Check Point ZoneAlarm

Secure Wireless Router Z100G

User Guide

Version 7.5

August 2007

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 router. Failure to follow these instructions may result in damage to equipment and/or personal injuries.

- Before cleaning the router, unplug the power cord. Use only a soft cloth dampened with water for cleaning.
- When installing the router, 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 router outdoors.
- Do not expose the router to liquid or moisture.
- Do not expose the router to extreme high or low temperatures.
- Do not disassemble or open the router. 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 router 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 manual easier, some types of information are marked with special symbols or formatting.

Boldface type is used for command and button names.

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

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

Chapter 1

Introduction

This chapter introduces the Check Point ZoneAlarm Secure Wireless Router Z100G and this guide.

This chapter includes the following topics:

About Your Check Point ZoneAlarm Router

The Check Point ZoneAlarm Secure Wireless Router Z100G is a unified threat management (UTM) router, developed and supported by SofaWare Technologies, an affiliate of Check Point Software Technologies, the worldwide leader in securing the Internet. The ZoneAlarm router enables secure high-speed Internet access from the home or home office for both wired and wireless devices, while the ZoneAlarm 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 ZoneAlarm router also allows sharing your Internet connection among several PCs or other network devices, enabling advanced home networking and saving the cost of purchasing static IP addresses.

With the ZoneAlarm router, 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 ZoneAlarm router allows you to securely connect to your home or home office network.

Product Features

Table 1: ZoneAlarm Z100G Features

Feature	ZoneAlarm Z100G
Concurrent Users	5 (Upgradable to 15)
Capacity	
Firewall Throughput	70 Mbps
VPN Throughput	5 Mbps
Concurrent Firewall Connections	4,000
Hardware Features	
4-Port LAN Switch	10/100 Mbps
WAN Port	10/100 Mbps
Print Server	✓
USB 2.0 Ports	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 (H.323) Support	✓
INSPECT Engine	✓
Instant Messenger Blocking / Monitoring	✓
P2P File Sharing Blocking / Monitoring	✓
Web Rules	✓
VPN	
Remote Access Users	1
VPN Server	SecuRemote
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
Transparent Bridge Mode	✓

Spanning Tree Protocol (STP)	✓
Traffic Monitoring	✓
DHCP Server, Client, and Relay	✓
MAC Cloning	✓
Static NAT	✓
Ethernet Cable Type Recognition	✓
Wireless	
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
Wireless QoS (WMM)	✓
Dual Diversity Antennas	✓
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
Management	
Central Management	SofaWare SMP
Local Management	HTTP / HTTPS
Remote Desktop	Integrated Microsoft Terminal Services Client

Local Diagnostics Tools	Ping, WHOIS, Packet Sniffer, VPN Tunnel Monitor, Connection Table Monitor, Wireless Monitor, My Computers Display
NTP Automatic Time Setting	✓
TFTP Rapid Deployment	✓
Hardware Specifications	
Power	100/110/120/210/220/230VAC (Linear Power Adapter) or 100~240VAC (Switched Power Adapter)
Mounting Options	Desktop or Wall Mounting
Warranty	1 Year Hardware

* 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 ZoneAlarm 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, go to www.zonelabs.com/z100g.

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 ZoneAlarm Portal, disable any pop-up blockers for http://my.firewall.

Getting to Know Your ZoneAlarm Z100G Router

Package Contents

The ZoneAlarm Z100G package includes the following:

- ZoneAlarm Z100G Secure Wireless Router
- Power supply
- CAT5 Straight-through Ethernet cable
- Getting Started Guide
- Resources CD-ROM
- Wall mounting kit
- Two antennas

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 ZoneAlarm router.

Figure 1: ZoneAlarm Z100G Router Rear Panel

The following table lists the ZoneAlarm Z100G router's rear panel elements.

Table 2: ZoneAlarm Z100G Router 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 ZoneAlarm router or resetting the ZoneAlarm router to its factory defaults. You need to use a pointed object to press this button. • Short press. Reboots the ZoneAlarm router • Long press (7 seconds). Resets the ZoneAlarm router to its factory defaults, and resets your firmware to the version that shipped with the ZoneAlarm router. 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 ZoneAlarm router. Do not reset the unit without consulting your system administrator.
USB	Two USB 2.0 ports used for connecting USB-based printers
WAN	Wide Area Network: An Ethernet port (RJ-45) used for connecting your cable or DSL modem, or for connecting a hub when setting up more than one Internet connection
LAN 1-4	Local Area Network switch: Four Ethernet ports (RJ-45) used for connecting computers or other network devices
ANT 1/ ANT 2	Antenna connectors, used to connect the supplied wireless antennas

Front Panel

The ZoneAlarm Z100G router includes several status LEDs that enable you to monitor the router's operation.

Figure 2: ZoneAlarm Z100G Router Front Panel

For an explanation of the ZoneAlarm Z100G router's status LEDs, see the following table.

Table 3: ZoneAlarm Z100G Router Status LEDs

LED	State	Explanation
PWR/SEC	Off	Power off
	Flashing quickly (Green)	System boot-up
	Flashing slowly (Green)	Establishing Internet connection
	Flashing (Red)	Hacker attack blocked
	On (Green)	Normal operation
	On (Red)	Error
	Flashing (Orange)	Software update in progress
LAN 1-4/ WAN	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

LED	State	Explanation
	LNK/ACT Flashing	Data is being transmitted/received
VPN	Off	No VPN activity
	Flashing (Green)	VPN activity
	On (Green)	VPN tunnels established, no activity
USB	Off	No USB port activity
	Flashing (Green)	USB port activity
WLAN	Off	No WLAN activity
	Flashing (Green)	WLAN activity

Contacting Technical Support

If there is a problem with your ZoneAlarm router, see http://www.sofaware.com/support. You can also download the latest version of this guide from the site.

Chapter 2

The ZoneAlarm Firewall

This chapter introduces the ZoneAlarm firewall and its advantages.

This chapter includes the following topics:

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 4: 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 5: 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.

ZoneAlarm routers use Stateful Inspection technology to analyze all packet communication layers and extract the relevant communication and application state information. The ZoneAlarm router 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 ZoneAlarm 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 ZoneAlarm 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 6: 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

Step	Channel Type	Description	Source	TCP Source Port	Destination	TCP Destination Port
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.

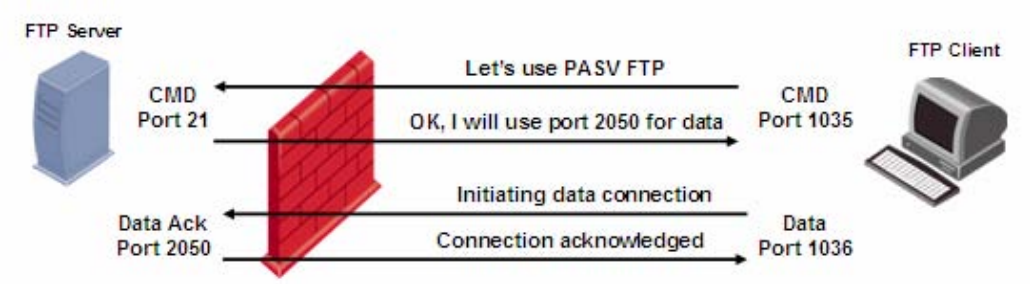


Figure 3: Establishment of Passive FTP Connection

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 7: 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 ZoneAlarm router provides true Stateful Inspection.

Chapter 3

Installing and Setting Up ZoneAlarm

This chapter describes how to properly set up and install your ZoneAlarm router in your networking environment.

This chapter includes the following topics:

Before You Install the ZoneAlarm Router

Prior to connecting and setting up your ZoneAlarm router 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.

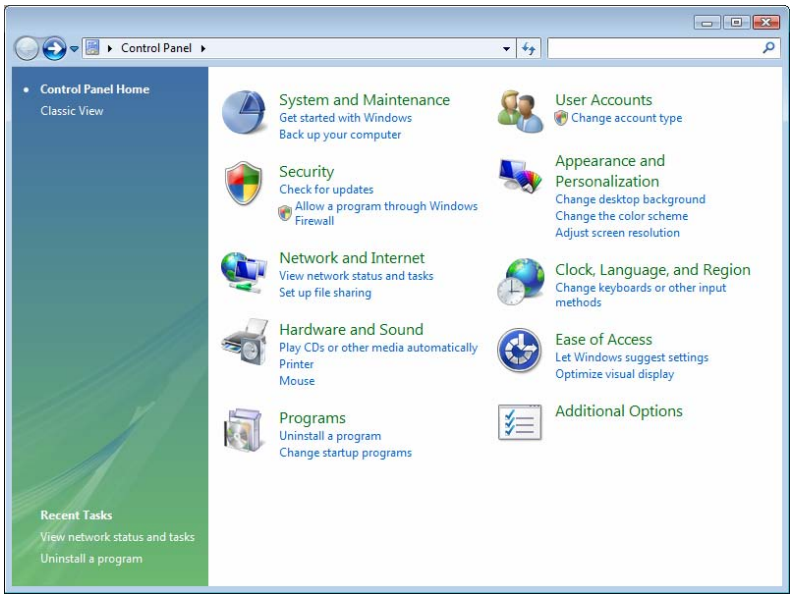
Refer to the relevant section in this guide in accordance with the operating system that runs on your computer. The sections below will guide you through the TCP/IP setup and installation process.

Windows Vista

Checking the TCP/IP Installation

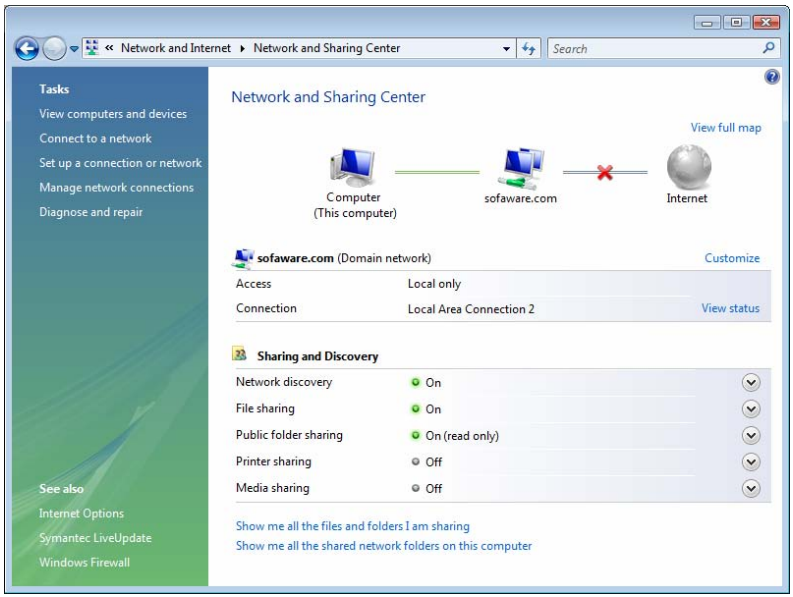
1. Click Start > Control Panel.

   The Control Panel window appears.



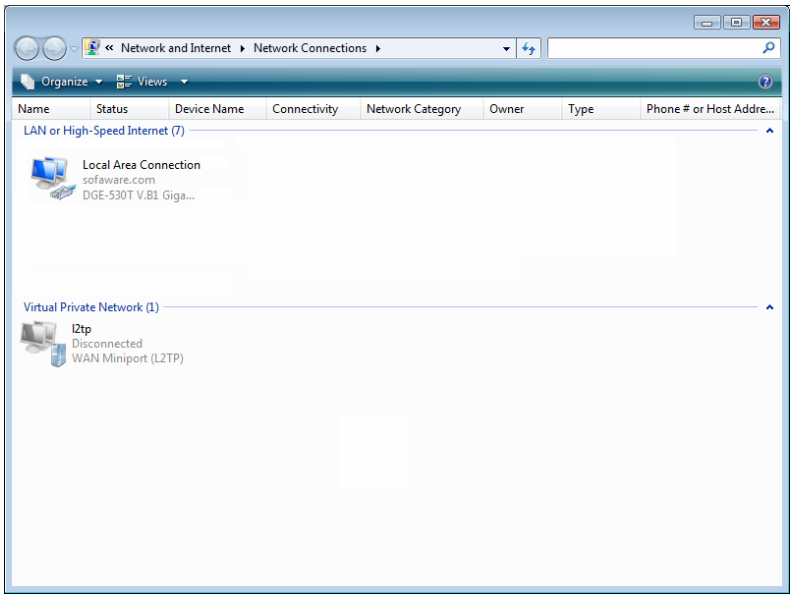
2. Under Network and Internet, click View network status and tasks.

The Network Sharing Center screen appears.



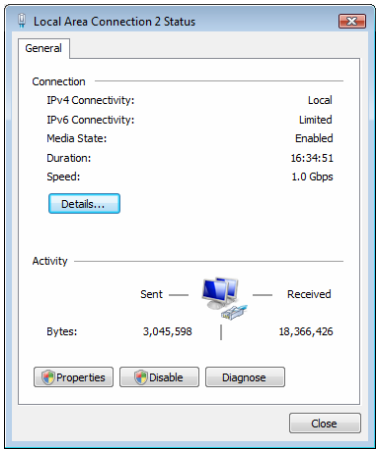
3. In the Tasks pane, click Manage network connections.

The Network Connections screen appears.



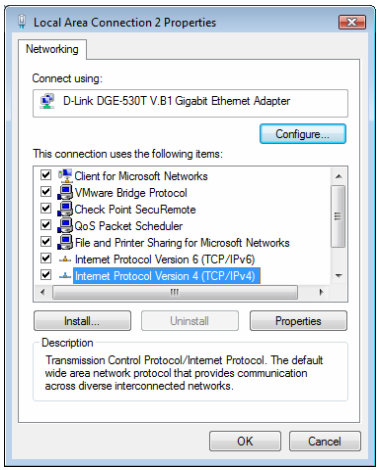
4. Double-click the Local Area Connection icon.

   The Local Area Connection Status window opens.



5. Click Properties.

The Local Area Connection Properties window opens.

