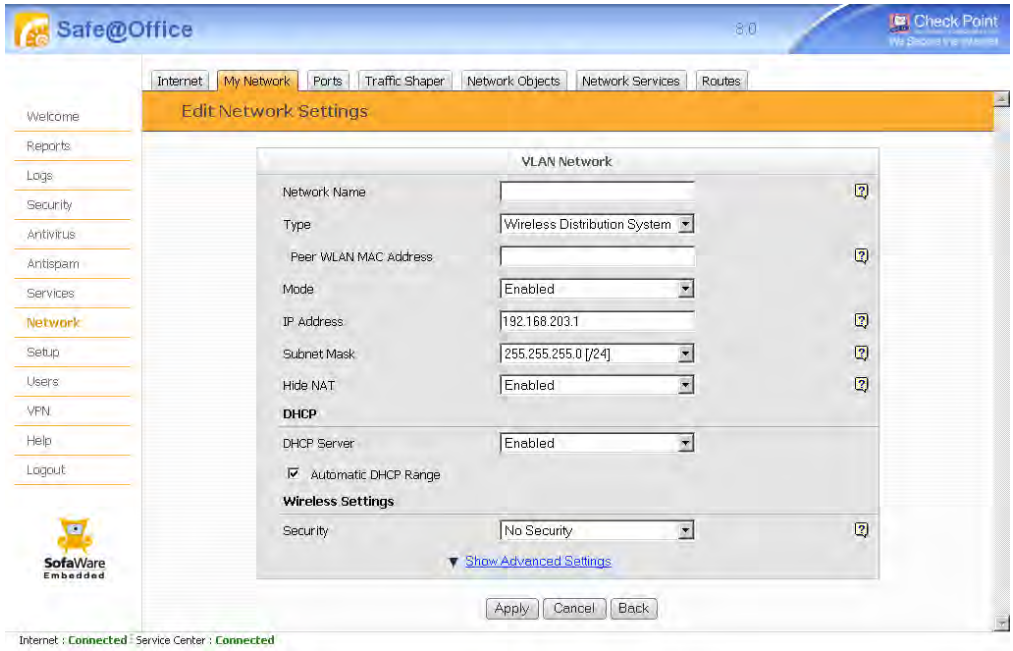
3. Click Add Network.

   The Edit Network Settings page appears.

4. In the Network Name field, type a name for the WDS link.

5. In the Type drop-down list, select Wireless Distribution System.

   New fields appear.



6. In the Peer WLAN MAC Address field, type the WLAN MAC address of the access point to which you want to create a WDS link.

Note: This is the MAC address of the *WLAN* interface, not the WAN MAC address. To see your access point's WLAN MAC address, click Reports in the main menu, and then click Wireless.

7. Do one of the following:
   - To create a bridged WDS link:
     1) In the Mode drop-down list, select Bridged.

        The fields are enabled and additional fields appear.
     2) Complete these fields as described in ***Bridged Network Fields*** on page 231.
   - To create a routed WDS link, do the following:
     1) In the Mode drop-down list, select Enabled.

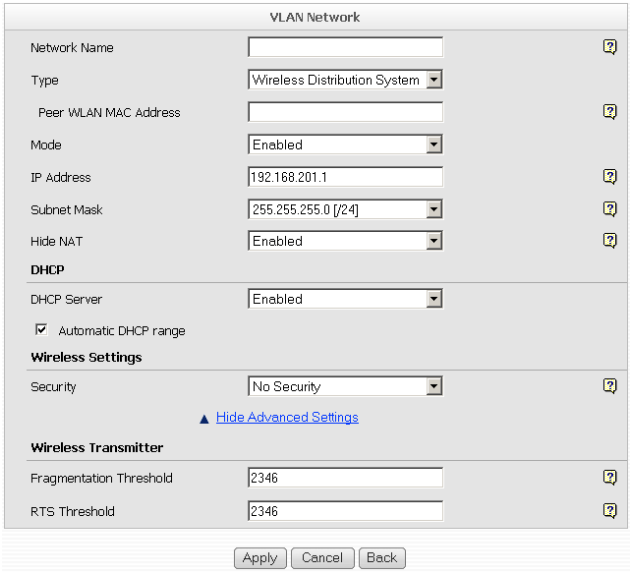
        The fields are enabled.
     2) In the IP Address field, type the IP address of the WDS link's default gateway.

        The WDS link must not overlap other networks.
     3) In the Subnet Mask field, type the WDS link's internal network range.
8. If desired, enable or disable Hide NAT.

   See ***Enabling/Disabling Hide NAT*** on page 157.
9. If desired, configure a DHCP server.

   See ***Configuring a DHCP Server*** on page 158.
10. Complete the fields using the relevant information in ***Basic Wireless Settings Fields*** on page 284.
11. To configure advanced settings, click Show Advanced Settings and complete the fields using the relevant information in ***Advanced Wireless Settings Fields*** on page 290.

New fields appear.



12. Click **Apply**.

Note: Both sides of the WDS link must use the same radio channel and security settings.

Note: WDS links support using the WEP security mode or no security. However, the access point can use any supported security protocol to communicate with wireless stations, including the WPA/WPA2 protocols.

Troubleshooting Wireless Connectivity

I cannot connect to a wireless network 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 195).
- Check that the wireless card region matches the access point region.
- Check the wireless card supports the wireless standard that you configured.

I cannot connect to an access point over a WDS link. What should I do?

- Check that both sides of the WDS link are configured with their peer's WLAN MAC address (and not the WAN MAC address).
- Check that both sides of the WDS link are configured to use the same radio channel and security settings.
- Make sure that the peer access points are not too far apart for proper reception.

How do I test wireless reception?

- Look at the Wireless page, and check for excessive errors or dropped packets.
- Look at the My 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 primary WLAN's advanced settings is set to Automatic (see ***Manually Configuring a Wireless Network*** on page 280).
- 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 primary WLAN's advanced settings.
- 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 wireless network's advanced settings, 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 My 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 wireless network's advanced settings 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 wireless network's advanced settings 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 than 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 11

Viewing Reports

This chapter describes the Safe@Office Portal reports.

This chapter includes the following topics:

Viewing the Safe@Office Appliance Status

500

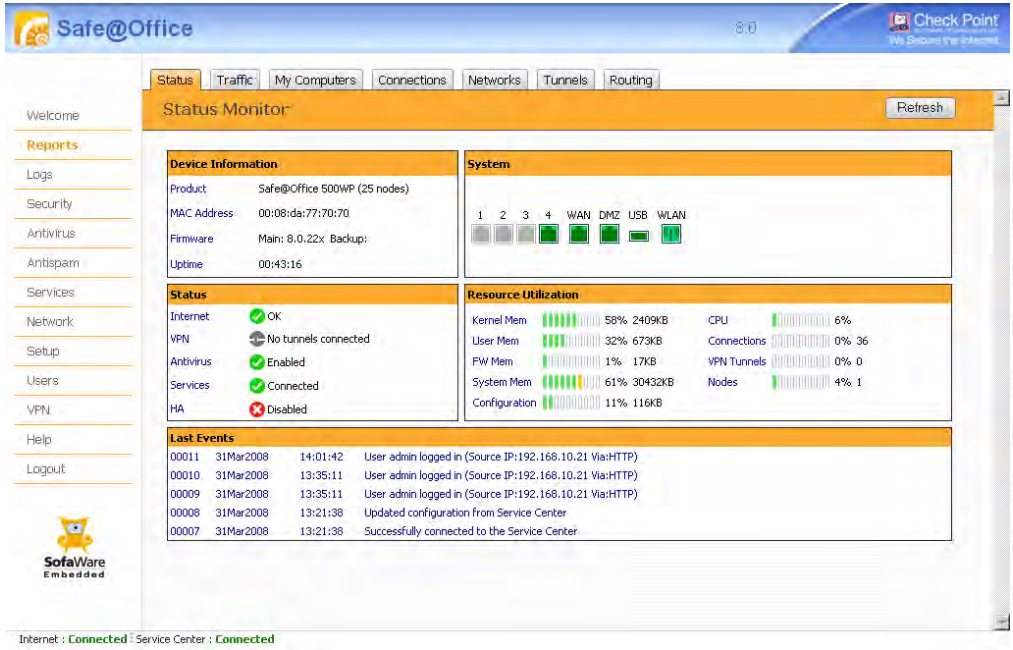
The Safe@Office Status Monitor provides a snapshot of the Safe@Office appliance's current status, enabling you to view the following information in a single glance:

- General appliance information
- Appliance module statuses
- Appliance port statuses
- Resource utilization information
- Recent logged events

To view the Safe@Office appliance's current status

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

   The Status Monitor page appears.



   The page displays the information in the following table.

2. To refresh the display, click Refresh.

Table 46: Status Monitor Fields

This field...	Displays...
Device Information	Information about the Safe@Office appliance.
Product	The licensed software and the number of allowed nodes.
MAC Address	The Safe@Office appliance's WAN MAC address.

This field…	Displays…
Firmware	The currently installed firmware: • Main. The version of the primary firmware • Backup. The version of the backup firmware
Uptime	The time that elapsed from the moment the unit was turned on
System	A diagram of the Safe@Office appliance's ports, indicating the ports' statuses. Ports that are currently in use appear in green.
Status	Information about the Safe@Office appliance's status.
Internet	The Safe@Office appliance's overall Internet connection status. This can be any of the following:

Icon	Description
	OK. One or both Internet connections are connected.
	Idle. Both Internet connections are in “idle” state.
	Disabled. Both Internet connections are disabled.
	Connected with problems. One Internet connection is connected, and the other Internet connection is in “Establishing Connection” state.
	No connectivity. All enabled Internet connections are in “Establishing Connection” state.

For information on individual Internet connections' statuses, see ***Status Bar*** on page 82.

This field...	Displays...
VPN	The Safe@Office appliance's VPN tunnel status. This can be any of the following:

Icon	Description
	No tunnels connected. There are no open VPN tunnels.
	Tunnels are established. There are open VPN tunnels.
	Some permanent tunnels are down. Some permanent VPN tunnels are currently down. To view VPN tunnels, click on the link.

Antivirus	The Safe@Office appliance's VStream Antivirus status. This can be any of the following:

Icon	Description
	Antivirus enabled. VStream Antivirus is enabled.
	Antivirus disabled. VStream Antivirus is disabled.
	Antivirus is enabled but no database is installed. VStream Antivirus is enabled; however, the VStream Antivirus databases are not installed.

This field...	Displays...
Services	The Safe@Office appliance's Service Center connection status. This can be any of the following:

Icon	Description
	Connected. The Safe@Office appliance is connected to the Service Center, and security services are active.
	Firmware download: *x*% completed. The Safe@Office appliance is currently downloading a firmware file from the Service Center. The download is *x*% complete.
	Disabled. You are not subscribed to a Service Center.
	Expired. Your subscription to security services has expired.
	Failed to connect. The Safe@Office appliance failed to connect to the Service Center.

HA	The Safe@Office appliance's High Availability status. This can be any of the following:

Icon	Description
	Passive. High Availability is enabled, and this appliance is a Passive Gateway.
	Master. High Availability is enabled, and this appliance is the Active Gateway.
	Disabled. High Availability is disabled.

This field…	Displays…
Resource Utilization	Safe@Office appliance resource utilization information. A bar graph next to each resource indicates the amount currently consumed.
Kernel Mem	The percentage of used memory in the kernel module, followed by the amount in kilobytes.
User Mem	The percentage of used memory in the user module, followed by the amount in kilobytes.
FW Mem	The percentage of used memory in the firewall module, followed by the amount in kilobytes.
System Mem	The percentage of system memory in use, followed by the amount in kilobytes.
Configuration	The percentage of configuration storage space in use out of the total amount of space allocated for configuration storage, followed by the amount in kilobytes.
CPU	The percentage of CPU in use.
Connections	The percentage of established connections out of the licensed number of connections, followed by the number of established connections.
VPN Tunnels	The percentage of established VPN tunnels out of the licensed number of VPN tunnels, followed by the number of established VPN tunnels.
Nodes	The percentage of nodes in use out of the licensed number of nodes, followed by the number of nodes in used.
Last Events	The last five messages logged to the Event Log.

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 313.

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

Table 47: 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 315.