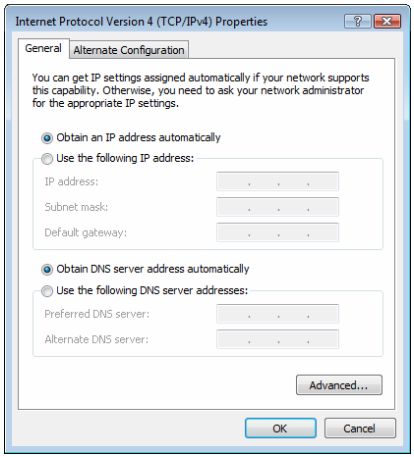


6. Check if Internet Protocol Version 4 (TCP/IPv4) appears in the list box and if it is properly configured with the Ethernet card installed on your computer.

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.

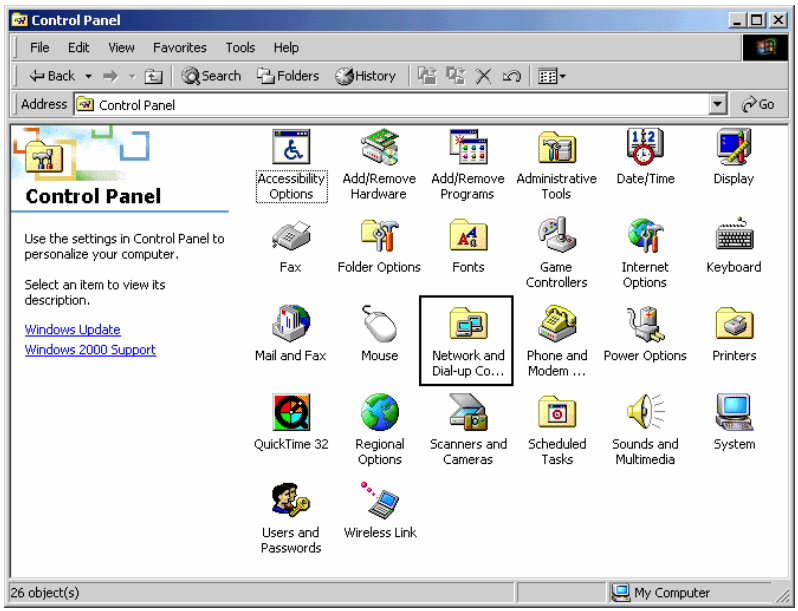
   Your computer is now ready to access your ZoneAlarm router.

Windows 2000/XP

Checking the TCP/IP Installation

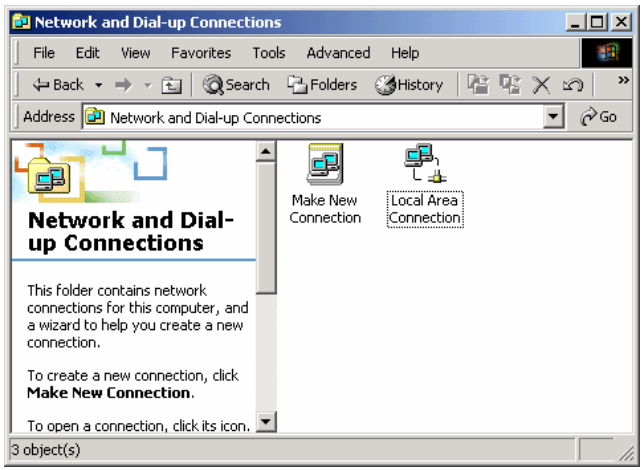
1. Click Start > Settings > Control Panel.

   The Control Panel window appears.



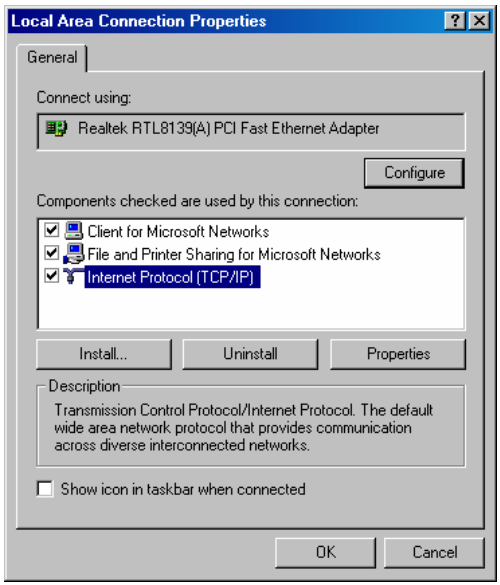
2. Double-click the Network and Dial-up Connections icon.

   The Network and Dial-up Connections window appears.



3. Right-click the Local Area Connection icon and select Properties from the pop-up menu that opens.

The Local Area Connection Properties window appears.

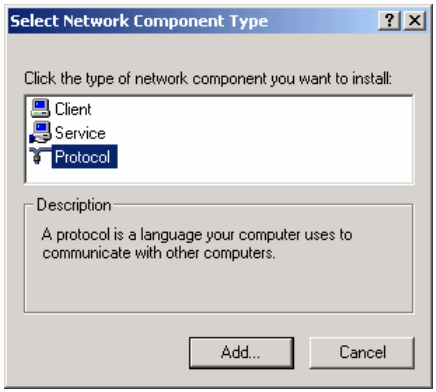


4. In the above window, check if TCP/IP appears in the components list and if it is properly configured with the Ethernet card installed on your computer. If TCP/IP does not appear in the Components list, you must install it as described in the next section.

Installing TCP/IP Protocol

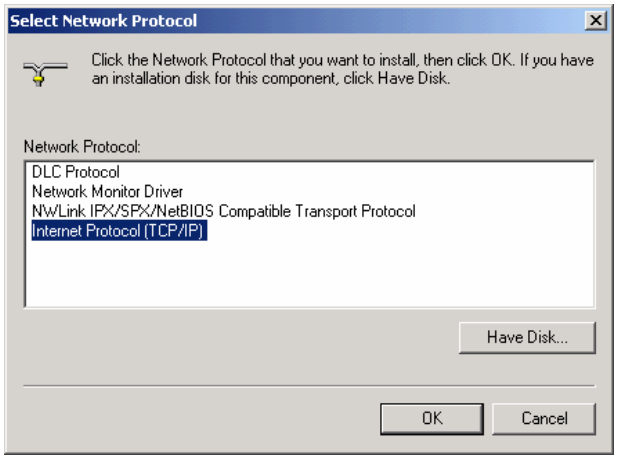
1. In the Local Area Connection Properties window click Install.

   The Select Network Component Type window appears.



2. Select Protocol and click Add.

   The Select Network Protocol window appears.



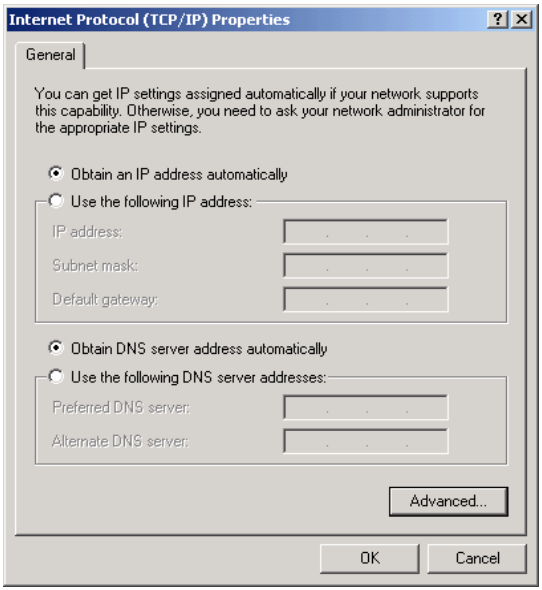
3. Choose Internet Protocol (TCP/IP) and click OK.

   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.

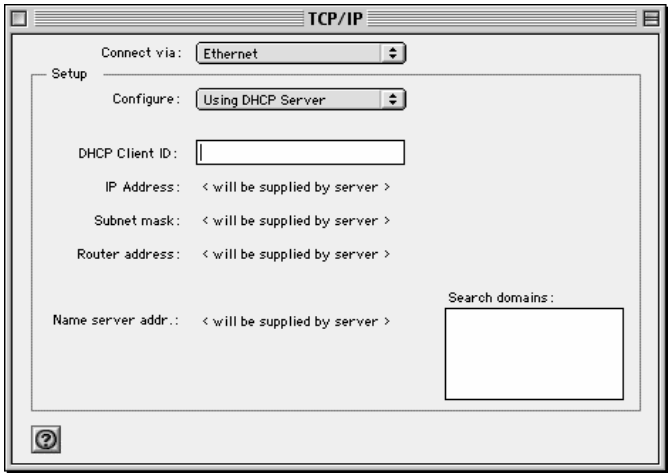
   Your computer is now ready to access your ZoneAlarm router.

Mac OS

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

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

   The TCP/IP window appears.



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

Mac OS-X

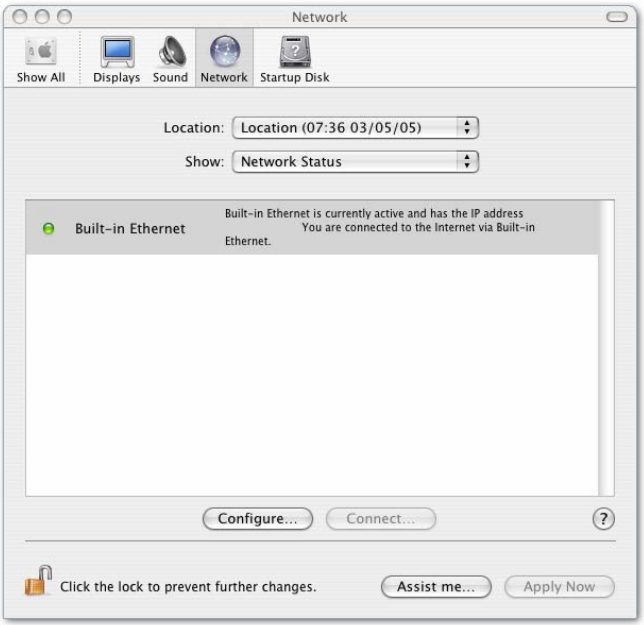
Use the following procedure for setting up the TCP/IP Protocol.

1. Choose Apple -> System Preferences.

   The System Preferences window appears.

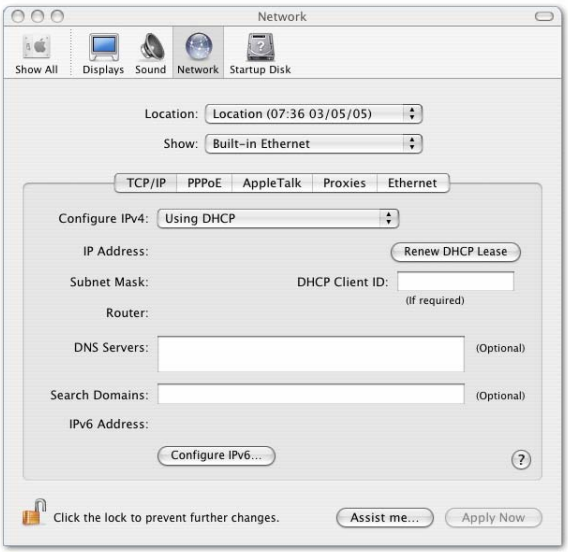
2. Click Network.

   The Network window appears.



3. Click **Configure.**

TCP/IP configuration fields appear.



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

Wall Mounting the ZoneAlarm Router

For your convenience, the ZoneAlarm router includes a wall mounting kit, which consists of two plastic conical anchors and two cross-head screws.

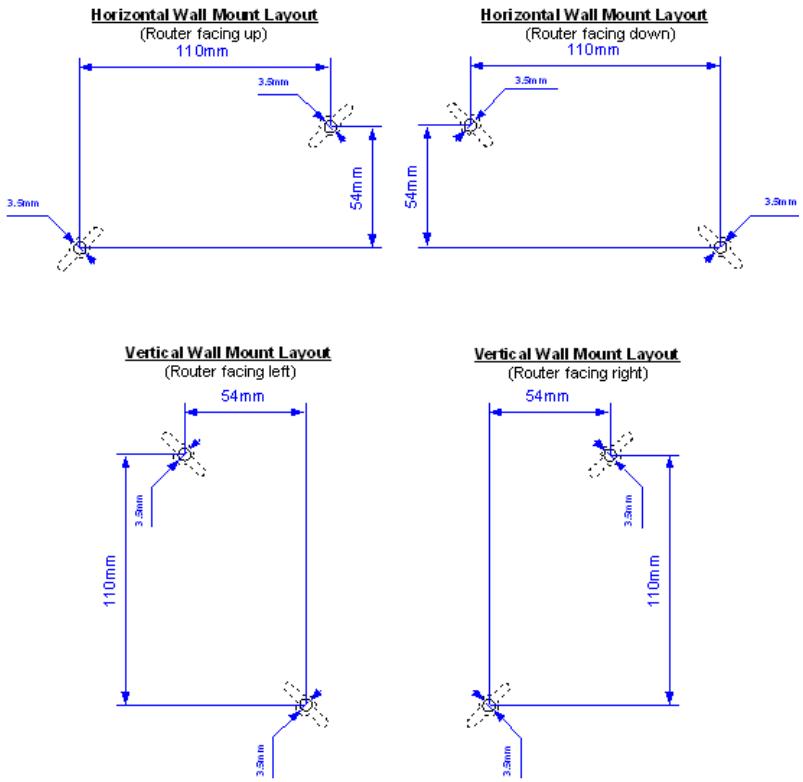
To mount the ZoneAlarm router on the wall

1. Decide where you want to mount your ZoneAlarm router.
2. Decide on the mounting orientation.

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

Note: Mounting the router 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 ZoneAlarm router are suitable for concrete walls. If you want to mount the router on a plaster wall, you must use anchors that are suitable for plaster walls.

6. Insert the two screws you received with your ZoneAlarm router into the plastic conical anchors, and turn them until they protrude approximately 5 mm from the wall.
7. Align the holes on the ZoneAlarm router's underside with the screws on the wall, then push the router in and down.

   Your ZoneAlarm router is wall mounted. You can now connect it to your computer.

Securing the ZoneAlarm Router against Theft

The ZoneAlarm router features a security slot to the rear of the right panel, which enables you to secure your router 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 router. A looped security cable typically includes the parts shown in the diagram below.

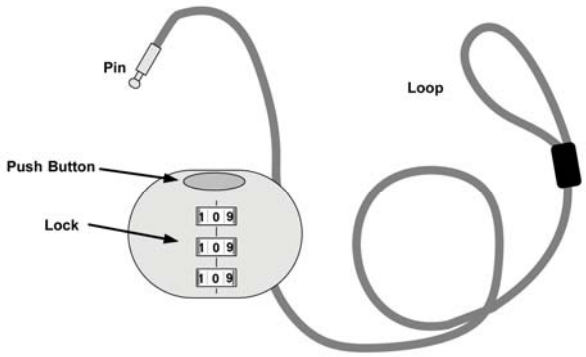


Figure 4: Looped Security Cable

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

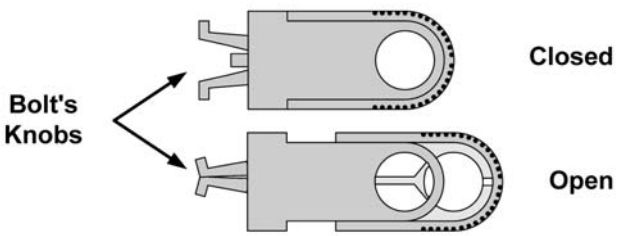
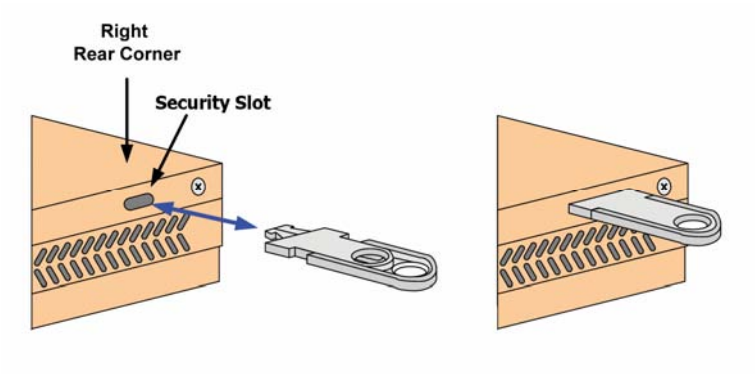


Figure 5: Looped Security Cable Bolt

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

To install an anti-theft device on the ZoneAlarm router

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 ZoneAlarm router'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.

Router Installation

Installing the ZoneAlarm Router

To install the ZoneAlarm router

1. Verify that you have the correct cable type.

   For information, see ***Network Requirements*** on page 7.

2. Connect the LAN cable:

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

3. Connect the WAN cable:

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

4. Connect the power supply to the power socket, labeled PWR, at the back of the ZoneAlarm router.
5. Plug the power supply into the wall electrical outlet.

Warning: The ZoneAlarm router 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.

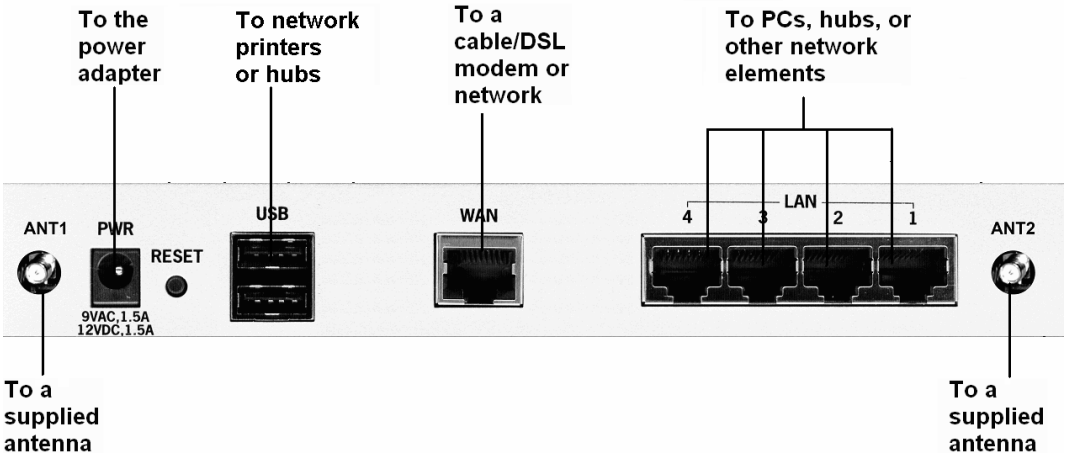


Figure 6: Typical Connection Diagram

Cascading Your Router

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

To cascade the ZoneAlarm router to a hub or switch

1. Connect a standard Ethernet cable to one of the router's LAN ports.

   The ZoneAlarm router 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 Router for a Wireless Connection

To prepare the ZoneAlarm router for a wireless connection

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

Connecting the Router to Network Printers

You can connect network printers to your ZoneAlarm Z100G router.

To connect network printers

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

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

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

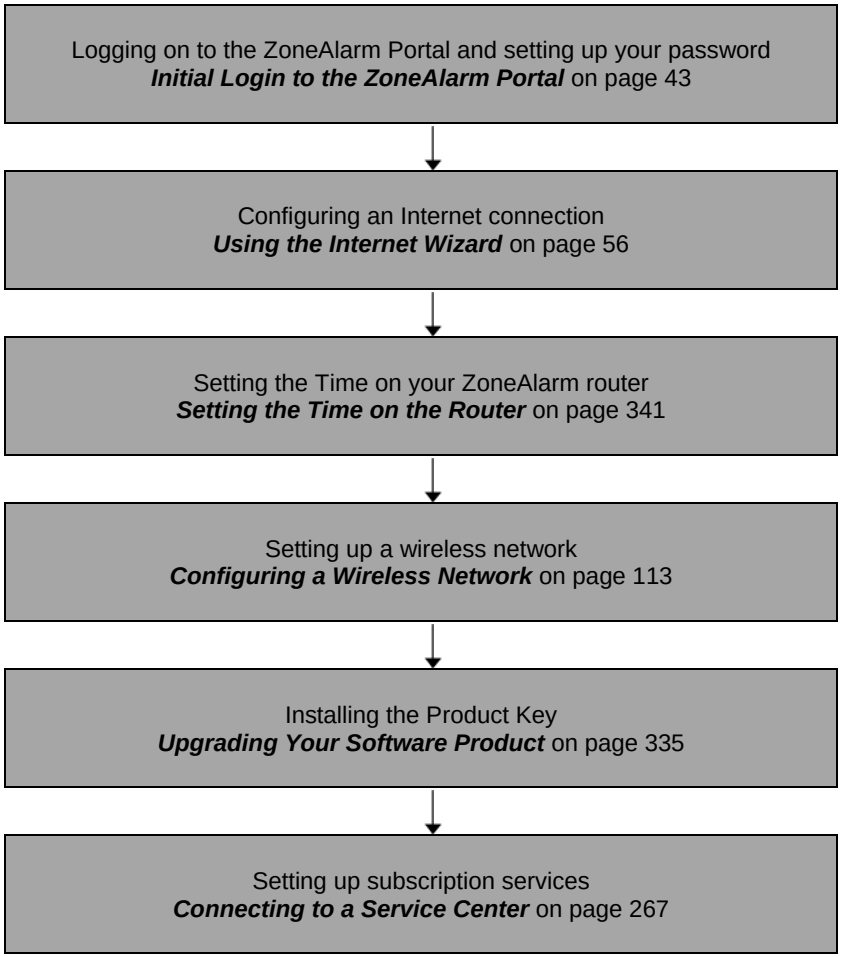
Warning: Verify that the USB devices' power requirement does not exceed the router's USB power supply capabilities. Failure to observe this warning may cause damage to the router and void the warranty.

For information on setting up network printers, see ***Setting up Network Printers*** on page 368.

Setting Up the ZoneAlarm Router

After you have installed the ZoneAlarm router, you must set it up using the steps shown below.

When setting up your ZoneAlarm router for the first time after installation, these steps follow each other automatically. After you have logged on and set up your password, the ZoneAlarm 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.

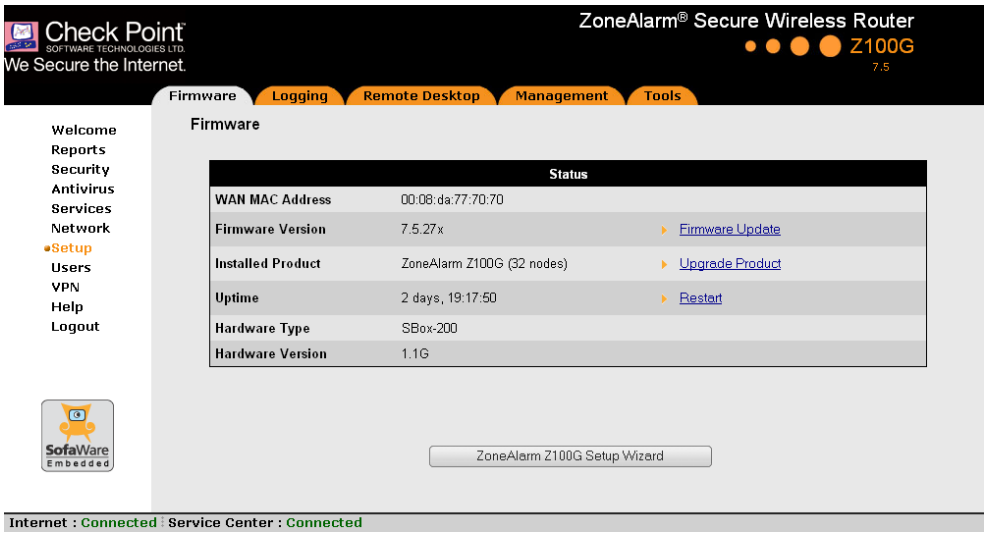


You can access the Setup Wizard at any time after initial setup, using the procedure below.

To access the Setup Wizard

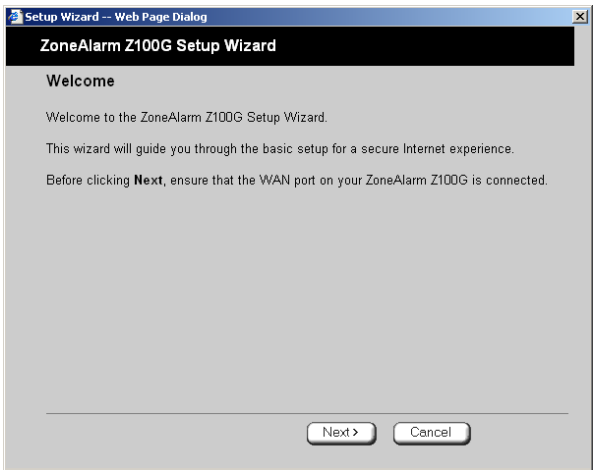
1. Click Setup in the main menu, and click the Firmware tab.

The Firmware page appears.



2. Click ZoneAlarm Setup Wizard.

   The ZoneAlarm 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 ZoneAlarm router.

This chapter includes the following topics:

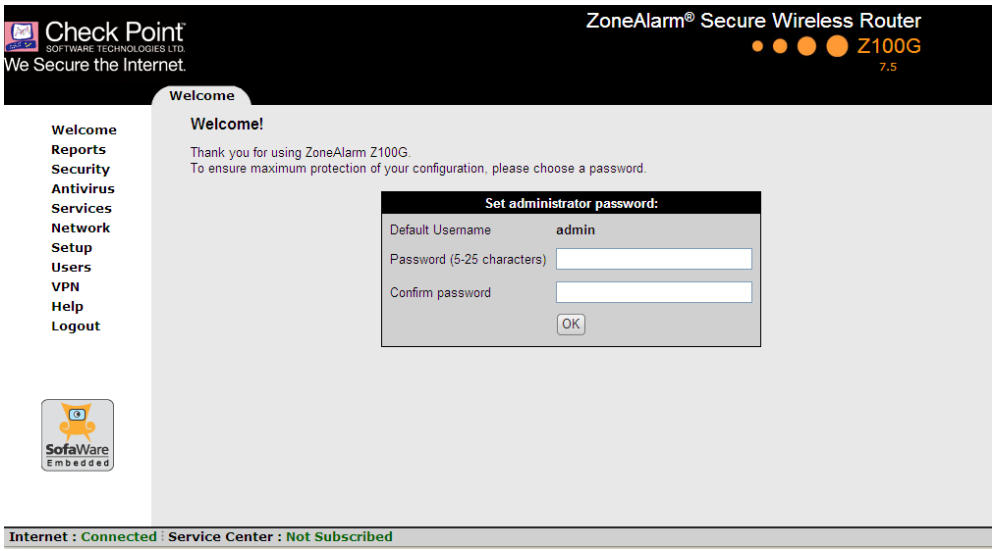
Initial Login to the ZoneAlarm Portal

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

To log on to the ZoneAlarm Portal for the first time

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

The initial login page appears.



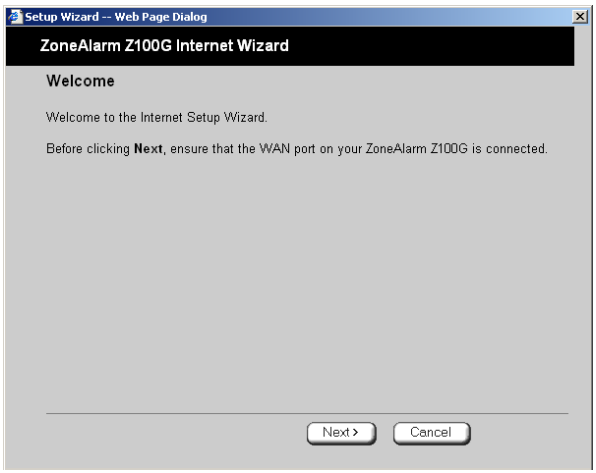
2. Type a password both in the Password and the Confirm password fields.