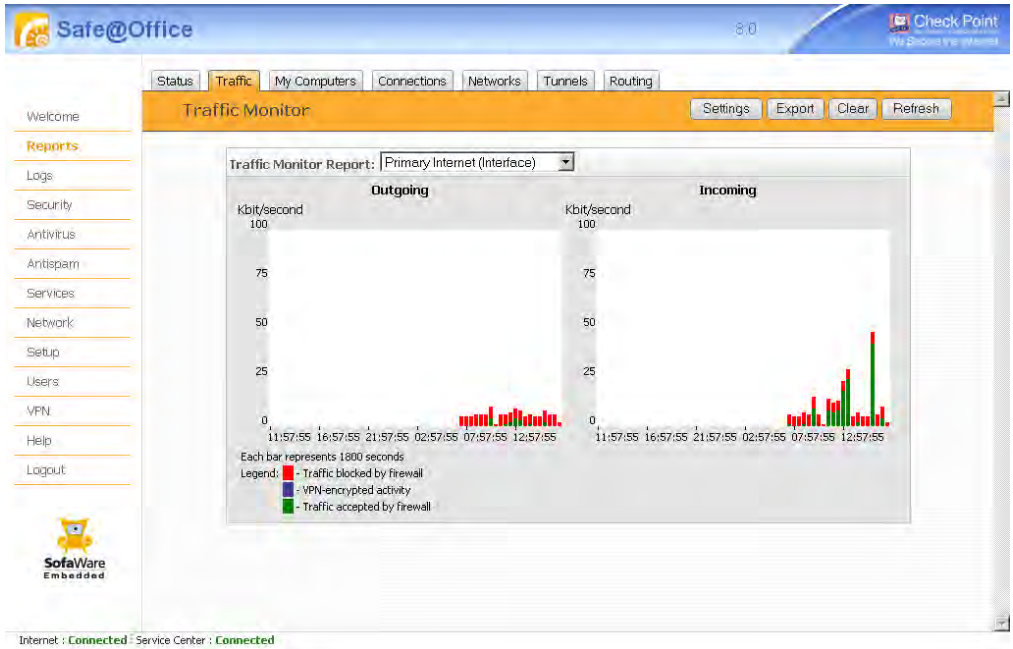
Viewing Traffic Reports

500

To view a traffic report

1. Click Reports in the main menu, and click the Traffic 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 102.

   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

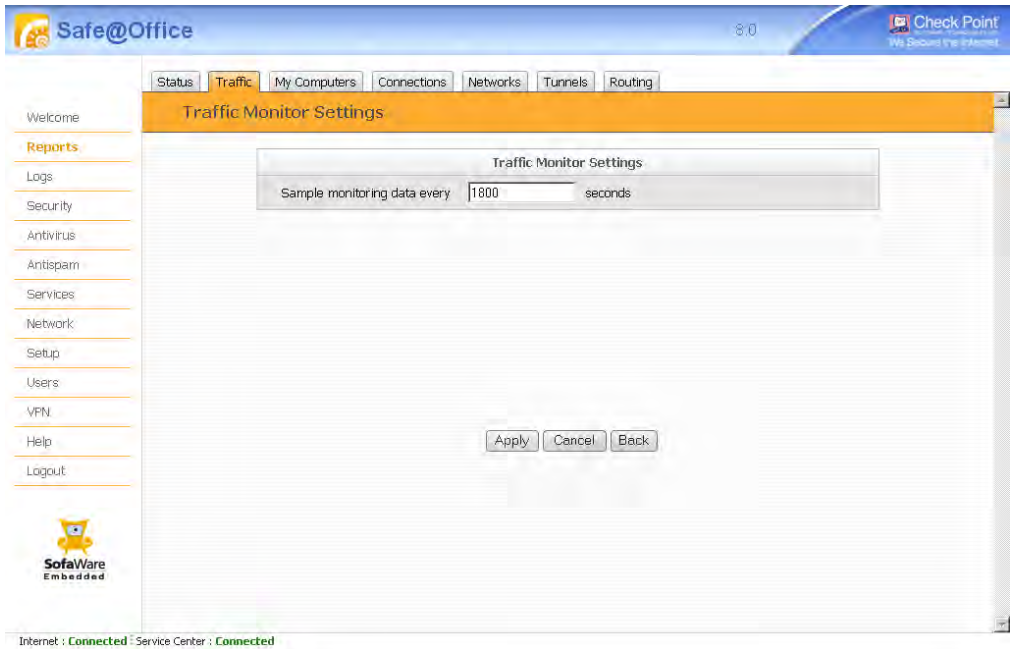
You can configure the interval at which the Safe@Office appliance should collect traffic data for network traffic reports.

To configure Traffic Monitor settings

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

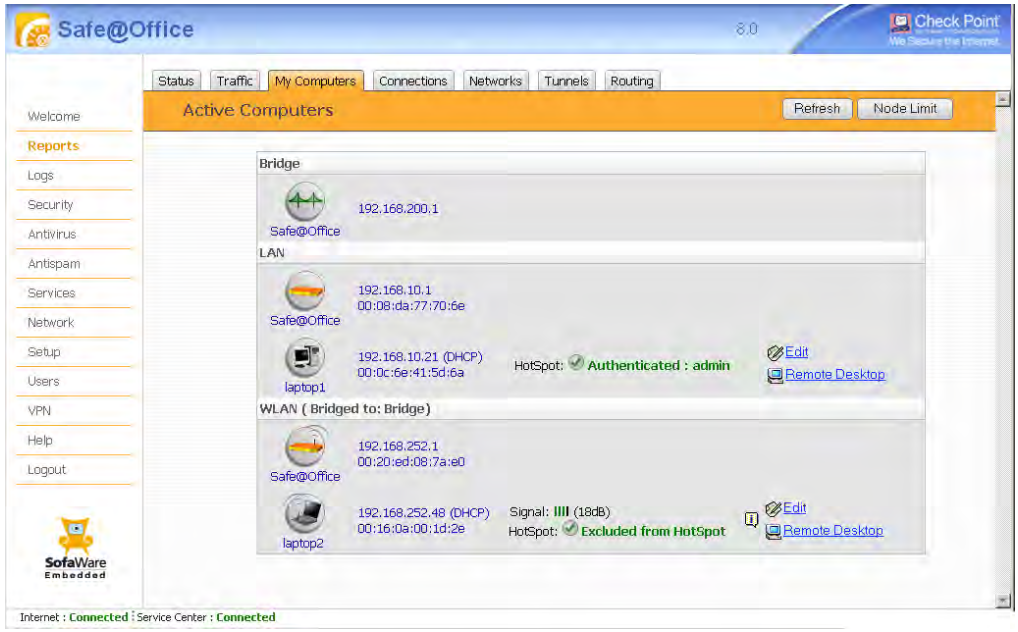
500

This option allows you to view the currently active computers on your network. The 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 computers

1. Click Reports in the main menu, and click the My 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 there are wireless networks, the wireless stations are shown under the network to which they are connected. For information on viewing statistics for these computers, see ***Viewing Wireless Station Statistics*** on page 336. 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 a network is bridged, the bridge's name appears in parentheses next to the network's name.

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.

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

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 685.

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

- Authenticated. The computer is logged in to My HotSpot.
- Not Authenticated. The computer is not logged in 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 187.

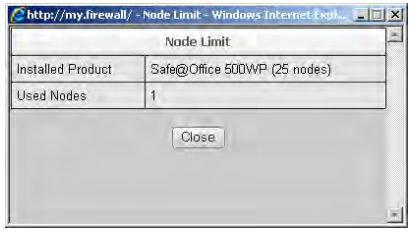
If Remote Desktop is enabled, a link appears next to each computer, enabling you to access its desktop remotely. For information on using Remote Desktop, see ***Using Remote Desktop*** on page 661.

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 187.

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

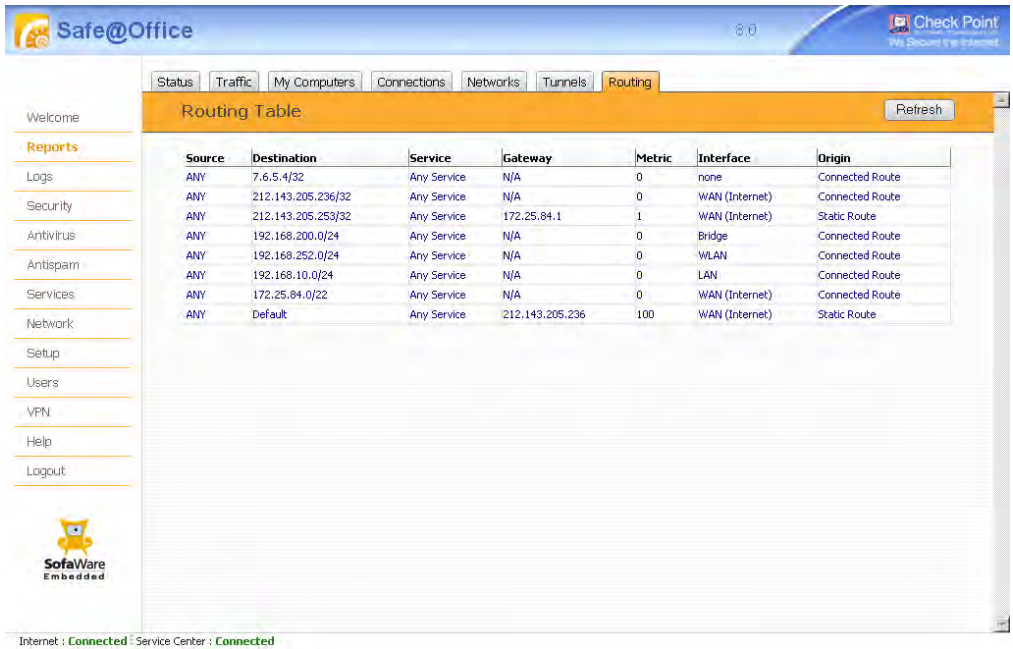
This option allows you to view currently active connections between your networks, as well as those from your networks to the Internet.

Note: The report does not display connections between bridged networks, where Firewall Between Members is disabled.

To view the active connections

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

The Connections page appears.



The page displays the information in the following table.

2. To view information about a 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.

3. To view information about a destination port, click the port.

   A window opens displaying information about the port.

4. To resize a column, drag the relevant column divider right or left.

5. To refresh the display, click Refresh.

Table 48: Connections Fields

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

Viewing Network Statistics

500

You can view statistics for each of the Safe@Office appliance's Internet connections, internal networks and bridges, using the Network Interface Monitor.

Viewing General Network Statistics

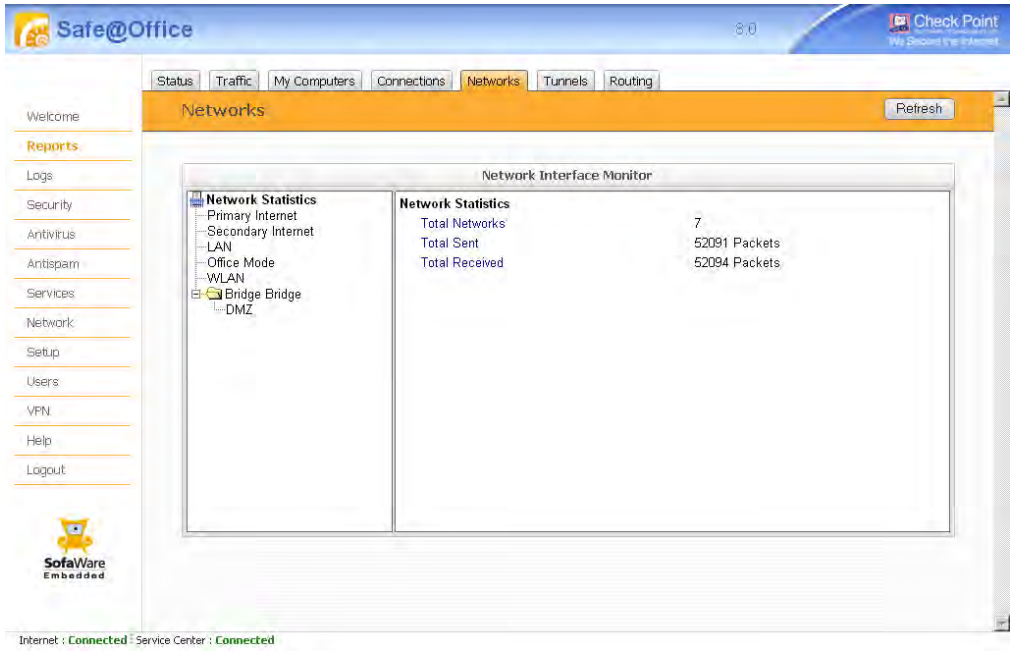
500

You can view general statistics for the Safe@Office appliance's network interfaces.

To view general network statistics

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

   The Networks page appears displaying general network statistics. For information on the fields, see the following table.



2. To refresh the display, click Refresh.

Table 49: General Network Statistics

This field…	Displays…
Total Networks	The total number of internal networks.
Total Sent	The total number of sent packets on all network interfaces.
Total Received	The total number of received packets on all network interfaces.

Viewing Internet Connection Statistics

500

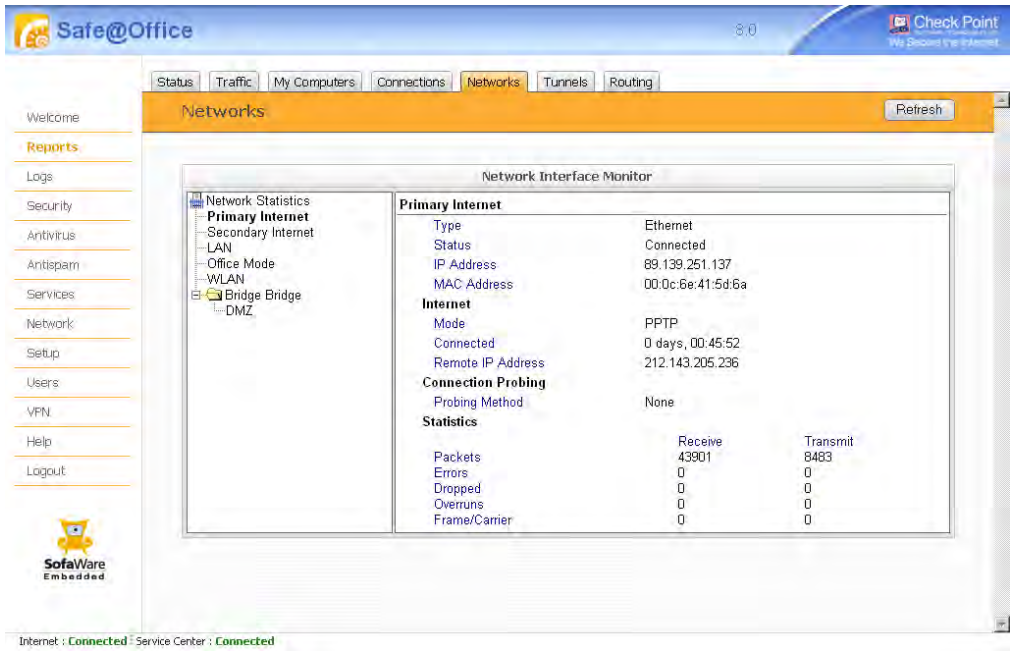
You can view statistics for the primary and secondary Internet connections.

To view statistics for an Internet connection

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

   The Networks page appears.
2. In the tree, click on the Internet connection.

The page displays statistics for the Internet connection. The following example shows statistics for the primary Internet connection.



For information on the fields, see the following table.

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

Table 50: Internet Connection Statistics

This field…	Displays…
Type	The Internet connection's type
Status	The Internet connection's status
IP Address	The appliance's current IP address on the network interface
MAC Address	The appliance's MAC address on the network interface
Internet	

This field…	Displays…
Mode	The Internet connection method used
Connected	The connection duration, in the format hh:mm:ss, where: hh=hours mm=minutes ss=seconds
Remote IP Address	The IP address of the PPP peer. This field is only relevant for PPP-based Internet connections.
Connection Probing	
Probing Method	The connection probing method configured for the Internet connection
ADSL	These fields only appear for ADSL connections.
Standard	The DSL line's standard
Annex	The Safe@Office ADSL model (Annex A, Annex B)
Self Test	Indicates whether DSL modem has passed a self-test
Trellis Coding	The DSL line's trellis coding
Framing Structure	The DSL line's framing structure
Line Rate	The line rate for transmission (TX) and reception (RX) in kbps
ADSL Firmware	The installed ADSL firmware
ADSL Firmware [Backup]	The installed backup ADSL firmware

This field…	Displays…
RF status	These fields only appear for ADSL connections.
Tx Power	The local and remote transmission power in dB
SNR Margin	The local and remote Signal to Noise Ration (SNR) margin in dB.
	The SNR margin is the difference between the amount of noise received by the by the local/remote line end, and the amount of noise it can tolerate.
Line Attenuation	The local and remote line attenuation in dB.
	The line attenuation is the difference between the signal power transmitted to the local/remote line end, and that which it received.
Statistics	Statistics only appear if the Internet connection is connected
Packets	The total number of transmitted and received packets
Errors	The total number of transmitted and received packets for which an error occurred
Dropped	The total number of transmitted and received packets that the firewall dropped
Overruns	The total number of transmitted and received packets that were lost, because they were sent or arrived more quickly that the appliance could handle

This field…	Displays…
Frame/Carrier	The total number of frame alignment and carrier errors. Frame alignment errors occur when a frame that has extra bits is received. The number of such errors appears in the Received column. Carrier errors occur when the carrier is not present at the start of data transmission, or when the carrier is lost during transmission. Such errors usually indicate a problem with the cable. The number of such errors appears in the Transmitted column.

Viewing Wired Network Statistics

500

You can view statistics for wired network interfaces, including the LAN, DMZ, OfficeMode, tag-based VLANs, and port-based VLANs.

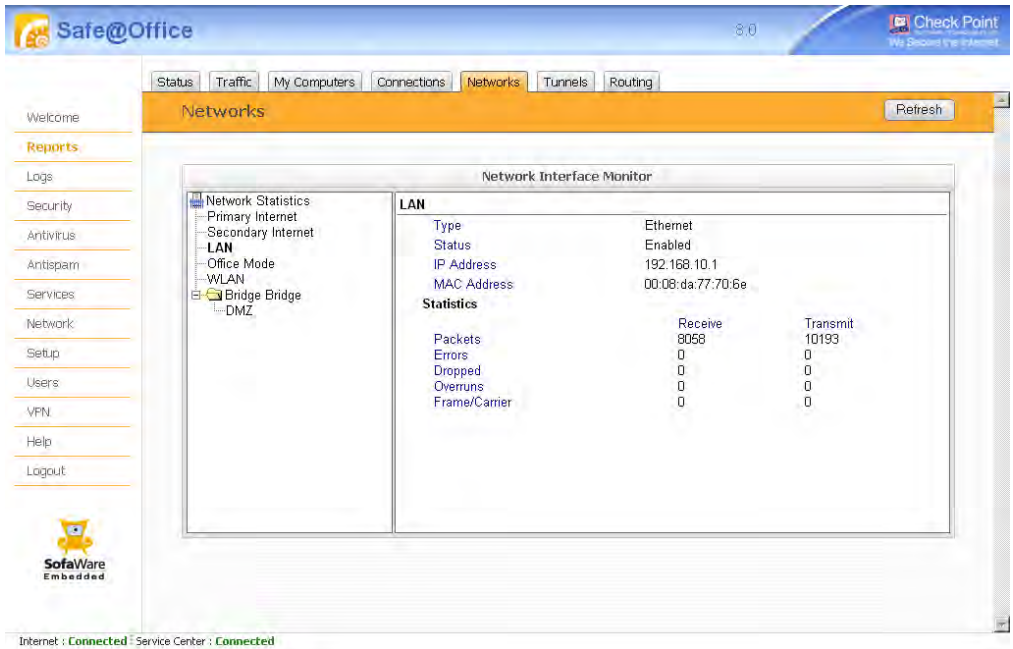
To view statistics for a wired network

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

   The Networks page appears.

2. In the tree, click on the wired network.

The page displays statistics for the network. The following example shows statistics for the LAN. For information on the fields, see the following table.



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

Table 51: Wired Network Statistics

This field…	Displays…
Type	The network's type.
Status	The network's current status (Enabled/Disabled).
IP Address	The appliance's current IP address on the network interface.
MAC Address	The appliance's MAC address on the network interface.

This field…	Displays…
Statistics	Statistics only appear if the network is enabled
Packets	The total number of transmitted and received packets
Errors	The total number of transmitted and received packets for which an error occurred
Dropped	The total number of transmitted and received packets that the firewall dropped
Overruns	The total number of transmitted and received packets that were lost, because they were sent or arrived more quickly that the appliance could handle
Frame/Carrier	The total number of frame alignment and carrier errors. Frame alignment errors occur when a frame that has extra bits is received. The number of such errors appears in the Received column. Carrier errors occur when the carrier is not present at the start of data transmission, or when the carrier is lost during transmission. Such errors usually indicate a problem with the cable. The number of such errors appears in the Transmitted column.

Viewing Wireless Network Statistics

500W

If the primary WLAN is enabled, you can view wireless statistics for the primary WLAN and VAPs.

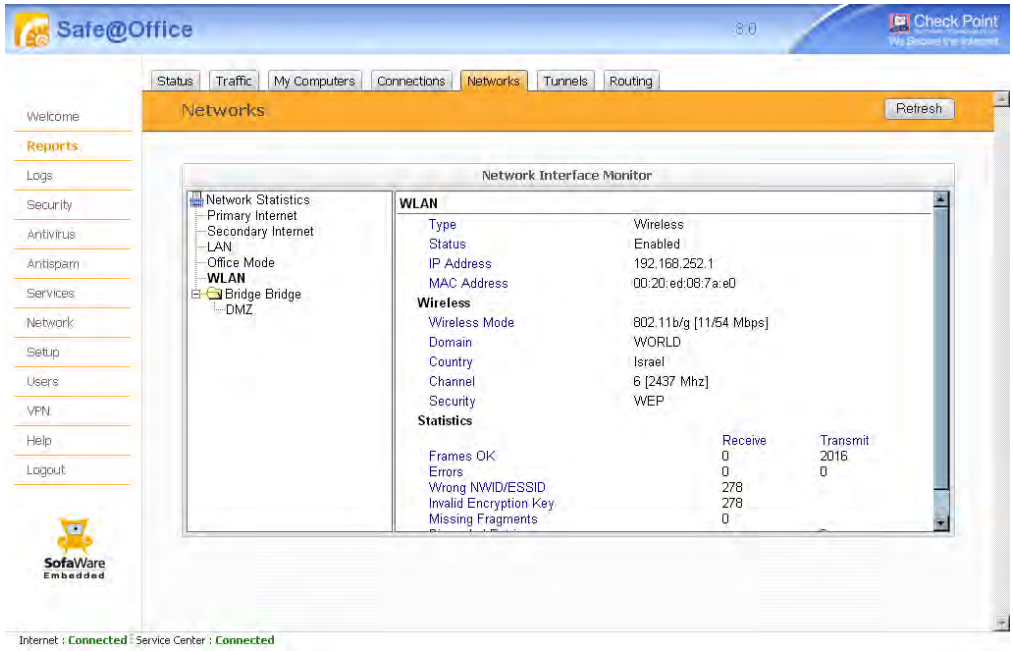
To view statistics for the primary WLAN and VAPs

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

   The Networks page appears.

2. In the tree, click on the wireless network's name.

   The page displays statistics for the network. For information on the fields, see the following table.



3. To refresh the display, click Refresh.

Table 52: Wireless Statistics

This field...	Displays...
Type	The network's type, in this case "Wireless"
Status	The network's current status (Enabled/Disabled)
IP Address	The IP address of the wireless network's default gateway
MAC Address	The MAC address of the wireless network interface
Wireless	
Wireless Mode	The operation mode used by the WLAN, followed by the transmission rate in Mbps
Domain	The Safe@Office access point's region
Country	The country configured for the WLAN
Channel	The radio frequency used by the WLAN
Security	The security mode used by the wireless network
Statistics	Statistics only appear if the network is enabled
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
Wrong NWID/ESSID	The total number of received packets that were dropped, because they were destined for another access point
Invalid Encryption Key	The total number of transmitted and received packets with the wrong encryption key

This field…	Displays…
Missing Fragments	The total number of packets missed during transmission and reception that were dropped, because fragments of the packet were lost
Discarded Retries	The total number of discarded retry packets that were transmitted and received
Discarded Misc	The total number of transmitted and received packets that were discarded for other reasons

Viewing Bridge Statistics

500

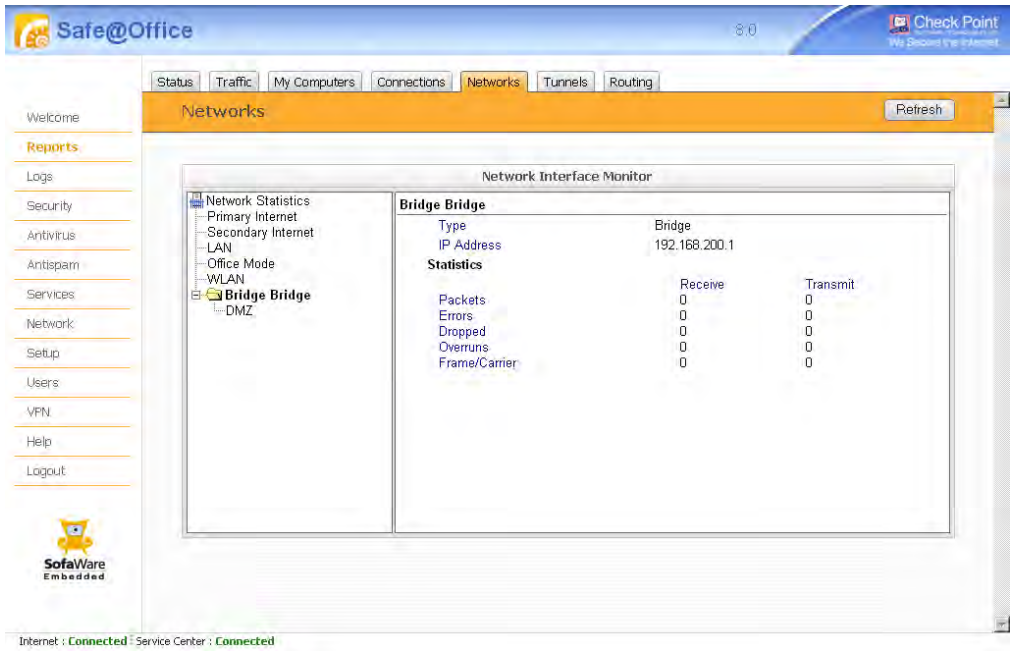
You can view statistics for bridges.