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 311.

3. Click OK.

The ZoneAlarm 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 56.

     After you have completed the Internet Wizard, the Setup Wizard continues to guide you through router setup. For more information, see ***Setting Up the ZoneAlarm Router*** on page 39.

   - Internet Setup

     Internet Setup offers advanced setup options. To use Internet Setup, click Cancel and refer to ***Using Internet Setup*** on page 64.

Logging on to the ZoneAlarm Portal

Note: By default, HTTP and HTTPS access to the ZoneAlarm 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 172.

  Or

- Enable HTTPS access from the Internet. See ***Configuring HTTPS*** on page 338.

To log on to the ZoneAlarm Portal

1. Do one of the following:

   - Browse to http://my.firewall.

     Or

   - To log on through HTTPS (locally or remotely), follow the procedure ***Accessing the ZoneAlarm Portal Remotely*** on page 47.

   The login page appears.

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

   The Welcome page appears.

Accessing the ZoneAlarm Portal Remotely Using HTTPS

You can access the ZoneAlarm 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 ZoneAlarm Portal from your internal network.

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

- Configure your password, using HTTP. See ***Initial Login to the ZoneAlarm Portal*** on page 43.
- Configure HTTPS Remote Access. See ***Configuring HTTPS*** on page 338.

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 ZoneAlarm Portal from your internal network

- Browse to https://my.firewall.

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

  The ZoneAlarm Portal appears.

To access the ZoneAlarm 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 ZoneAlarm Portal through HTTPS, the certificate in the ZoneAlarm router 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 ZoneAlarm router. 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 ZoneAlarm Portal appears.

Using the ZoneAlarm Portal

The ZoneAlarm Portal is a Web-based management interface, which enables you to manage and configure the ZoneAlarm router operation and options.

The ZoneAlarm Portal consists of three major elements.

Table 8: ZoneAlarm 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.

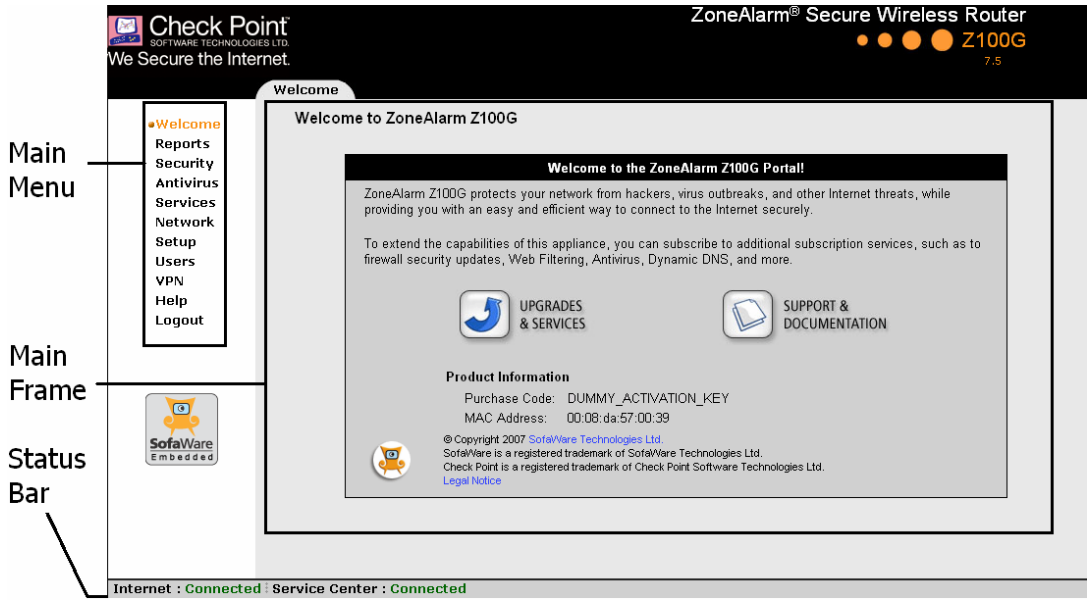


Figure 7: ZoneAlarm Portal

Main Menu

The main menu includes the following submenus.

Table 9: Main Menu Submenus

This submenu…	Does this…
Welcome	Displays general welcome information.
Reports	Provides reporting capabilities in terms of event logging, traffic monitoring, active computers, and established connections.
Security	Provides controls and options for setting the security of any computer in the network.

This submenu…	Does this…
Antivirus	Allows you to configure VStream Antivirus settings.
Services	Allows you to control your subscription to subscription services.
Network	Allows you to manage and configure your network settings and Internet connection.
Setup	Provides a set of tools for managing your ZoneAlarm router. Allows you to upgrade your license and firmware and to configure HTTPS access to your ZoneAlarm router.
Users	Allows you to manage ZoneAlarm router users.
VPN	Allows you to configure VPN settings.
Help	Provides context-sensitive help.
Logout	Allows you to log off of the ZoneAlarm Portal.

Main Frame

The main frame displays the relevant data and controls pertaining to the menu and tab you select.

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 10: Status Bar Fields

This field…	Displays this…
Internet	Your Internet connection status. The connection status may be one of the following: • Connected. The ZoneAlarm router is connected to the Internet. • Not Connected. The Internet connection is down. • Establishing Connection. The ZoneAlarm router is connecting to the Internet. • Contacting Gateway. The ZoneAlarm router is trying to contact the Internet default gateway. • Disabled. The Internet connection has been manually disabled.
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 ZoneAlarm router failed to connect to the Service Center. • Connecting. The ZoneAlarm router is connecting to the Service Center. • Connected. You are connected to the Service Center, and security services are active.

Logging off

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

To log off of the ZoneAlarm Portal

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

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

Chapter 5

Configuring the Internet Connection

This chapter describes how to configure and work with a ZoneAlarm Internet connection.

This chapter includes the following topics:

Overview

In order to access the Internet through your ZoneAlarm router, you must configure an Ethernet-based connection on the WAN port. The Ethernet-based connection can be connected to another network by means of a switch, a router, a bridge, or an Ethernet-enabled broadband modem.

You can configure your Internet connection using any of the following setup tools:

- Setup Wizard. Guides you through the ZoneAlarm router 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 ZoneAlarm Router*** on page 39.
- Internet Wizard. Guides you through the Internet connection configuration process step by step. For further information, see ***Using the Internet Wizard*** on page 56.
- Internet Setup. Offers advanced setup options. For further information, see ***Using Internet Setup*** on page 64.

Using the Internet Wizard

The Internet Wizard allows you to configure your ZoneAlarm router for Internet connection quickly and easily through its user-friendly interface.

Note: The first time you log on to the ZoneAlarm 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.

To configure the Internet connection using the Internet Wizard

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

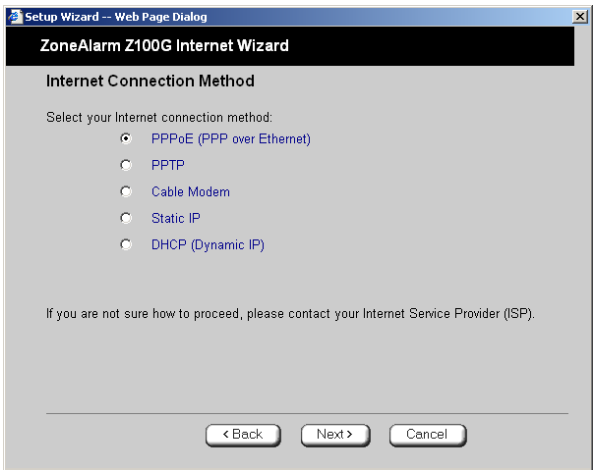
   The Internet page appears.

2. Click Internet Wizard.

   The Internet Wizard opens with the Welcome page displayed.

3. Click Next.

The Internet Connection Method dialog box appears.



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

   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 58.

   If you chose PPTP, continue at ***Using a PPTP Connection*** on page 60.

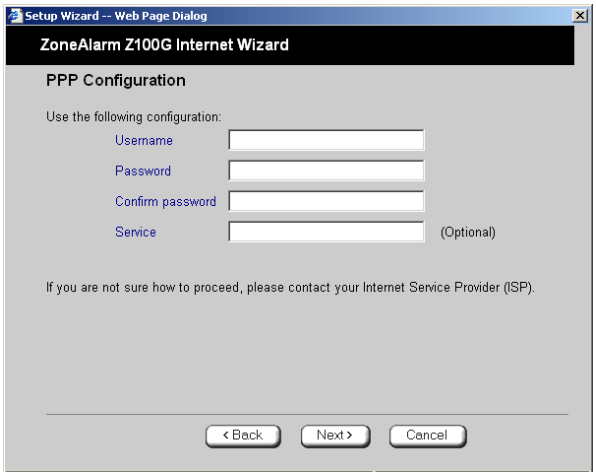
   If you chose Cable Modem, continue at ***Using a Cable Modem Connection*** on page 61.

   If you chose Static IP, continue at ***Using a Static IP Connection*** on page 62.

   If you chose DHCP, continue at ***Using a DHCP Connection*** on page 63.

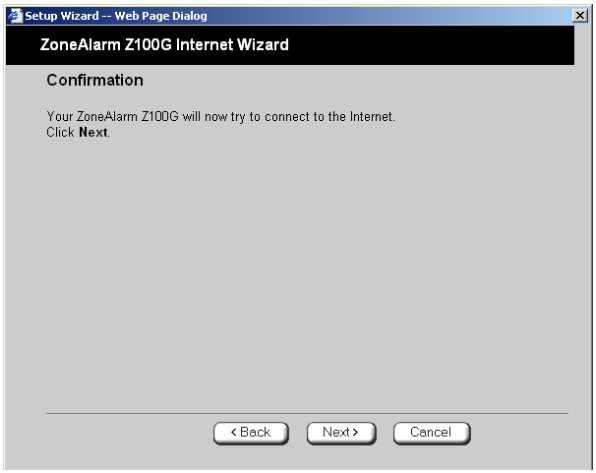
Using a PPPoE Connection

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.

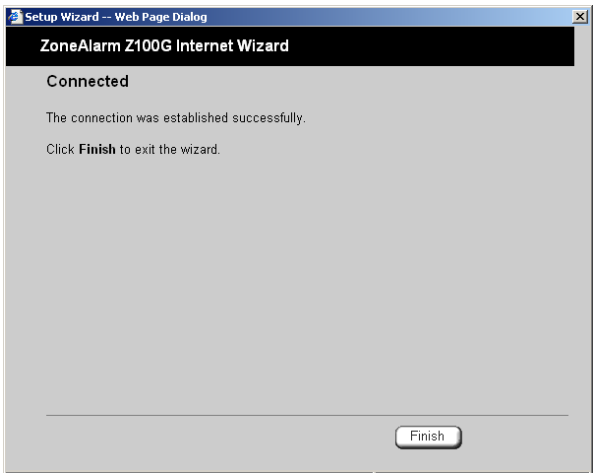


3. Click Next.

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.



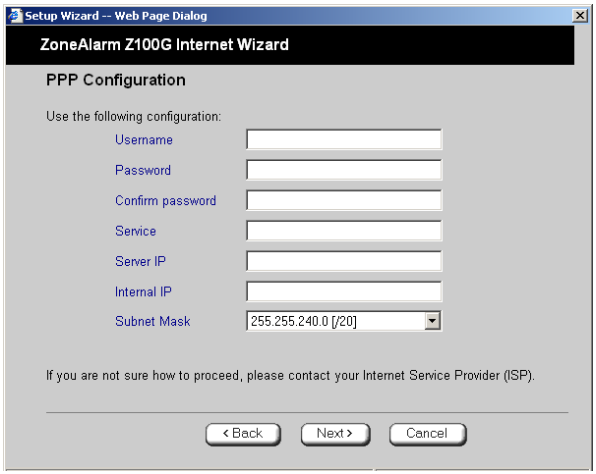
4. Click Finish.

Table 11: 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 12: 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.

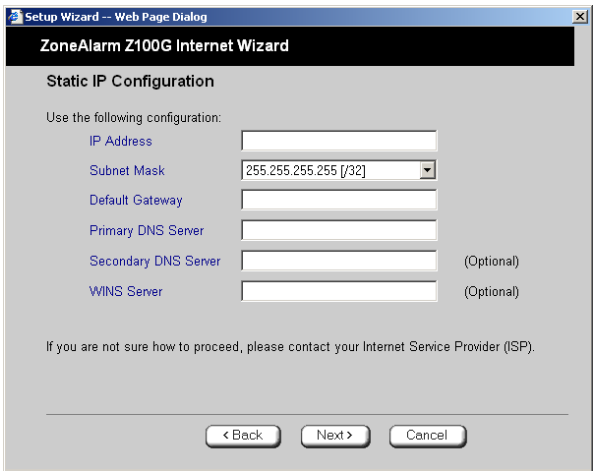
   The Connecting... screen appears.

   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 13: PPPoE Connection Fields

In this field…	Do this…
IP Address	Type the static IP address of your ZoneAlarm router.
Subnet Mask	Select the subnet mask that applies to the static IP address of your ZoneAlarm router.
Default Gateway	Type the IP address of your ISP's default gateway.
Primary DNS Server	Type the Primary DNS server IP address.
Secondary DNS Server	Type the Secondary DNS server IP address. This field is optional.
WINS Server	Type the WINS server IP address. 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.