To view statistics for a bridge

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

   The Networks page appears.
2. In the tree, click on the bridge.

The page displays statistics for the bridge. For information on the fields, see the following table.



3. To view statistics for bridged networks, in the tree, expand the bridge's node.

   The page displays statistics for the bridged network.

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

Table 53: Bridge Statistics

This field…	Displays…
Type	The network's type, in this case "Bridge"
IP Address	The appliance's current IP address on the bridge interface
Statistics	Statistics only appear if the bridge is enabled
Packets	The total number of transmitted and received packets

This field…	Displays…
Errors	The total number of transmitted and received packets for which an error occurred
Dropped	The total number of transmitted and received packets that the firewall dropped
Overruns	The total number of transmitted and received packets that were lost, because they were sent or arrived more quickly that the appliance could handle
Frame/Carrier	The total number of frame alignment and carrier errors. Frame alignment errors occur when a frame that has extra bits is received. The number of such errors appears in the Received column. Carrier errors occur when the carrier is not present at the start of data transmission, or when the carrier is lost during transmission. Such errors usually indicate a problem with the cable. The number of such errors appears in the Transmitted column.

Viewing the Routing Table

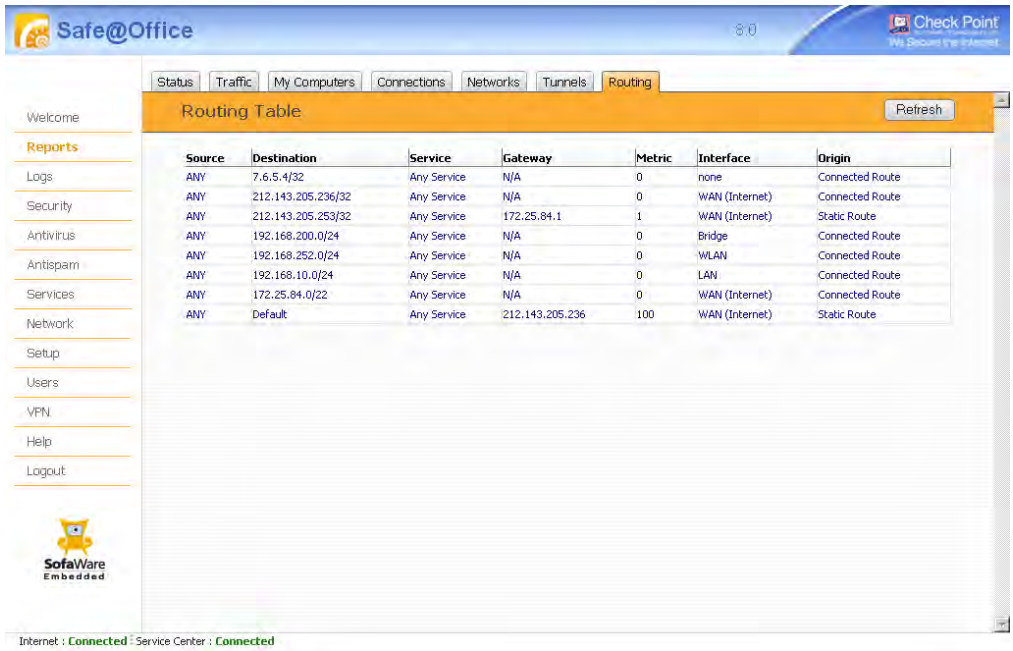
500

This option allows you to view the routing table currently in effect on the Safe@Office appliance.

To view the current routing table

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

   The Routing Table page appears.



Source	Destination	Service	Gateway	Metric	Interface	Origin
ANY	7.6.5.4/32	Any Service	N/A	0	none	Connected Route
ANY	212.143.205.236/32	Any Service	N/A	0	WAN (Internet)	Connected Route
ANY	212.143.205.253/32	Any Service	172.25.84.1	1	WAN (Internet)	Static Route
ANY	192.168.200.0/24	Any Service	N/A	0	Bridge	Connected Route
ANY	192.168.252.0/24	Any Service	N/A	0	WLAN	Connected Route
ANY	192.168.10.0/24	Any Service	N/A	0	LAN	Connected Route
ANY	172.25.84.0/22	Any Service	N/A	0	WAN (Internet)	Connected Route
ANY	Default	Any Service	212.143.205.236	100	WAN (Internet)	Static Route

   The page displays the information in the following table.

2. To resize a column, drag the relevant column divider right or left.
3. To refresh the display, click Refresh.

Table 54: Routing Table Fields

This field…	Displays…
Source	The route's source
Destination	The route's destination
Service	The network service for which the route is configured
Gateway	The gateway's IP address
Metric	The route's metric
Interface	The interface for which the route is configured
Origin	The route's type: • Connected Route. A route to a network that is directly connected to the Safe@Office appliance • Static Route. A destination-based or service-based static route. See ***Using Static Routes*** on page 199. • Dynamic Route. A route obtained through a dynamic routing protocol, such as OSPF • Source Route. A source-based static route. See ***Using Static Routes*** on page 199.

Viewing Wireless Station Statistics

500W

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

To view statistics for a wireless station

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

   The Active Computers page appears.

   The following information appears next to each wireless station:

   - The signal strength in dB
   - A series of bars representing the signal strength
2. Mouse-over the information icon next to the wireless station.

   A tooltip displays statistics for the wireless station, as described in the following table.
3. To refresh the display, click Refresh.

Table 55: 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
Management	The total number of transmitted and received management packets
Control	The total number of received control packets
Errors	The total number of transmitted and received frames for which an error occurred
Dup ratio	The percentage of frames received more than once.

This field…	Displays…
Cipher	The security protocol used for the wireless connection
QoS	Indicates whether the client is using Multimedia QoS (WMM). Possible values are: • yes. The client is using WMM. • no. The client is not using WMM.
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.

Chapter 12

Viewing Logs

This chapter describes the Safe@Office appliance logs.

This chapter includes the following topics:

Viewing the Event Log

500

The Event Log displays general appliance events, including the following:

- Authentication attempts
- Changes in setup
- Internet connection status changes
- Errors
- Warnings

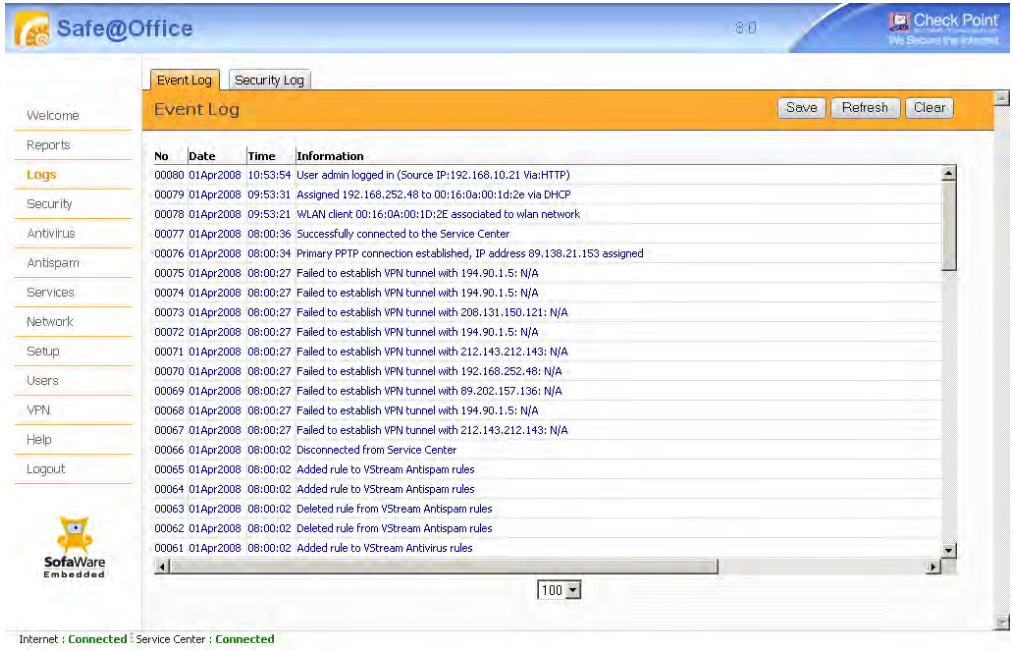
This information is useful for troubleshooting. You can export the logs to an *.xls (Microsoft Excel) file, and then store it for analysis purposes or send it to technical support.

Note: You can configure the Safe@Office appliance to send event and security logs to a Syslog server. For information, see ***Configuring Syslog Logging*** on page 689.

To view the event log

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

   The Event Log page appears.



   The log table contains the columns described in ***Event Log Columns*** on page 342. The log messages are color-coded as described in ***Event Log Color Coding*** on page 343.

2. To navigate the log table, do any of the following:

   - To scroll through the displayed log page:
     - Use the scroll bars, or
     - Click on a log message and then press the UP and DOWN arrows on your keyboard.
   - To view the next log page, click Next.
   - To view the previous log page, click Back.

3. To specify the number of logs to display per page, in the drop-down list at the bottom of the log table, select the desired number.

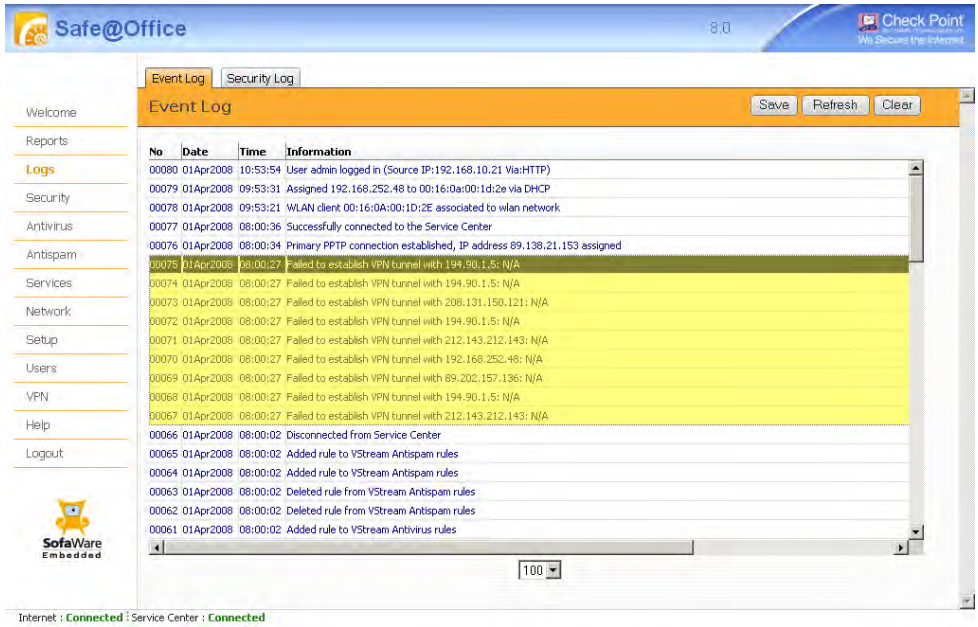
4. To resize a column, drag the relevant column divider right or left.
5. To refresh the display, click **Refresh**.
6. To save the displayed events to an *.xls file:
   a. Click **Save**.

      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.
7. To copy log messages, do the following:
   a. Select the desired logs, by clicking in the log table and dragging the cursor.

      The selected logs are highlighted in yellow.



b. Press CTRL+C.

If you are using Internet Explorer, and this is the first time that you copy logs, a dialog box asks you whether you want to allow the Safe@Office Portal to access your clipboard. In this case, click Allow access.

The selected logs are copied to your clipboard.

8. To clear all displayed events:

a. Click Clear.

A confirmation message appears.

b. Click OK.

All events are cleared.

Table 56: Event Log Columns

This column...	Displays...
No	The log message number
Date	The date on which the event occurred, in the format DD:MM:YYYY, where: DD=date MM=month, in abbreviated form YYYY=year
Time	The time at which the event occurred, in the format hh:mm:ss, where: hh=hour mm=minutes ss=seconds
Information	A description of the logged event

Table 57: Event Log Color Coding

An event marked in this color…	Indicates…
Red	An error message
Orange	A warning message
Blue	An informational message

Viewing the Security Log

500

The Security Log displays security-related events, including the following:

- Connections logged by firewall rules
- Connections logged by VStream Antivirus
- Connection logged by VStream Antispam
- Security events logged by SmartDefense
- Web sites blocked by Web rules or the centralized Web Filtering service

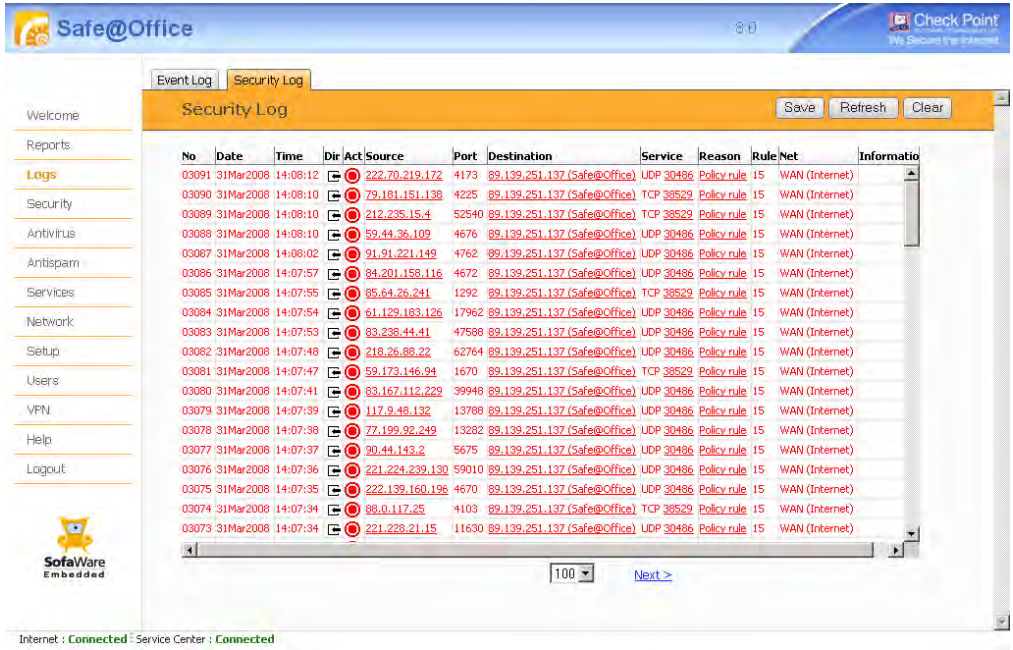
This information is useful for troubleshooting. You can export the logs to an *.xls (Microsoft Excel) file, and then store it for analysis purposes or send it to technical support.

Note: You can configure the Safe@Office appliance to send event and security logs to a Syslog server. For information, see ***Configuring Syslog Logging*** on page 689.

To view the event log

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

   The Security Log page appears.



   The log table contains the columns described in ***Security Log Columns*** on page 347. The log messages are color-coded as described in ***Security Log Color Coding*** on page 349.

2. To display information about a connection source or destination, click the relevant IP address.

   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 view information about a destination port, click the port.

   A window opens displaying information about the port.

4. To navigate the log table, do any of the following:

   - To scroll through the displayed log page:

- Use the scroll bars, or
- Click on a log message and then press the UP and DOWN arrows on your keyboard.

- To view the next log page, click Next.
- To view the previous log page, click Back.

5. To specify the number of logs to display per page, in the drop-down list at the bottom of the log table, select the desired number.
6. To resize a column, drag the relevant column divider right or left.
7. To refresh the display, click Refresh.
8. 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.

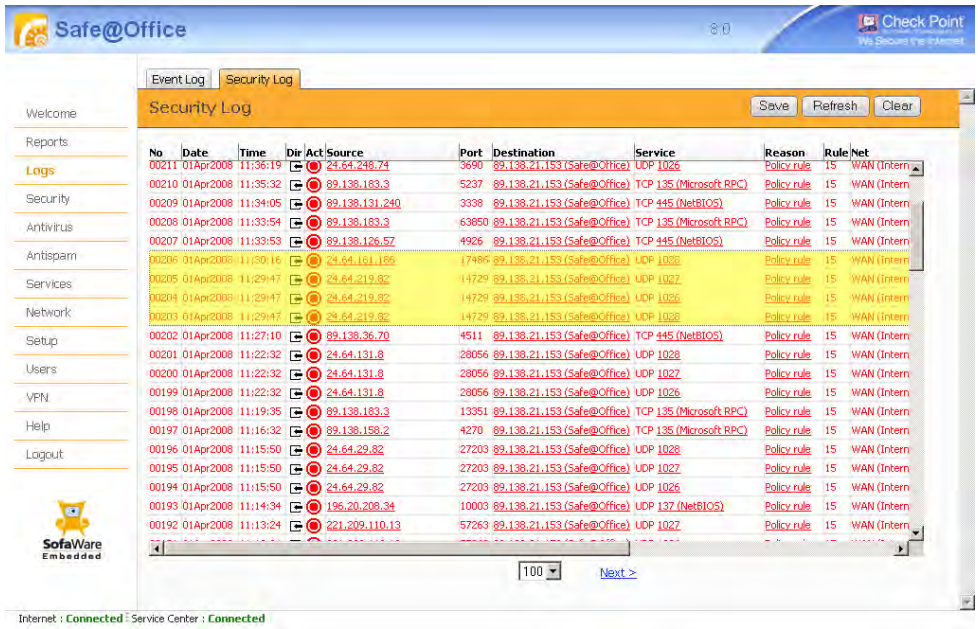
   d. Type a name for the configuration file and click Save.

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

9. To copy log messages, do the following:

   a. Select the desired logs, by clicking in the log table and dragging the cursor.

The selected logs are highlighted in yellow.



b. Press CTRL+C.

If you are using Internet Explorer, and this is the first time that you copy logs, a dialog box asks you whether you want to allow the Safe@Office Portal to access your clipboard. In this case, click **Allow access**.

The selected logs are copied to your clipboard.

10. To clear all displayed events:

a. Click **Clear**.

A confirmation message appears.

b. Click **OK**.

All events are cleared.

Table 58: Security Log Columns

This column...	Displays...
No	The log message number
Date	The date on which the action occurred, in the format DD:MM:YYYY, where: DD=date MM=month, in abbreviated form YYYY=year
Time	The time at which the action occurred, in the format hh:mm:ss, where: hh=hour mm=minutes ss=seconds
Dir	An icon indicating the direction of the connection on which the firewall acted. This can be one of the following: • Incoming connection • Outgoing connection • Internal connection
Act	An icon indicating the action that the firewall performed on a connection. For a list of Actions icons, see ***Security Log Actions*** on page 348.
Source	The IP address of the connection's source.
Port	The source port used for the connection.
Destination	The IP address of the connection's destination.

This column...	Displays...
Service	The protocol and destination port used for the connection.
Reason	The reason the action was logged.
Rule	The number of the firewall rule that was executed.
Net	The internal network where the action occurred.
Information	Additional information about the logged action.

Table 59: Security Log Actions

Action	Icon	Description
Connection accepted		The firewall accepted a connection.
Connection decrypted		The firewall decrypted a connection.
Connection dropped		The firewall dropped a connection.
Connection encrypted		The firewall encrypted a connection.
Connection rejected		The firewall rejected a connection.
URL Allowed		The firewall allowed a URL.
URL Blocked		The firewall blocked a URL.
Spam Stamped		VStream Antispam marked an email as spam.
Spam Detected		VStream Antispam rejected a spam email.
Connection Monitored		A security event was monitored; however, it was not blocked, due to the current configuration.
Mail Allowed		VStream Antispam logged a non-spam email.

Action	Icon	Description
Blocked by VStream Antivirus		VStream Antivirus blocked a connection.

Table 60: Security Log Color Coding

An event marked in this color…	Indicates…
Red	Connection attempts that were blocked by your firewall, by a security policy downloaded from your Service Center, or by user-defined rules.
Orange	Traffic detected as suspicious, but accepted by the firewall. For example, if a SmartDefense protection's Action field is set to "Track" instead of "Block", and a connection triggers this protection, the connection is accepted and logged in orange.
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.

Chapter 13

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 551.

This chapter includes the following topics:

The Safe@Office Firewall Security Policy

What Is a Security Policy?

A security policy is a set of rules that defines your security requirements, including (but not limited to) network security. By themselves, the network security-related rules comprise the network security policy.

When configured with the necessary network security rules, the Safe@Office appliance serves as the enforcement agent for your network security policy. Therefore, the Safe@Office appliance's effectiveness as a security solution is directly related to the network security policy's content.

Security Policy Implementation

The key to implementing a network security policy is to understand that a firewall is simply a technical tool that reflects and enforces a network security policy for accessing network resources.

A *rule base* is an ordered set of individual network security rules, against which each attempted connection is checked. Each rule specifies the source, destination, service, and action to be taken for each connection. A rule also specifies how a communication is tracked, logged, and displayed. In other words, the rule base is the implementation of the security policy.

Security Policy Enforcement

The Safe@Office appliance uses the unique, patented INSPECT engine to enforce the configured security policy and to control traffic between networks. The INSPECT engine examines all communication layers and extracts only the relevant data, enabling highly efficient operation, support for a large number of protocols and applications, and easy extensibility to new applications and services.

Planning the Safe@Office Firewall Security Policy

Before creating a security policy for your system, answer the following questions:

- Which services, including customized services and sessions, are allowed across the network?
- Which user permissions and authentication schemes are needed?
- Which objects are in the network? Examples include gateways, hosts, networks, routers, and domains.
- Which network objects can connect to others, and should the connections be encrypted?
- What should be the event logging policy?
- Which Quality of Service (QoS) classes will you need?

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, primary WLAN, VLANs, VAPs, 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, primary WLAN, VLANs, VAPs, and OfficeMode).
- Access is blocked from the DMZ, primary WLAN, VLAN, VAP, and OfficeMode networks to the other internal networks, (including between different VLANs and VAPs).
- HTTPS access to the Safe@Office Portal (my.firewall, my.hotspot, and my.vpn) is allowed from all internal networks.
- HTTP access to the Safe@Office Portal (my.firewall, my.hotspot, and my.vpn) is allowed from all internal networks except the WLAN and VAPs. You can allow HTTP access from the primary WLAN and VAPs by creating a specific user-defined firewall rule.
- When using the print server function (see ***Using Network Printers*** on page 733), 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 360.

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 the following states.

Table 61: 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).

This level…	Does this…	Further Details
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.
Block All	Blocks all access between networks.	All inbound and outbound traffic is blocked between the internal networks. This does not affect traffic to and from the gateway itself.

The definitions of firewall security levels provided in this table represent the Safe@Office appliance's default security policy.

You can easily override the default security policy, by creating user-defined firewall rules. For further information, see ***Using Rules*** on page 360.

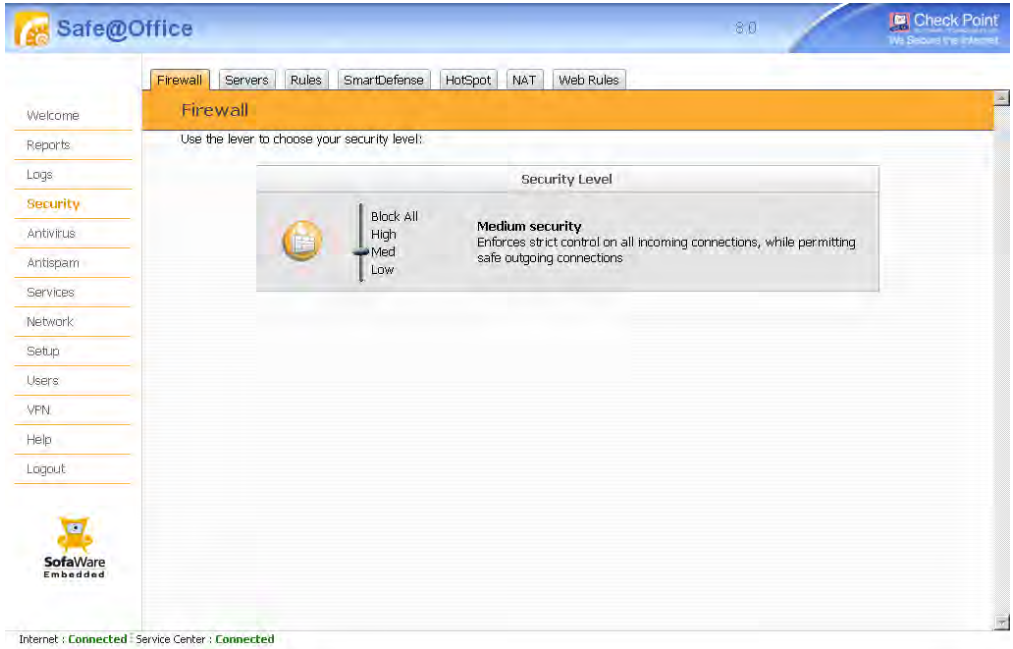
Note: If the security policy is remotely managed, this lever might be disabled.