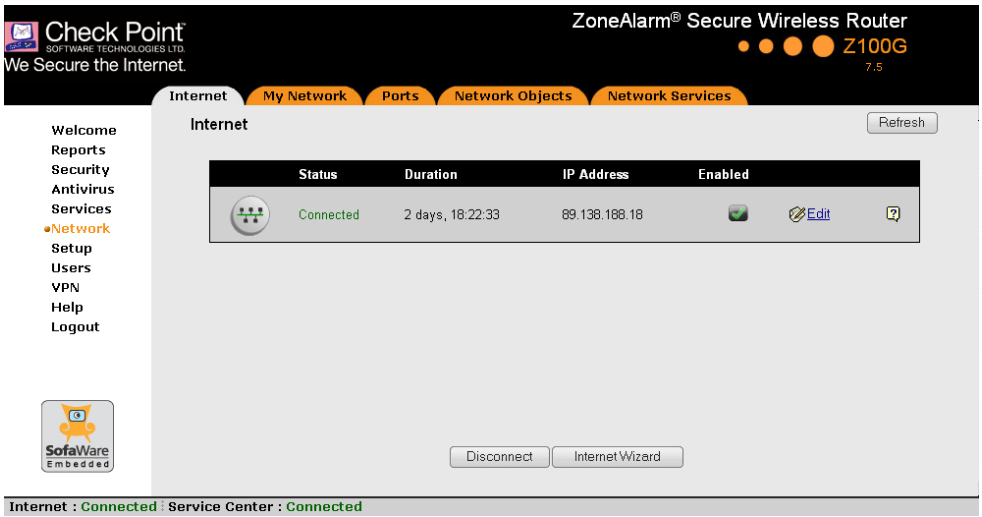
Using Internet Setup

Internet Setup allows you to manually configure your Internet connection.

To configure the Internet connection using Internet Setup

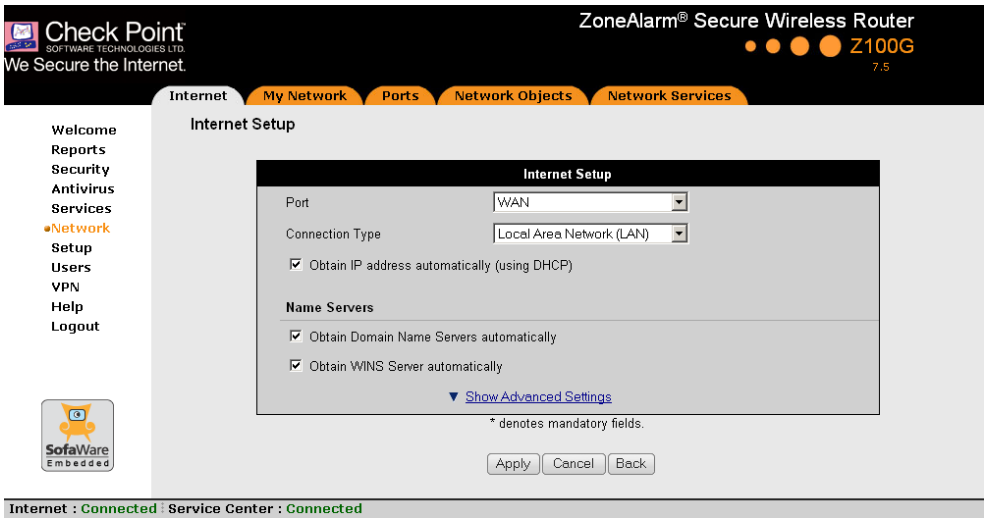
1. Click Network in the main menu, and click the Internet tab.

   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 Ethernet-based connection, continue at ***Configuring an Ethernet-Based Connection*** on page 66.
   - To configure no connection, continue at ***Using No Connection*** on page 74.

Configuring an Ethernet-Based Connection

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.
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 66.

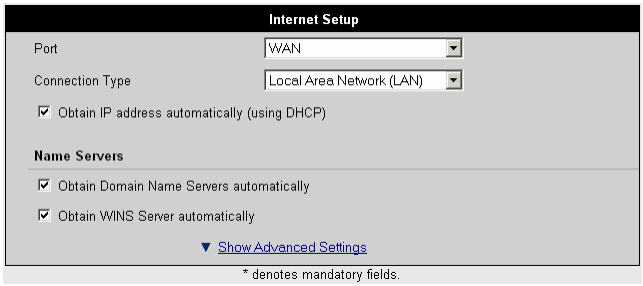
   If you chose Cable Modem, continue at ***Using a Cable Modem Connection*** on page 68.

   If you chose PPPoE, continue at ***Using a PPPoE Connection*** on page 69.

   If you chose PPTP, continue at ***Using a PPTP Connection*** on page 71.

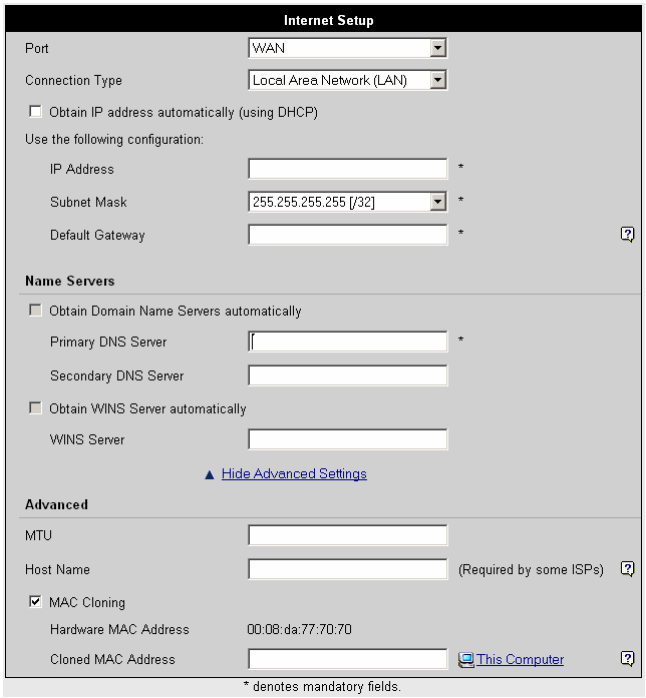
   If you chose Telstra, continue at ***Using a Telstra (BPA) Connection*** on page 73.

Using a LAN Connection



1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 75.

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

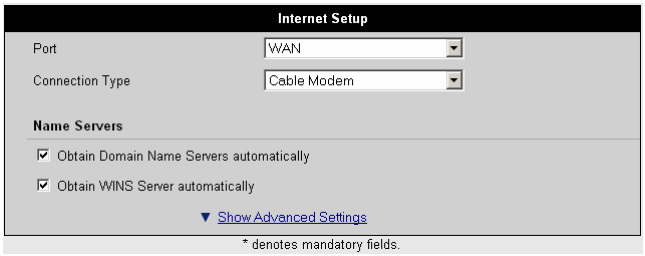


2. Click Apply.

   The ZoneAlarm router attempts to connect to the Internet, and the Status Bar displays the Internet status “Connecting”. This may take several seconds.

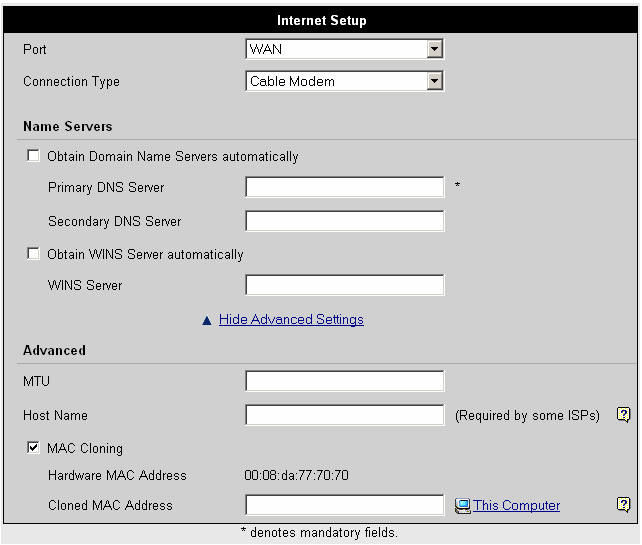
   Once the connection is made, the Status Bar displays the Internet status “Connected”.

Using a Cable Modem Connection



1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 75.

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

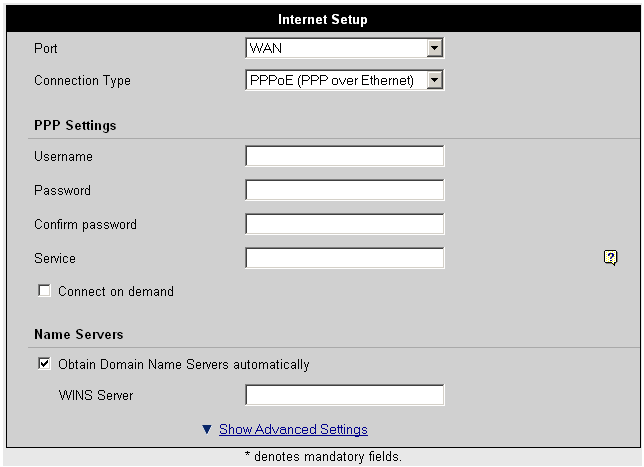


2. Click Apply.

   The ZoneAlarm router attempts to connect to the Internet, and the Status Bar displays the Internet status “Connecting”. This may take several seconds.

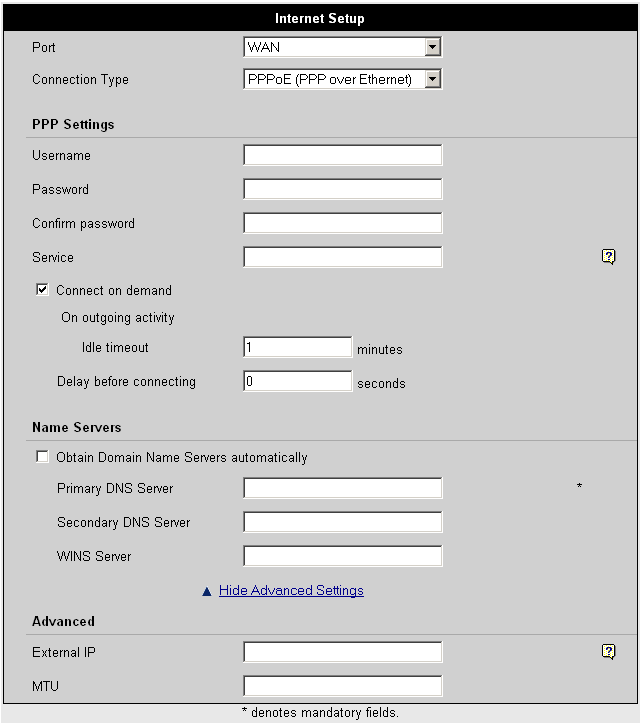
   Once the connection is made, the Status Bar displays the Internet status “Connected”.

Using a PPPoE Connection



1. Complete the fields using the relevant information in ***Internet Setup Fields*** on page 75.

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



2. Click Apply.

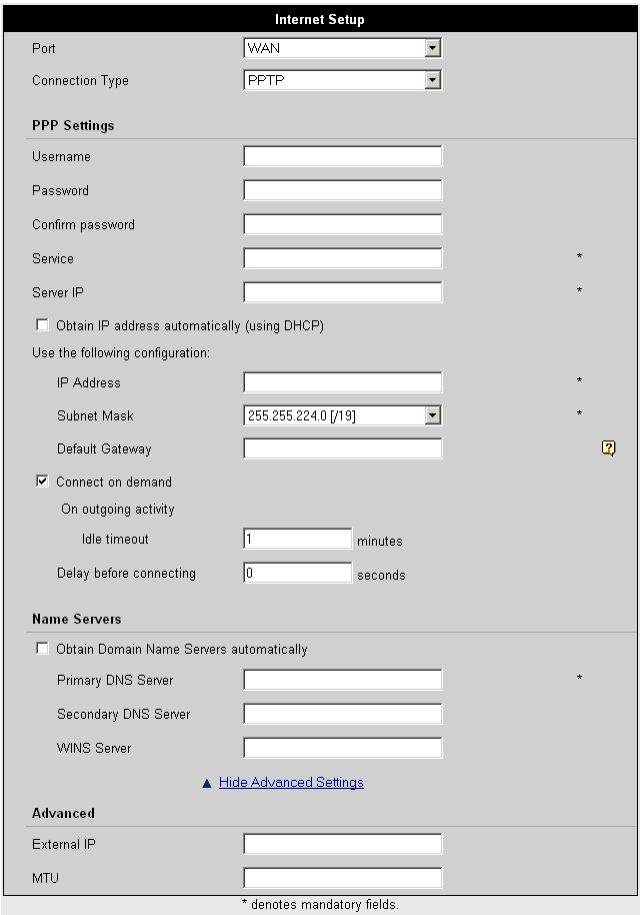
   The ZoneAlarm router attempts to connect to the Internet, and the Status Bar displays the Internet status “Connecting”. This may take several seconds.

   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 75.

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



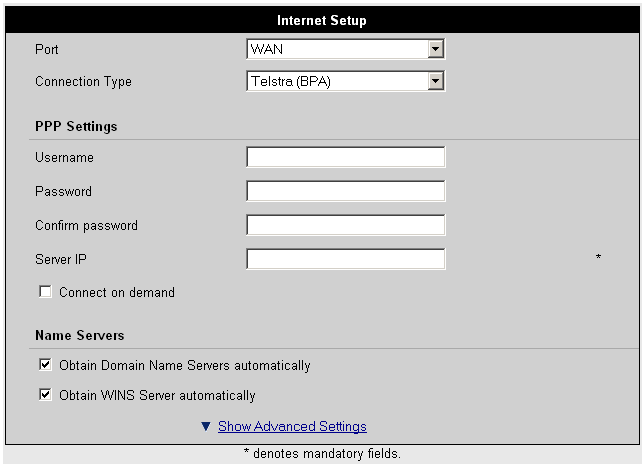
2. Click Apply.

   The ZoneAlarm router 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 75.

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

2. Click Apply.

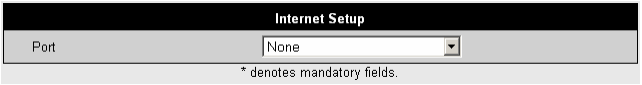
   The ZoneAlarm router attempts to connect to the Internet, and the Status Bar displays the Internet status “Connecting”. This may take several seconds.

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

Configuring No Connection

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

   The fields disappear.