Note: Security updates downloaded from a Service Center may alter the security 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 in your network (such as a Web Server, Mail Server, or an exposed host), you can skip this section.

The Safe@Office appliance enables you to configure the following types of public Internet servers:

- Servers for specific services

  You can allow all incoming connections of a specific service and forward them to a particular host in your network. For example, you can set up your own Web server, Mail server, or FTP server.

Note: Configuring servers is equivalent to creating simple Allow and Forward rules for common services, where the destination is This Gateway. For information on creating more complex rules, see ***Using Rules*** on page 360.

- Exposed host

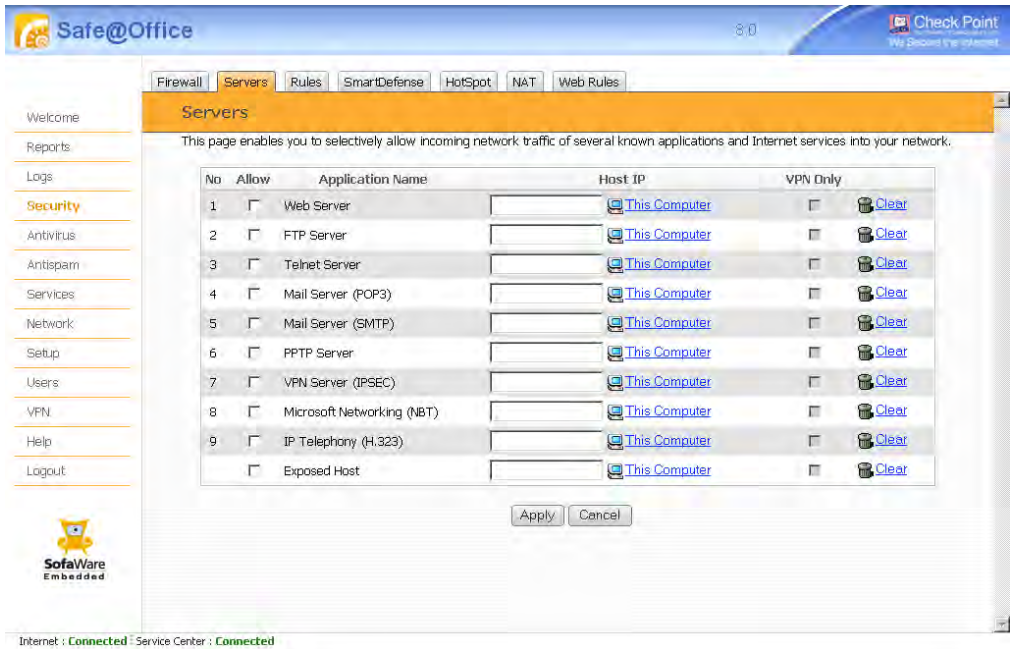
  If you need to allow unlimited incoming and outgoing connections between the Internet and a particular host, you can define an exposed host. An exposed host is not protected by the firewall, and it receives all traffic that was not forwarded to another computer by use of Allow and Forward rules.

Warning: Defining an exposed host is not recommended unless you are fully aware of the security risks. For example, an exposed host may be vulnerable to hacker attacks.

To allow services 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 following table.
3. Click **Apply**.

   A success message appears.

Table 62: Servers Page Fields

In this column…	Do this…
Allow	Select the check box next to the public server you want to configure. This can be either of the following: • A specific service or application (rows 1-9) • An exposed host (row 10)

In this column…	Do this…
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.
VPN Only	Select this option to allow only connections made through a VPN.

To stop the forwarding of services to a specific host

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

   The Servers page appears.

2. In the desired server's row, click Clear.

   The Host IP field is cleared.

3. Click Apply.

Using Rules

500

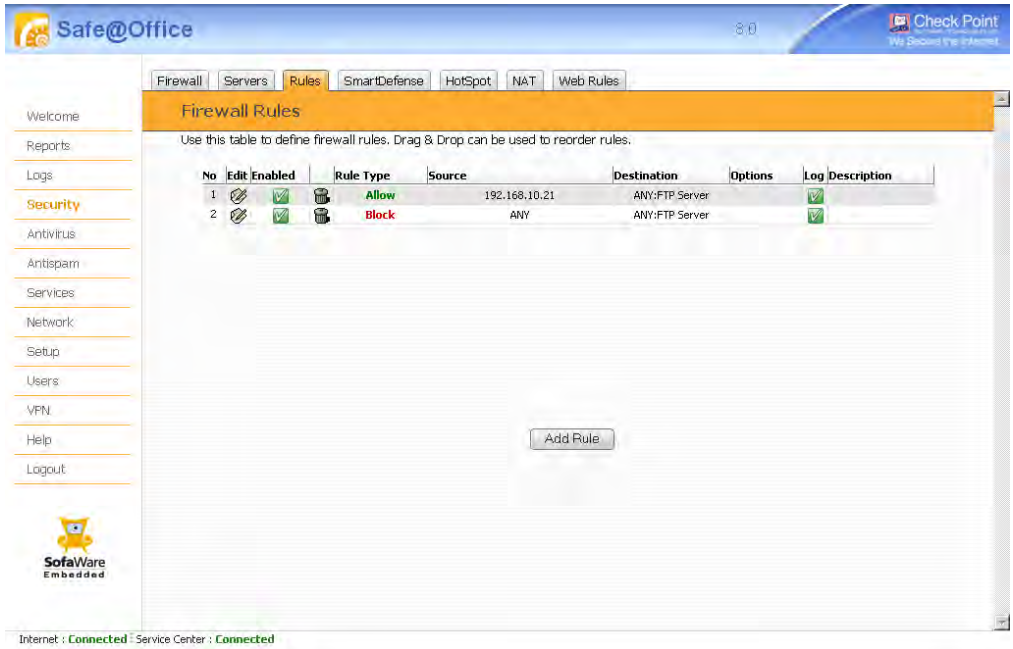
The Safe@Office appliance checks the protocol used, the ports range, and the destination IP address, when deciding whether to allow or block traffic.

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 63: Firewall Rule Types

Rule	Description
Allow and Forward	This rule type enables you to do the following: • Permit incoming traffic from the Internet to a specific service and destination IP address in your internal network and then forward all such connections to a specific computer in your network. Such rules are called NAT forwarding rules. For example, if the gateway has two public IP addresses, 62.98.112.1 and 62.98.112.2, and the network contains two private Web servers, A and B, you can forward all traffic with the destination 62.98.112.1 to server A, while forwarding all traffic with the destination 62.98.112.2 to server B. Note: Creating an Allow and Forward rule for incoming traffic to the default destination This Gateway (which represents the Safe@Office IP address), is equivalent to defining a server in the Servers page. • Permit outgoing traffic from your internal network to a specific service and destination IP address on the Internet and then divert all such connections to a specific IP address. Such rules are called transparent proxy rules. For example, you can redirect all traffic destined for a specific Web server on the Internet to a different IP address. • 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 251. Note: You must use this type of rule to allow incoming connections if your network uses Hide NAT.

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. 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 251. Note: You cannot use an Allow rule to permit incoming traffic, if the network or VPN uses Hide NAT. Use an “Allow and Forward” rule instead. 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. • Block connections between hosts on different internal networks.

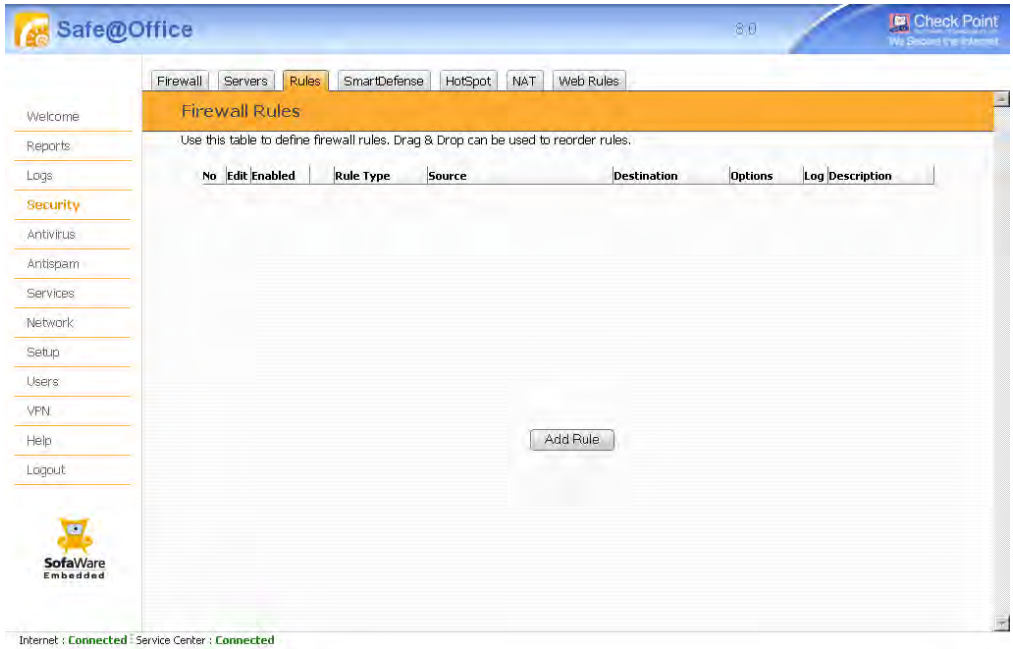
Adding and Editing Firewall Rules

500

To add or edit a firewall rule

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

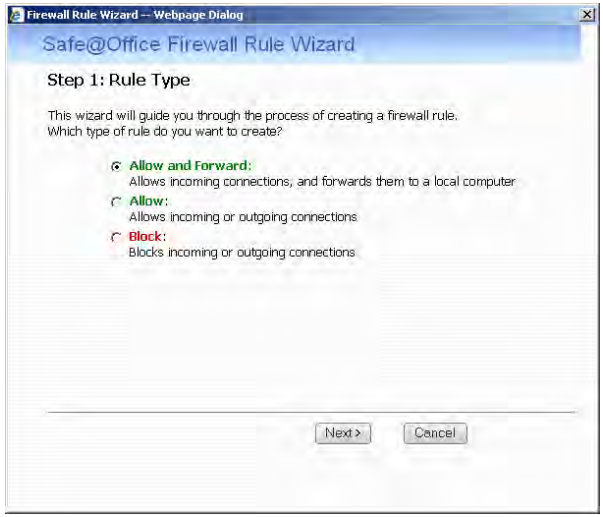
   The Rules page appears.



2. Do one of the following:

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

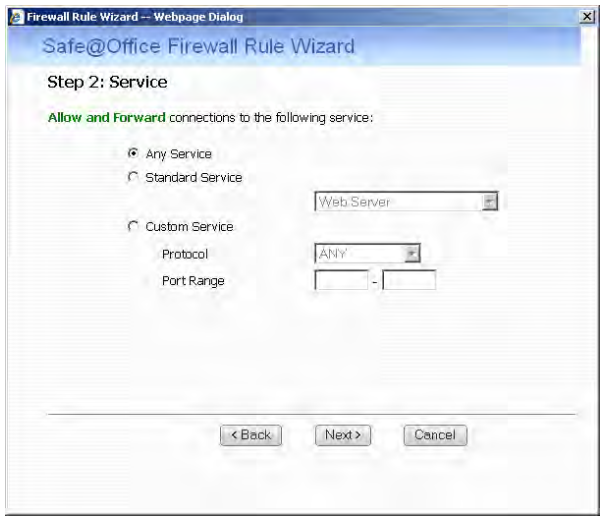
The **Safe@Office Firewall Rule** wizard opens, with the **Step 1: Rule Type** dialog box displayed.



3. Select the type of rule you want to create.
4. Click **Next**.

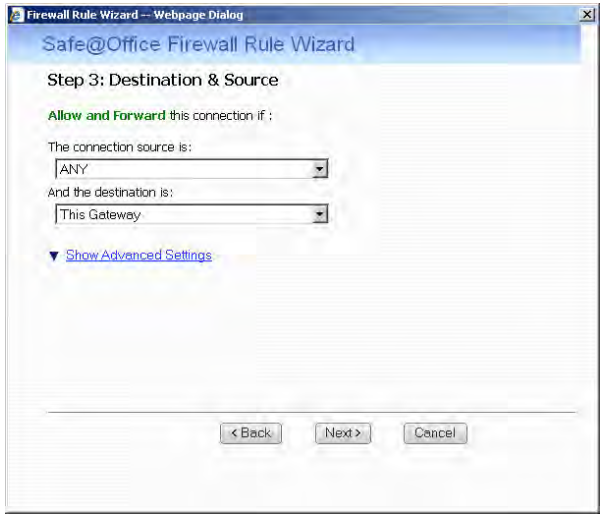
   The **Step 2: Service** dialog box appears.

   The example below shows an Allow and Forward rule.