2. Click Apply.

Table 14: Internet Setup Fields

In this field…	Do this…
PPP Settings	
Username	Type your user name.
Password	Type your password.
Confirm password	Type your password.
Service	Type your service name. If your ISP has not provided you with a service name, leave this field empty.
Server IP	If you selected PPTP, type the IP address of the PPTP server as given by your ISP. If you selected Telstra (BPA), type the IP address of the Telstra authentication server as given by Telstra.
Obtain IP address automatically (using DHCP)	Clear this option if you do not want the ZoneAlarm router to obtain an IP address automatically using DHCP.
IP Address	Type the static IP address of your ZoneAlarm router.
Subnet Mask	Select the subnet mask that applies to the static IP address of your ZoneAlarm router.
Default Gateway	Type the IP address of your ISP's default gateway.
Connect on demand	Select this option if you do not want the router to be constantly connected to the Internet. The router will establish a connection only under certain conditions.

In this field…	Do this…
On outgoing activity	Select this option to specify that the router should only establish a connection if there is outgoing activity (that is, packets need to be transmitted to the Internet). If the connection times out, the router 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 router will disconnect. The default value is 1.
Delay before connecting	Type the amount of time (in seconds) that the router 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.
Name Servers	
Obtain Domain Name Servers automatically	Clear this option if you want the ZoneAlarm router 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 ZoneAlarm router to obtain an IP address automatically using DHCP, but not to automatically configure the WINS server.
Primary DNS Server	Type the Primary DNS server IP address.

In this field…	Do this…
Secondary DNS Server	Type the Secondary DNS server IP address.
WINS Server	Type the WINS server IP address.
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.
Host Name	If your ISP requires a specific hostname for authentication, type it in this field. The ISP will supply you with the proper hostname, if needed. Most ISPs do not require a specific hostname.
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.
Hardware MAC Address	This field displays the ZoneAlarm router's MAC address. This field is read-only.

In this field…	Do this…
Cloned MAC Address	Do one of the following: • Click This Computer to automatically "clone" the MAC address of your computer to the ZoneAlarm router. • If the ISP requires authentication using the MAC address of a different computer, type the MAC address in this field.

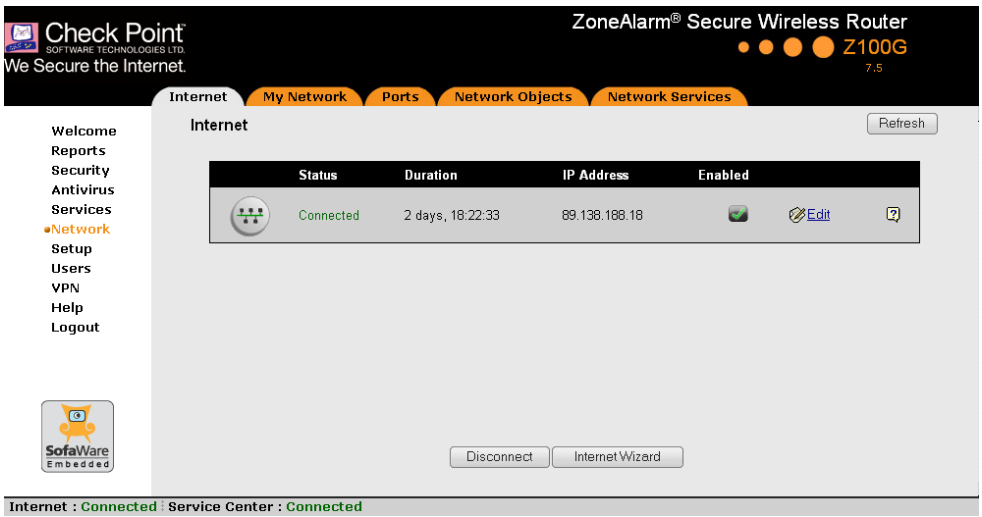
Viewing Internet Connection Information

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 15: 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 80

Enabling/Disabling the Internet Connection

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.

The Internet connection's Enabled/Disabled status is persistent through ZoneAlarm router 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

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 ZoneAlarm router is rebooted. The ZoneAlarm router 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 80.

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

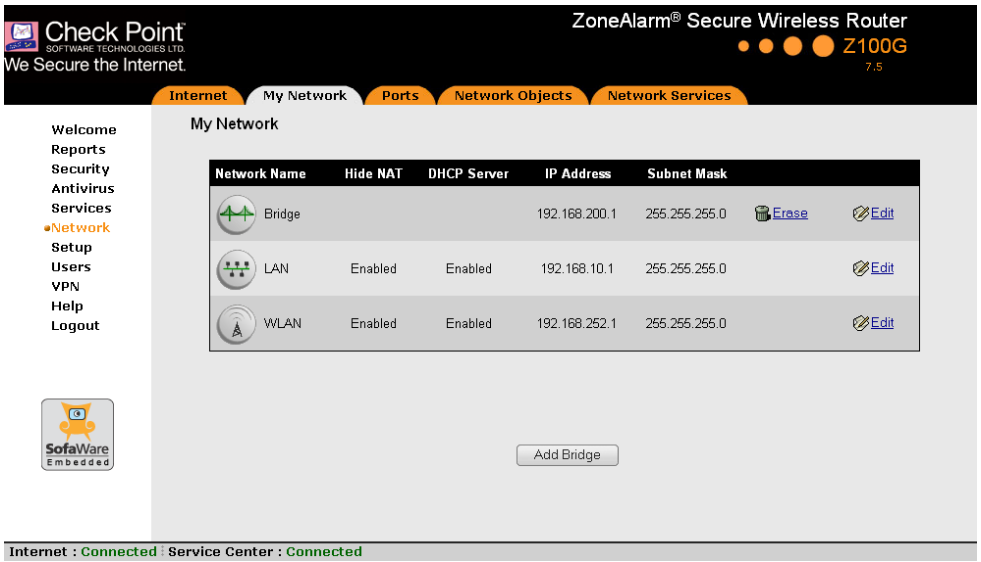
Note: If you accidentally change the network settings to incorrect values and are unable to connect to the my.firewall Web portal, you can reset the ZoneAlarm router to its default settings (see ***Resetting the ZoneAlarm router to Defaults*** on page 361).

Configuring the LAN Network

To configure the LAN network

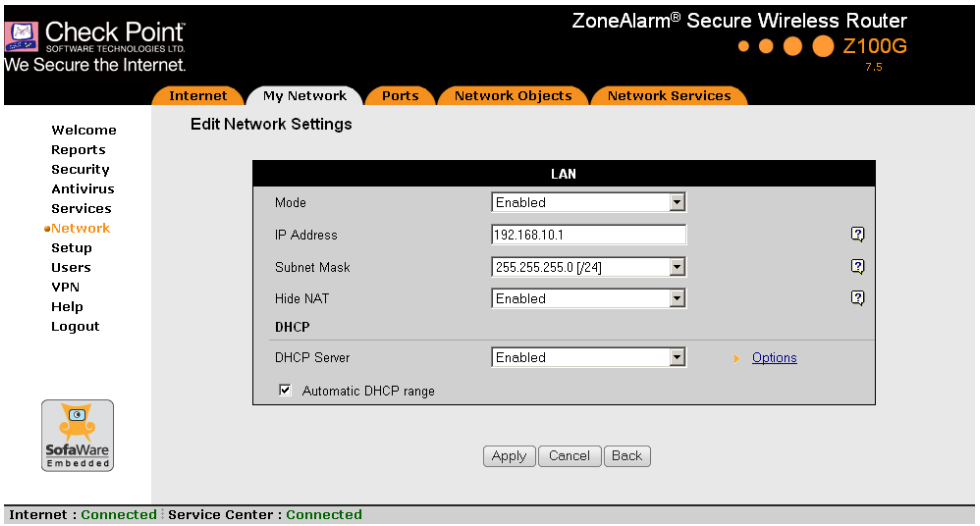
1. Click Network in the main menu, and click the My Network tab.

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 ZoneAlarm router's internal IP address.

   See ***Changing IP Addresses*** on page 83.

5. If desired, enable or disable Hide NAT.

   See ***Enabling/Disabling Hide NAT*** on page 85.

6. If desired, configure a DHCP server.

   See ***Configuring a DHCP Server*** on page 86.

7. Click Apply.

   A warning message appears.

8. Click OK.

   A success message appears.

Changing IP Addresses

If desired, you can change your ZoneAlarm router'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 ZoneAlarm router'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 ZoneAlarm router's internal IP address and by the subnet mask.

For example, if the ZoneAlarm router'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 ZoneAlarm router'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 ZoneAlarm 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 28.

Enabling/Disabling Hide NAT

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 ZoneAlarm router's single Internet IP address.

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

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

To enable/disable Hide NAT

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

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

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

   A warning message appears.
5. Click OK.

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

Configuring a DHCP Server

By default, the ZoneAlarm router operates as a DHCP (Dynamic Host Configuration Protocol) server. This allows the ZoneAlarm router 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 ZoneAlarm DHCP server, you must disable the ZoneAlarm 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 ZoneAlarm DHCP server, you can configure DHCP relay. When in DHCP relay mode, the ZoneAlarm router 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 95.

Enabling/Disabling the ZoneAlarm DHCP Server

You can enable and disable the ZoneAlarm DHCP Server for internal networks.

To enable/disable the ZoneAlarm 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 ZoneAlarm 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

By default, the ZoneAlarm 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 ZoneAlarm 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.

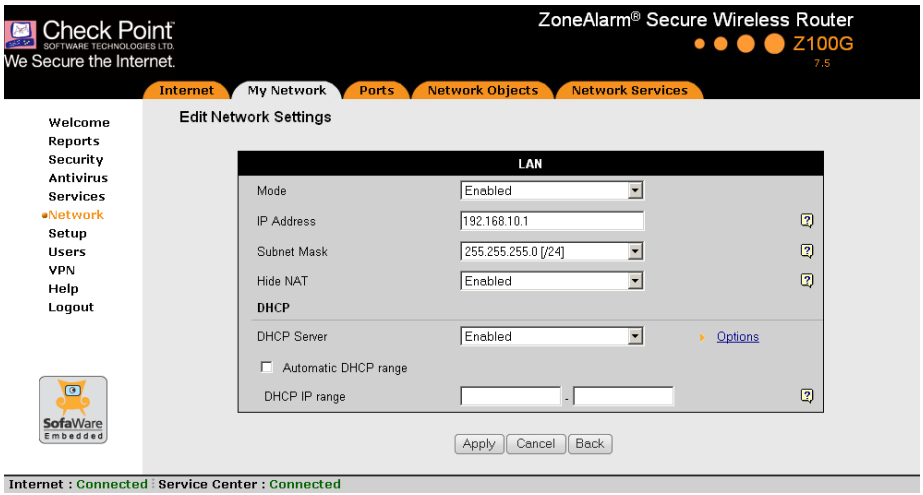
   The Edit Network Settings page appears.

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 ZoneAlarm 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

You can configure DHCP relay for internal networks.

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

To configure DHCP relay

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

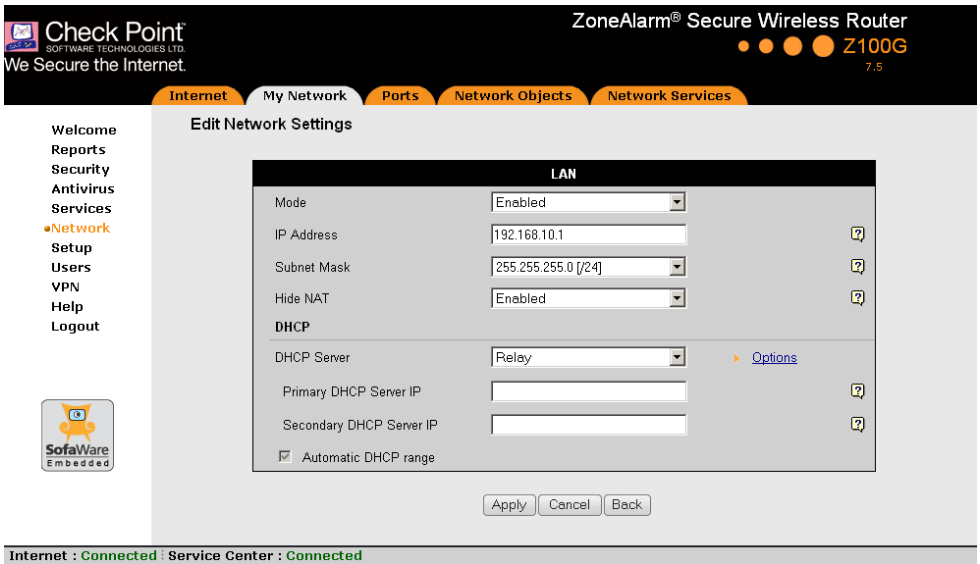
   The My Network page appears.

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 ZoneAlarm 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

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

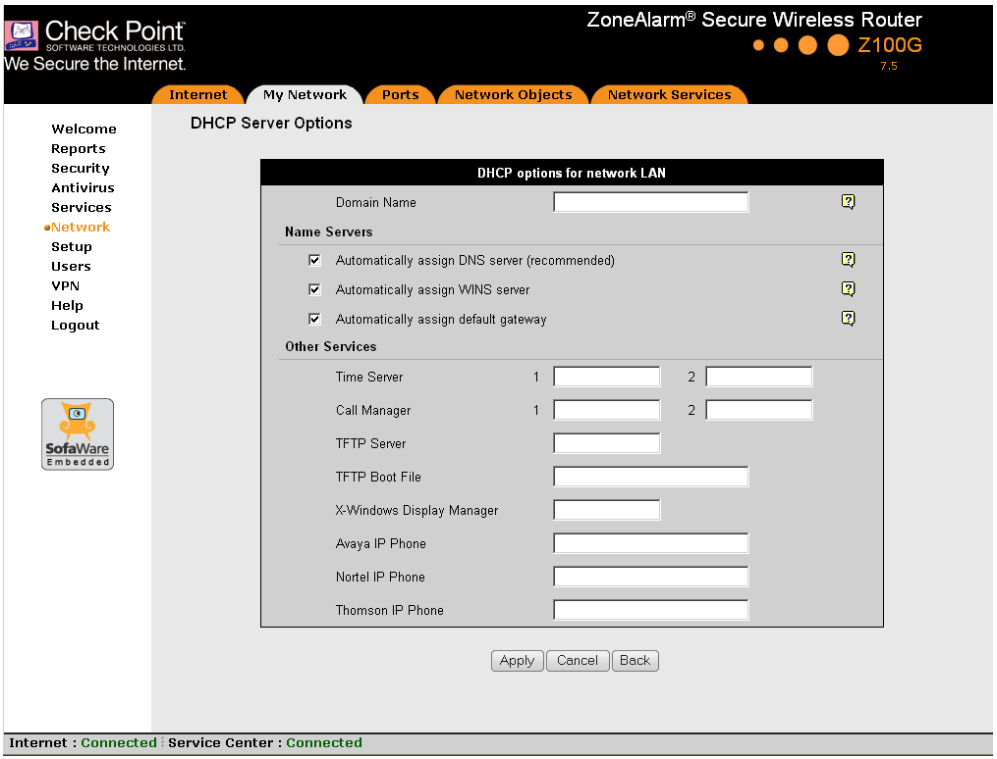
To configure DHCP options

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.

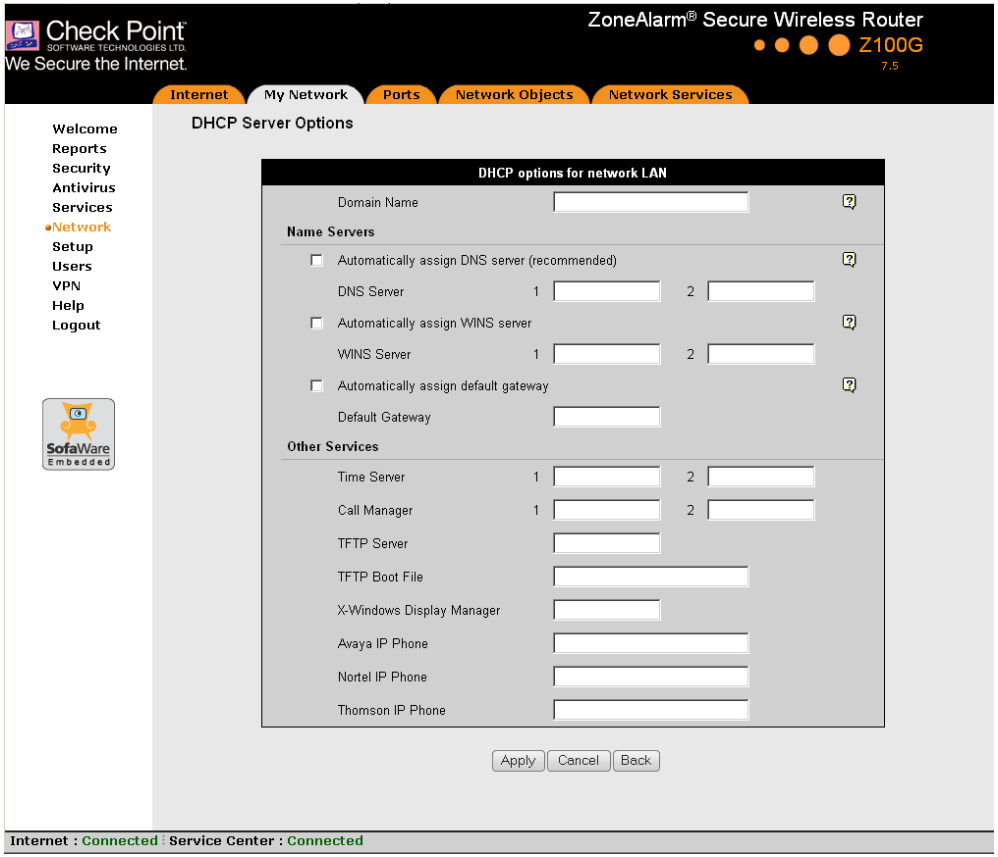
   The Edit Network Settings page appears.
3. In the DHCP area, click Options.

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 16: 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	
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.

Using Network Objects

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 172.

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

Note: The ZoneAlarm router supports Proxy ARP (Address Resolution Protocol). When an external source attempts to communicate with such a computer, the ZoneAlarm router 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 ZoneAlarm DHCP server consistently assigns the same IP address to a specific computer. However, if the ZoneAlarm 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 276. For information on Web rules, see ***Using Web Rules*** on page 187.

Adding and Editing Network Objects

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

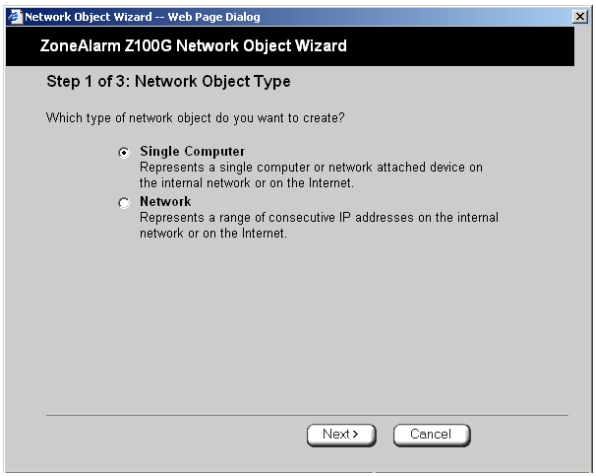
1. Click Network in the main menu, and click the Network Objects tab.

   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 Edit next to the desired computer in the list.

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

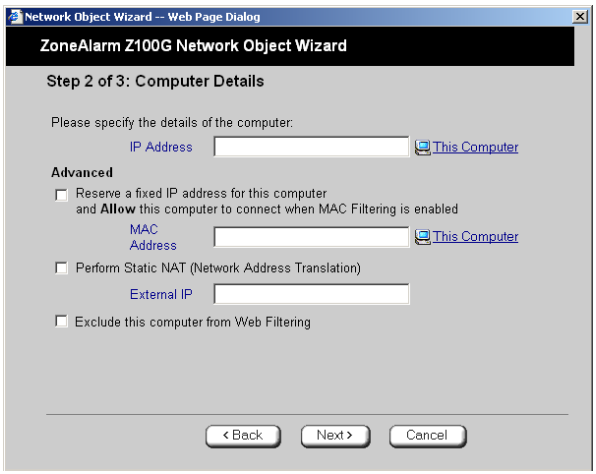


3. Do one of the following:

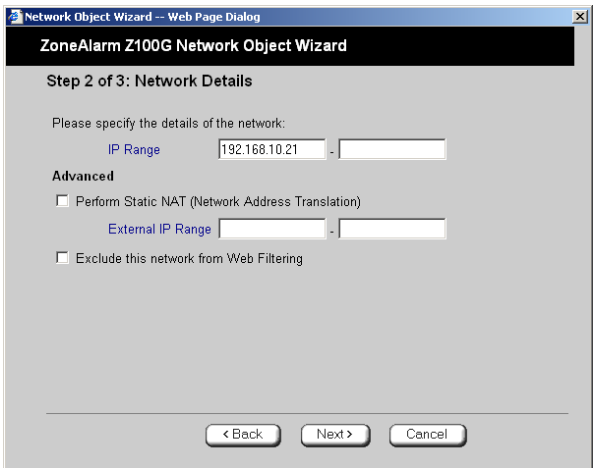
   - To specify that the network object should represent a single computer or device, click Single Computer.
   - To specify that the network object should represent a network, click Network.

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.

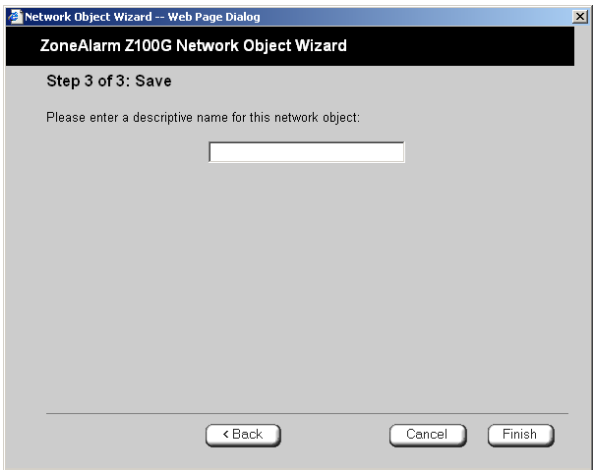


If you chose Network, the dialog box does not include this option.



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

The Step 3: Save dialog box appears.

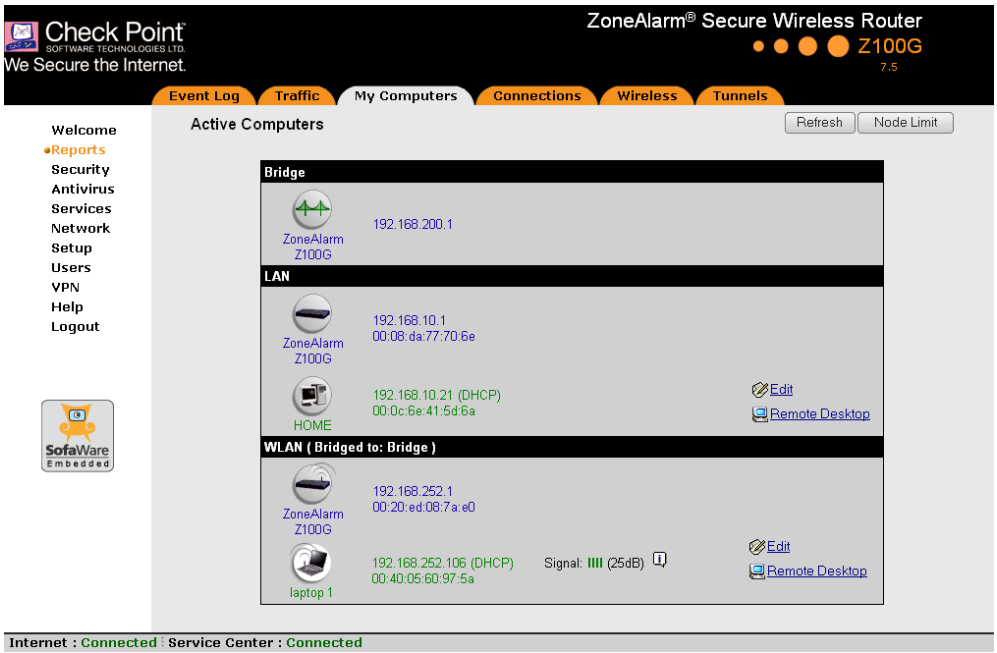


7. Type a name for the network object in the field.
8. Click Finish.

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 ZoneAlarm 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 17: Network Object Fields for a Single Computer

In this field…	Do this…
IP Address	Type the IP address of the local computer, or click This Computer to specify your computer.
Reserve a fixed IP address for this computer	Select this option to assign the network object's IP address to a MAC address, and to allow the network object to connect to the WLAN when MAC Filtering is used. For information about MAC Filtering, see ***Configuring a Wireless Network*** on page 113.
MAC Address	Type the MAC address you want to assign to the network object's IP address, or click This Computer to specify your computer's MAC address.
Perform Static NAT (Network Address Translation)	Select this option to map the local computer's IP address to an Internet IP address. You must then fill in the External IP field.

In this field…	Do this…
External IP	Type the Internet IP address to which you want to map the local computer's IP address.
Exclude this computer from Web Filtering	Select this option to exclude this computer from the Web Filtering service and Web rule enforcement.

Table 18: 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 Web Filtering	Select this option to exclude this network from the Web Filtering service and Web rule enforcement.

Viewing and Deleting Network Objects

To view or delete a network object

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

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

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

      A confirmation message appears.

   b. Click OK.

      The network object is deleted.

Configuring Network Service Objects

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

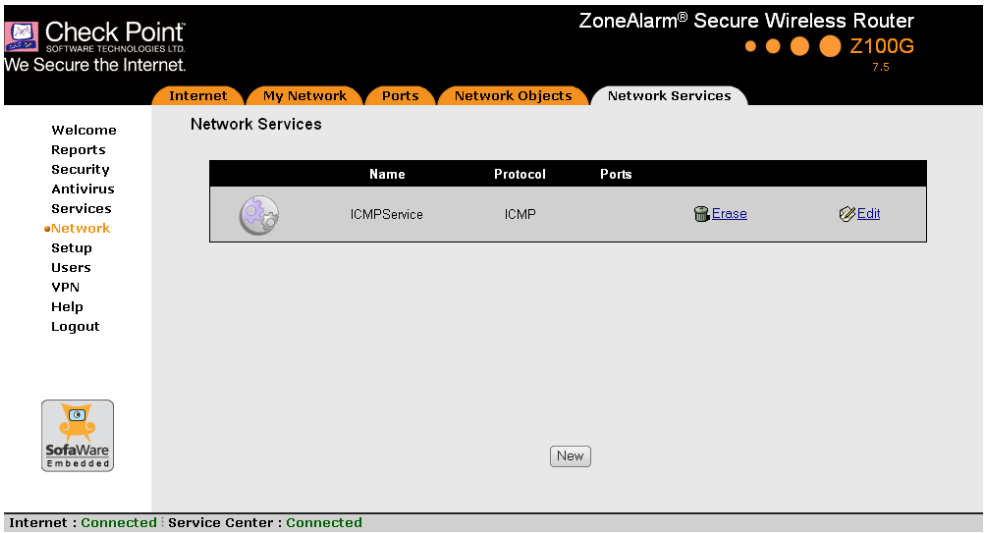
Defining network service objects can make your policies easier to understand and maintain. When a network service object is modified, the change automatically takes effect in all rules and settings that reference the network service object.