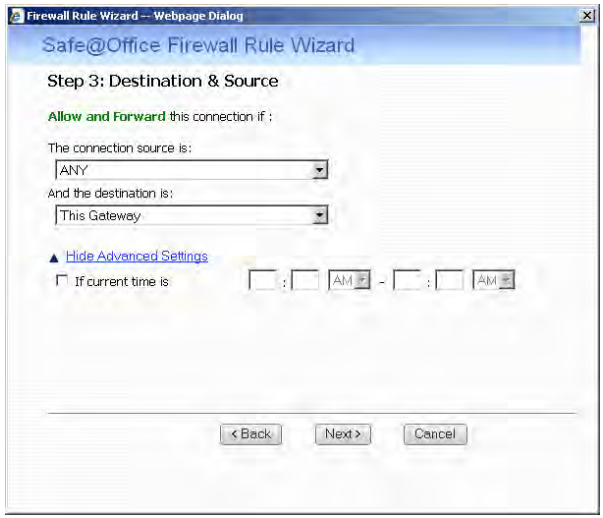
5. Complete the fields using the relevant information in the following table.
6. Click **Next**.

   The **Step 3: Destination & Source** dialog box appears.



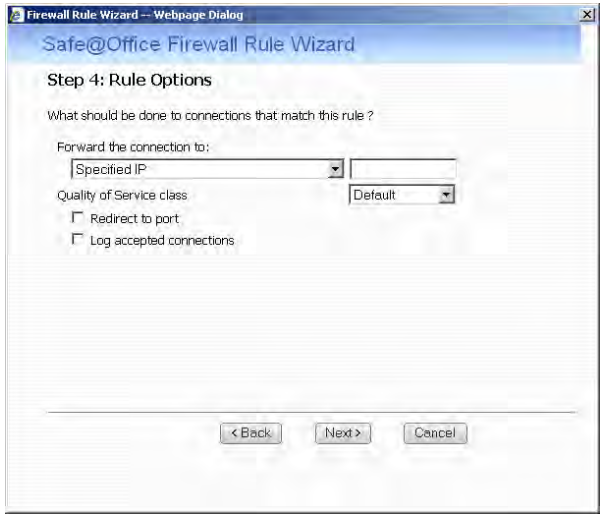
7. To configure advanced settings, click **Show Advanced Settings**.

   New fields appear.



8. Complete the fields using the relevant information in the following table.
9. Click **Next**.

   The **Step 4: Rule Options** dialog box appears.



10. Complete the fields using the relevant information in the following table.
11. Click **Next**.

The Step 5: Done dialog box appears.

12. If desired, type a description of the rule in the field provided.
13. Click Finish.

    The new rule appears in the Rules page.

Table 64: 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 or a network service object. You must then select the desired service or network service object 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.

In this field...	Do this...
Protocol	Select the protocol for which the rule should apply (ESP, GRE, TCP, UDP, ICMP, IGMP, or OSPF). To specify that the rule should apply for any protocol, select ANY. To specify a protocol by number, select Other. The Protocol Number field appears.
Port Range	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.
Protocol Number	Type the number of the protocol for which the rule should apply.
Source	Select the source of the connections you want to allow/block. This list includes network objects. To specify an IP address, select Specified IP and type the desired IP address in the field provided. To specify an IP address range, select Specified Range and type the desired IP address range in the fields provided. To specify the Safe@Office IP address, select This Gateway. To specify any source, select ANY.

In this field…	Do this…
Destination	Select the destination of the connections you want to allow/block. This list includes network objects. 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. To specify the Safe@Office IP addresses, select This Gateway. To specify any destination *except* the Safe@Office Portal IP addresses, select ANY.
If the current time is	Select this option to specify that the rule should be applied only during certain hours of the day. You must then use the fields and drop-down lists provided, to specify the desired time range.
Forward the connection to	Select the destination to which matching connections should be forwarded. To specify an IP address, select Specified IP and type the desired IP address in the text box. This field only appears when defining an Allow and Forward rule.

In this field…	Do this…
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 251. This drop-down list only appears when defining an Allow rule or an Allow and Forward rule.
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.
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.

Enabling/Disabling Firewall Rules

500

You can temporarily disable a user-defined rule.

To enable/disable a firewall rule

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

   The Rules page appears.

2. Next to the desired rule, in the Enabled column, 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.

Reordering Firewall Rules

500

To reorder firewall rules

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

   The Rules page appears.

2. For each rule you want to move, click on the rule and drag it to the desired location in the table.

Enabling/Disabling Firewall Rule Logging

500

You can enable or disable logging for a firewall rule, by using the information in ***Adding and Editing Firewall Rules*** on page 364, or by using the following shortcut.

To enable/disable logging for a firewall rule

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

   The Rules page appears.

2. Next to the desired rule, in the Log column, do one of the following:

   - To enable logging, click .

     The button changes to and logging is enabled for the rule.

   - To disable logging, click .

     The button changes to and logging is disabled for the rule.

Viewing and Deleting Firewall Rules

500

To view or delete an existing firewall rule

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

   The Rules page appears with a list of existing firewall rules.

2. To resize a column, drag the relevant column divider right or left.
3. To delete a rule, do the following.

   a. In the desired rule's row, click .

      A confirmation message appears.

   b. Click OK.

The rule is deleted.

Using Port-Based Security

Power Pack

The Safe@Office appliance supports the IEEE 802.1x standard for secure authentication of users and devices that are directly attached to Safe@Office appliance's LAN and DMZ ports, as well as the wireless LAN. Authentication can be performed either by an external RADIUS server, or by the Safe@Office appliance's built-in EAP authenticator. For information on the Safe@Office EAP authenticator, see ***Using the Safe@Office EAP Authenticator*** on page 394.

When an 802.1x security scheme is implemented for a port, users attempting to connect to that port are required to authenticate using their network user name and password. The Safe@Office appliance sends the user's credentials to the configured authentication server, and if authentication succeeds, a connection is established. If the user fails to authenticate, the port is physically isolated from other ports on the gateway.

If desired, you can specify how users should be handled after successful or failed authentication. Users who authenticate successfully on a specific port are assigned to the network with which that port is associated. For example, if the port is assigned to the DMZ network, all users who authenticate successfully on that port are assigned to the DMZ network.

When using a RADIUS server for authentication, you can assign authenticated users to specific network segments, by configuring dynamic VLAN assignment on the RADIUS server. Upon successful authentication, the RADIUS server sends RADIUS option 81 [Tunnel-Private-Group-ID] to the Safe@Office appliance, indicating to which network segment the user should be assigned. For example, if a member of the Accounting team connects to a network port and attempts to log in, the Safe@Office appliance relays the information to the RADIUS server, which replies with RADIUS option 81 and the value “Accounting”. The appliance then assigns the user’s port to the Accounting network, granting the user access to all the resources of the Accounting team.

The Safe@Office appliance also enables you to automatically assign users to a “Quarantine” network when authentication fails. All Quarantine network security and network rules will apply to those users. For example, you can create security rules allowing users on the Quarantine network to access the Internet and blocking them from

accessing sensitive company resources. You can also configure Traffic Shaper to grant members of the Quarantine network a lower amount of bandwidth than authorized users.

You can choose to exclude specific network objects from 802.1x port-based security enforcement. Excluded network objects will be able to connect to the Safe@Office appliance's ports and access the network without authenticating. For information on excluding network objects from 802.1x port-based security enforcement, see ***Using Network Objects*** on page 185.

Configuring Port-Based Security

Power Pack

To configure 802.1x port-based security for a port

1. Do one of the following:

   - To use the Safe@Office EAP authenticator for authenticating clients, follow the workflow ***Using the Safe@Office EAP Authenticator for Authentication of Wired Clients*** on page 396.

     You will be referred back to this procedure at the appropriate stage in the workflow, at which point you can continue from the next step.

   - To use a RADIUS server for authenticating clients, do the following:

     1) Configure a RADIUS server.

        See ***Using RADIUS Authentication*** on page 650.

     2) Configure the clients for 802.1x authentication.

        For information, refer to your RADIUS server documentation.

2. To configure dynamic VLAN assignment, do the following:

   a. Add port-based VLAN networks as needed.

      See ***Adding and Editing Port-Based VLANs*** on page 178.

   b. Configure RADIUS option 81 [Tunnel-Private-Group-ID] on the RADIUS server.

      For information, refer to your RADIUS server documentation.

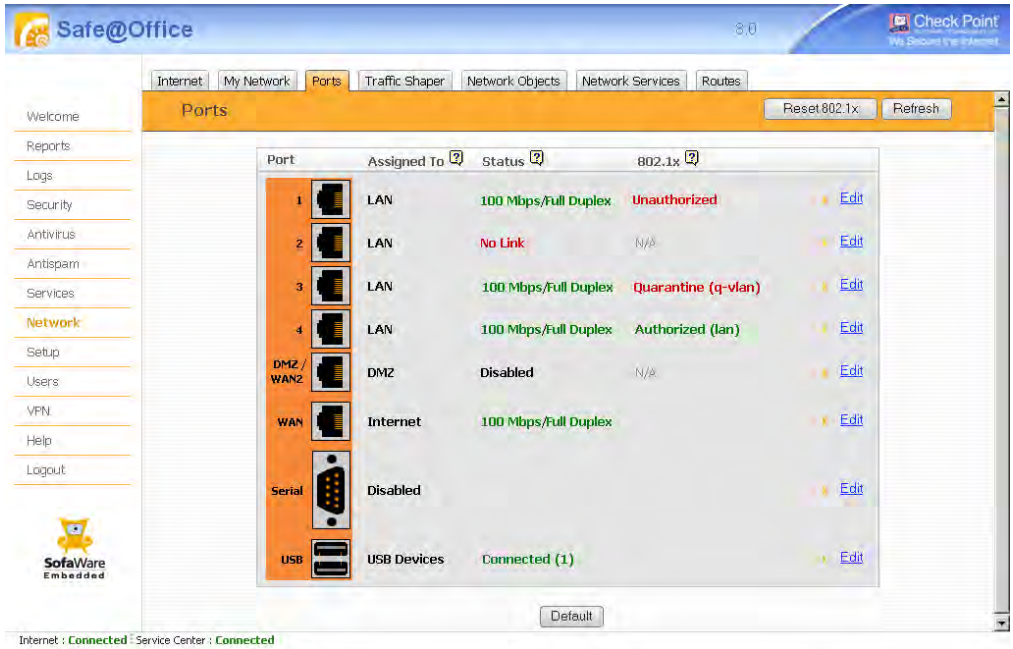
This step is only relevant when using a RADIUS server.

3. To configure a Quarantine network other than the LAN or DMZ, add a port-based VLAN network.

   See ***Adding and Editing Port-Based VLANs*** on page 178.

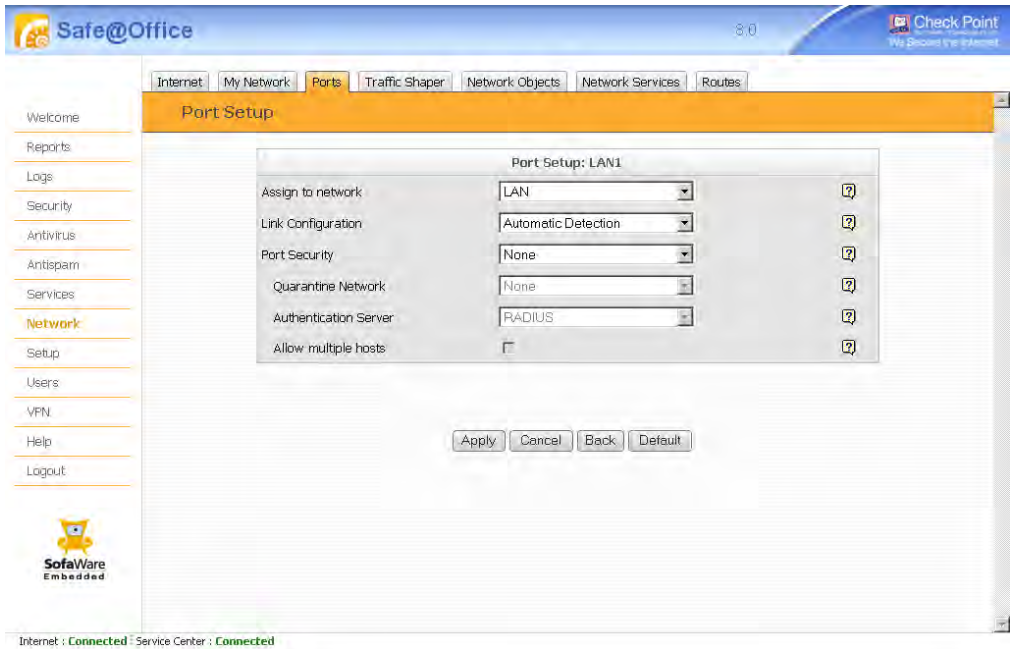
4. Click Network in the main menu, and click the Ports tab.

   The Ports page appears.



5. Next to the desired port, click Edit.

The Port Setup page appears.



6. In the Port Security drop-down list, select 802.1x.

   The Quarantine Network, Authentication Server, and Allow multiple hosts fields are enabled.

7. Complete the fields using the information in the following table.

8. Click Apply.

   A warning message appears.

9. Click OK.

Table 65: Port-Based Security Fields

In this field…	Do this…
Assign to network	Specify how the Safe@Office appliance should handle users who authenticate successfully, by selecting one of the following: • A network name. All users who authenticate to this port successfully are assigned to the specified network. • From RADIUS. Use dynamic VLAN assignment to assign users to specific networks. This option is only relevant when using a RADIUS server.
Authentication Server	Specify which authentication server you are using, by selecting one of the following: • RADIUS. A RADIUS server. • Internal User Database. The Safe@Office EAP authenticator.
Quarantine Network	Specify which network should serve as the Quarantine network, by selecting one of the following: • A network name. All users for whom authentication to this port fails are assigned to the specified network. • None. No Quarantine network is selected.

In this field…	Do this…
Allow multiple hosts	To allow multiple hosts to connect to this port, select this option. Normally, 802.1x port-based security allows only a single host to connect to each port. However, when this option is selected, multiple clients can connect to the same port via a hub or switch. Each client on the port must authenticate separately. If authentication fails for one client, then all clients on the port will be blocked. For information on cascading the Safe@Office appliance to a hub or switch, see ***Cascading Your Appliance*** on page 62. Note: Enabling this option makes 802.1x port-based security less secure. Therefore, it is recommended to enable this option only in locations where the number of ports are a limiting factor, and where an external 802.1x-capable switch cannot be installed.

Resetting 802.1x Locking

Power Pack

When 802.1x port-based security is configured for a LAN port, the first host that attempts to connect to this port is “locked” to the port. In order to connect a different computer to the port, you must first reset 802.1x locking.

To reset 802.1x locking on all ports

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

   The Ports page appears.
2. Click Reset 802.1x.

   A confirmation message appears.
3. Click OK.

   The 802.1x status of all ports is reset to "Unauthenticated".

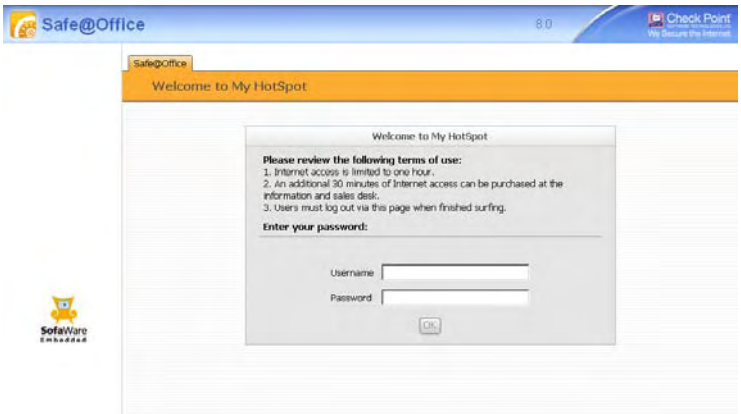
Using Secure HotSpot

Power Pack

You can enable your Safe@Office appliance as a public Internet access hotspot for specific networks. When users on those networks attempt to access the Internet, they are automatically re-directed to the My HotSpot page http://my.hotspot.

Note: You can configure Secure HotSpot to use HTTPS. In this case, the My HotSpot page will be https://my.hotspot.

On this page, users must read and accept the My HotSpot terms of use, and if My HotSpot is configured to be password-protected, they must log in using their Safe@Office username and password. The users may then access the Internet or other corporate networks.



Users can also log out in the My HotSpot page.

Note: HotSpot users are automatically logged out after one hour of inactivity. If you are using RADIUS authentication, you can change the Secure HotSpot session timeout by configuring the RADIUS Session-Timeout Attribute. See ***Using RADIUS Authentication*** on page 650.

Safe@Office Secure HotSpot is useful in any wired or wireless environment where Web-based user authentication or terms-of-use approval is required prior to gaining access to the

network. For example, Secure HotSpot can be used in public computer labs, educational institutions, libraries, Internet cafés, and so on.

The Safe@Office appliance allows you to add guest users quickly and easily. By default, guest users are given a username and password that expire in 24 hours and granted HotSpot Access permissions only. For information on adding quick guest users, see ***Adding Quick Guest Users*** on page 647.

You can choose to exclude specific network objects from HotSpot enforcement. Excluded network objects will be able to access the network without viewing the My HotSpot page. Furthermore, users will be able to access the excluded network object without viewing the My HotSpot page. For information on excluding network objects from HotSpot enforcement, see ***Using Network Objects*** on page 185.

Important: SecuRemote/SecureClient VPN software users who are authenticated by the Internal VPN Server are automatically exempt from HotSpot enforcement. This allows, for example, authenticated employees to gain full access to the corporate LAN, while guest users are permitted to access the Internet only.

Note: HotSpot enforcement can block traffic passing through the firewall; however, it does not block local traffic on the same network segment (traffic that does not pass through the firewall).

Setting Up Secure HotSpot

Power Pack

To set up Secure HotSpot

1. Enable Secure HotSpot for the desired networks.

   See ***Enabling/Disabling Secure HotSpot*** on page 382.

2. Customize Secure HotSpot as desired.

   See ***Customizing Secure HotSpot*** on page 384.

3. Grant HotSpot Access permissions to users on the selected networks.

   See ***Adding and Editing Users*** on page 643.

4. To exclude specific computers from Secure HotSpot enforcement, add or edit their network objects.

   See ***Adding and Editing Network Objects*** on page 187.

   You must select Exclude this computer/network from HotSpot enforcement option.

5. Add quick guest users as needed.

   See ***Adding Quick Guest Users*** on page 647.

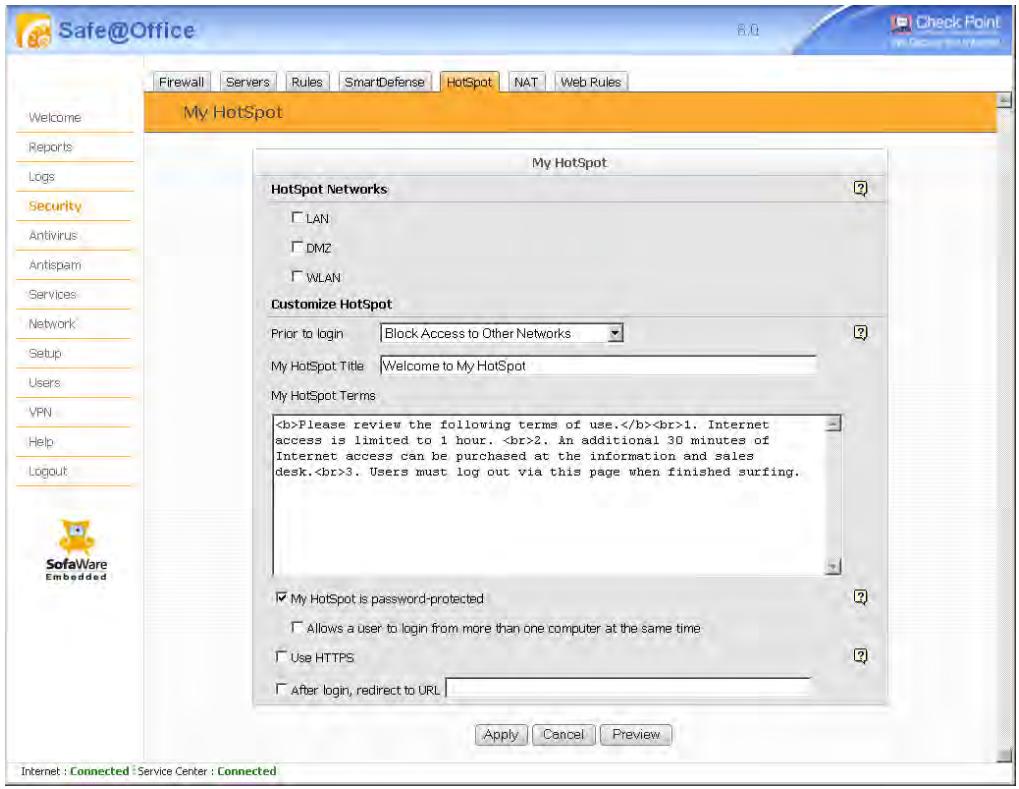
Enabling/Disabling Secure HotSpot

Power Pack

To enable/disable Secure HotSpot

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

The My HotSpot page appears.



2. In the HotSpot Networks area, do one of the following:

   - To enable Secure HotSpot for a specific network, select the check box next to the network.
   - To disable Secure HotSpot for a specific network, clear the check box next to the network.

3. Click Apply.

Customizing Secure HotSpot

Power Pack

To customize Secure HotSpot

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

   The My HotSpot page appears.
2. Complete the fields using the information in the following table.
3. To preview the My HotSpot page, click Preview.

   A browser window opens displaying the My HotSpot page.
4. Click Apply.

   Your changes are saved.

Table 66: My HotSpot Fields

In this field…	Do this…
Prior to login	Specify the degree of access to grant users who have not yet logged in to Secure HotSpot or for whom authentication failed, by selecting one of the following: • Block Access to Other Networks. Users cannot access internal networks, the Internet, or VPN. This is the default. • Block Access to External Networks Only. Users can access internal networks, but not the Internet or VPN. • Block Access to VPN Only. Users can access internal networks and the Internet, but not VPN.
My HotSpot Title	Type the title that should appear on the My HotSpot page. The default title is "Welcome to My HotSpot".

In this field…	Do this…
My HotSpot Terms	Type the terms to which the user must agree before accessing the Internet. You can use HTML tags as needed.
My HotSpot is password-protected	Select this option to require users to enter their username and password before accessing the Internet. If this option is not selected, users will be required only to accept the terms of use before accessing the network. The Allow a user to login from more than one computer at the same time check box appears.
Allow a user to login from more than one computer at the same time	Select this option to allow a single user to log in to My HotSpot from multiple computers at the same time.
Use HTTPS	Select this option to use HTTPS for Secure HotSpot.
After login, redirect to URL	To redirect users to a specific URL after logging in to My HotSpot, select this option and type the desired URL in the field provided. For example, you can redirect authenticated users to your company's Web site or a "Welcome" page.

Using NAT Rules

500

Overview

In an IP network, each computer is assigned a unique IP address that defines both the host and the network. A computer's IP address can be public and Internet-routable, or private and non-routable. Since IPv4, the current version of IP, provides only 32 bits of address space, available public IP addresses are becoming scarce, most having already been assigned. Internet Service Providers will usually allocate only one or a few public IP addresses at a time, and while larger companies may purchase several such addresses for use, purchasing addresses for every computer on the network is usually impossible.

Due to the lack of available public IP addresses, most computers in an organization are assigned private, non-routable IP addresses. Even if more public IP addresses became available, changing the private IP address of every machine in a large network to a public IP address would be an administrative nightmare, being both labor intensive and time consuming. Therefore, organization's computers will most likely remain with private, non-routable IP addresses, even though in most cases they require access to the Internet.

In addition to the issue of arranging Internet access for computers with non-routable IP addresses, IP networks present a security challenge. Since making a network’s internal addresses public knowledge can reveal the topology of the entire network, the network administrator may want to conceal both routable and non-routable IP addresses from outside the organization, or even from other parts of the same organization, in order to enhance security.

The Safe@Office appliance solves both issues through the use of Network Address Translation (NAT) rules. A NAT rule is a setting used to change the source, destination, and/or service of specific connections.

Supported NAT Rule Types

The Safe@Office appliance enables you to define the following types of *custom NAT rules*:

- Static NAT (or One-to-One NAT). Translation of an IP address range to another IP address range of the same size.

  This type of NAT rule allows the mapping of Internet IP addresses or address ranges to hosts inside the internal network. This is useful if you want each computer in your private network to have its own Internet IP addresses.

- Hide NAT (or Many-to-One NAT). Translation of an IP address range to a single IP address.

  This type of NAT rule 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. For more information on Hide NAT, see ***How Does Hide NAT Work?*** on page 388.

- Few-to-Many NAT. Translation of a smaller IP address range to a larger IP address range.

  When this type of NAT rule is used, static NAT is used to map the IP addresses in the smaller range to the IP addresses at the beginning of the larger range. The remaining IP addresses in the larger range remain unused.

- Many-to-Few NAT. Translation of a larger IP address range to a smaller IP address range.

  When this type of NAT rule is used, static NAT is used to map the IP addresses in the larger range to all but the final IP address in the smaller range. Hide NAT is then used to map all of the remaining IP addresses in the larger range to the final IP address in the smaller range.

- Service-Based NAT. Translation of a connection's original service to a different service.

The Safe@Office appliance also supports *implicitly defined NAT rules*. Such rules are created automatically upon the following events:

- Hide NAT is enabled on an internal network
- An Allow and Forward firewall rule is defined