Adding and Editing Network Service Objects

To add or edit a network service object

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

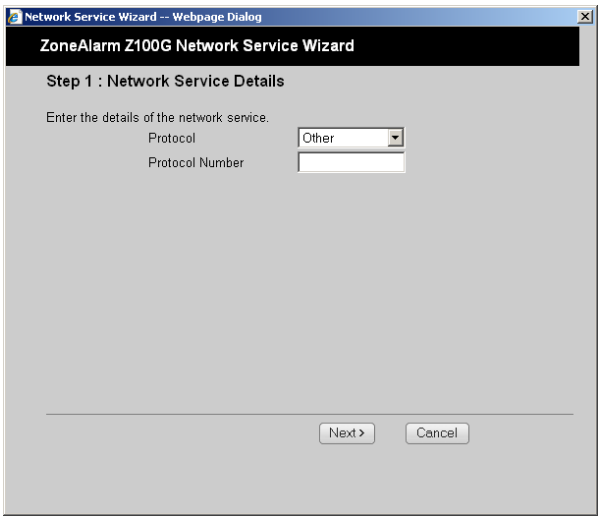
The Network Services page appears with a list of network service objects.



2. Do one of the following:

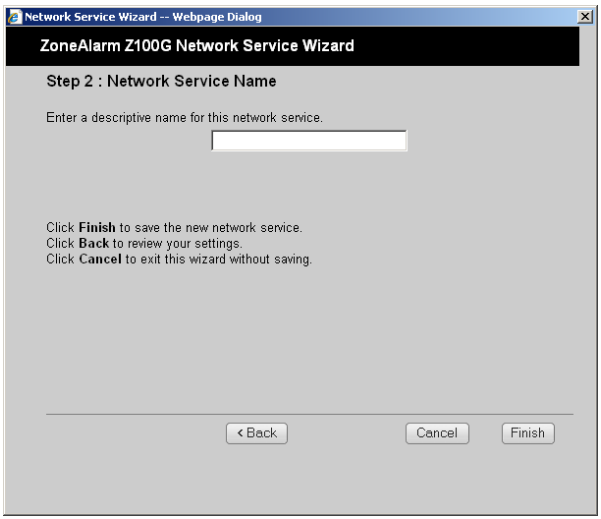
   - To add a network service object, click New.
   - To edit an existing network service object, click Edit next to the desired object in the list.

The ZoneAlarm 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 19: 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

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 the Erase icon.
      A confirmation message appears.
   b. Click OK.
      The network service object is deleted.

Managing Ports

The ZoneAlarm router allows you to restrict the LAN1-4 ports and the WAN port to a specific link speed and duplex setting. If desired, you can also disable ports.

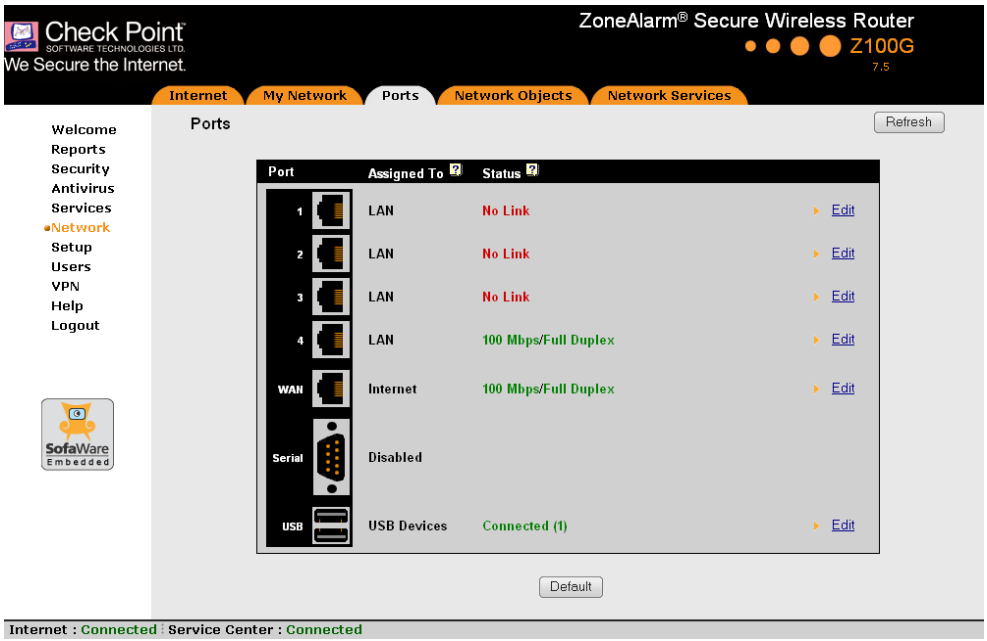
Viewing Port Statuses

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

To view port statuses

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

   The Ports page appears.



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

2. To refresh the display, click Refresh.

Table 20: Ports Fields

This field…	Displays…
Assign To	The port's current assignment. For example, if the LAN1 port is not assigned to a network, the field displays "None".
Status	The port's current status. This can be any of the following: • The detected link speed (10 Mbps or 100 Mbps) and duplex (Full Duplex or Half Duplex) • No Link. The router does not detect anything connected to the port. • Disabled. The port is disabled. For example, the LAN1 port's status will be "Disabled" if the port is assigned to "None". • Connected (number). Printers are connected to the USB ports. The number of connected printers appears in parentheses. This status is relevant for the USB ports only. • Not Connected. No printers are connected to the USB ports. This status is relevant for the USB ports only.

Enabling/Disabling Ports

You can enable ports by assigning them to the LAN network, or disable them by assigning them to no network.

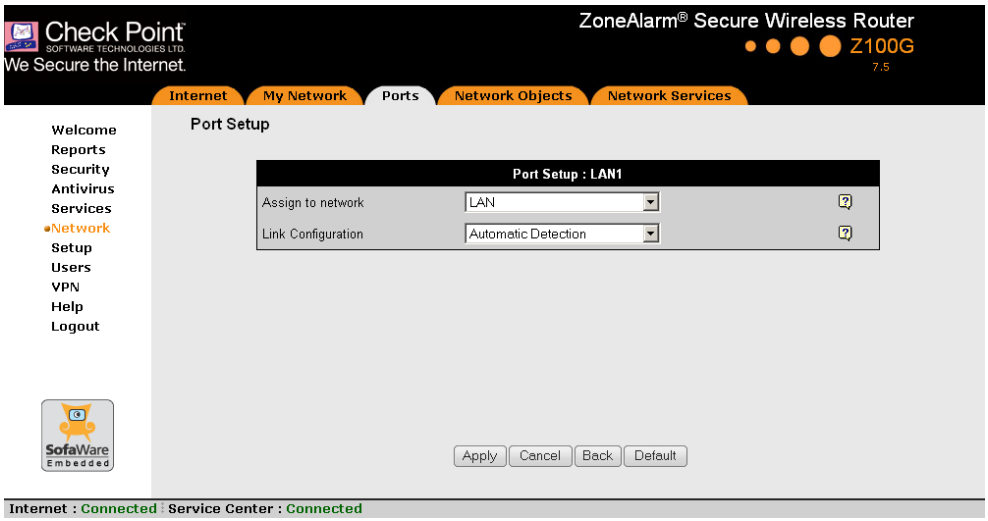
To enable/disable a port

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 enable a LAN port, select LAN.
   - To enable the WAN port, select Internet.
   - To disable a port, select None.
4. Click Apply.

   A warning message appears.
5. Click OK.

   The port is reassigned to the specified network or purpose.

Modifying Link Configurations

By default, the ZoneAlarm router automatically detects the link speed and duplex. If desired, you can manually restrict the router'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

You can reset the ZoneAlarm router's ports to their default link configurations ("Automatic Detection") and default assignments.

The LAN1-4 ports' default assignment is "LAN".

Resetting All Ports to Defaults

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

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

Configuring a Wireless Network

This chapter describes how to configure a wireless internal network.

This chapter includes the following topics:

Overview

In addition to the LAN network, you can define a wireless internal network called a WLAN (wireless LAN) network. You can configure a WLAN network in either of the following ways:

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

  See ***Using the Wireless Configuration Wizard*** on page 116.

- Manual configuration. Offers advanced setup options.

  See ***Manually Configuring a WLAN*** on page 122.

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

For information on default security policy rules controlling traffic to and from the WLAN, see ***Default Security Policy*** on page 168.

About the Wireless Hardware in Your ZoneAlarm Wireless Router

Your ZoneAlarm wireless router features a built-in 802.11b/g access point that is tightly integrated with the firewall and VPN.

ZoneAlarm wireless routers 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. SZoneAlarm wireless routers 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.

ZoneAlarm wireless routers transmit in 2.4GHz range, using dual diversity antennas to increase the range. In addition, ZoneAlarm routers 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).

Wireless Security Protocols

The ZoneAlarm wireless security router supports the following security protocols:

Table 21: Wireless Security Protocols

Security Protocol	Description
None	No security method is used. This option is not recommended, because it allows unauthorized users to access your WLAN network, although you can still limit access from the WLAN by creating firewall rules. This method is suitable for creating public access points.

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 router and the wireless stations must be configured with the same WEP key.
WPA-Personal: password authentication, encryption	The WPA-Personal (Wi-Fi Protected Access) security method (also called WPA-PSK) uses MIC (message integrity check) to ensure the integrity of messages, and TKIP (Temporal Key Integrity Protocol) to enhance data encryption. 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. Note: The router and the wireless stations must be configured with the same passphrase.
WPA2 (802.11i)	The WPA2 security method uses the more secure Advanced Encryption Standard (AES) cipher, instead of the RC4 cipher used by WPA and WEP. When using the WPA-Personal security methods, the ZoneAlarm enables you to restrict access to the WLAN network to wireless stations that support the WPA2 security method. If this setting is not selected, the ZoneAlarm router allows clients to connect using both WPA and WPA2.

Using the Wireless Configuration Wizard

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

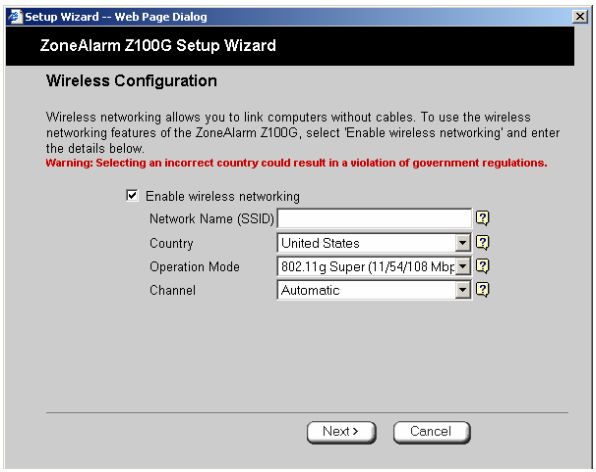
To configure a WLAN using the Wireless Configuration Wizard

1. Prepare the router for a wireless connection as described in ***Preparing the Router for a Wireless Connection*** on page 38.
2. Click Network in the main menu, and click the My Network tab.

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

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

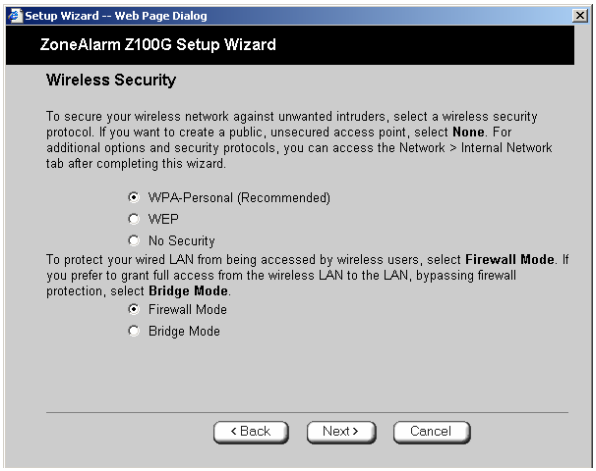
   The Wireless Configuration Wizard opens, with the Wireless Configuration dialog box displayed.



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

   The fields are enabled.
6. Complete the fields using the information in ***Basic WLAN Settings Fields*** on page 126.

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. 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 122.

   - 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 139.

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

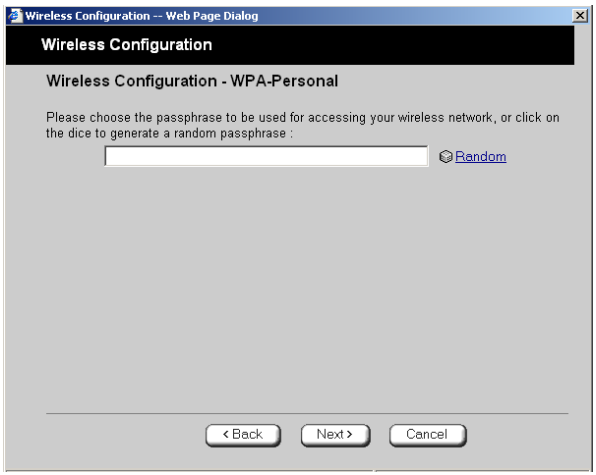
      The WLAN and LAN will be assigned separate, isolated IP networks, and traffic from the WLAN to the LAN will be subjected to the defined firewall policy.

      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*** on page 172.

11. Click Next.

WPA-Personal

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



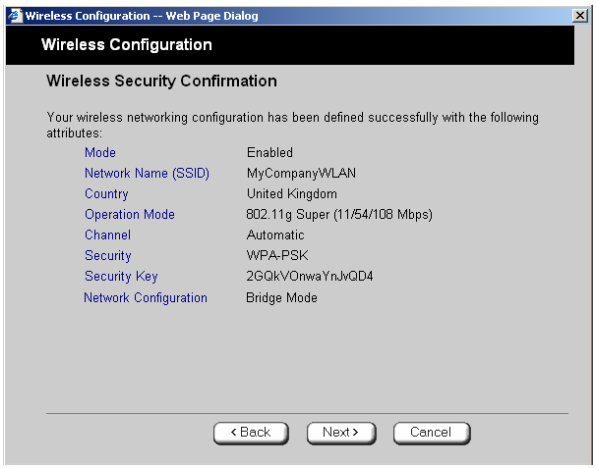
Do the following:

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

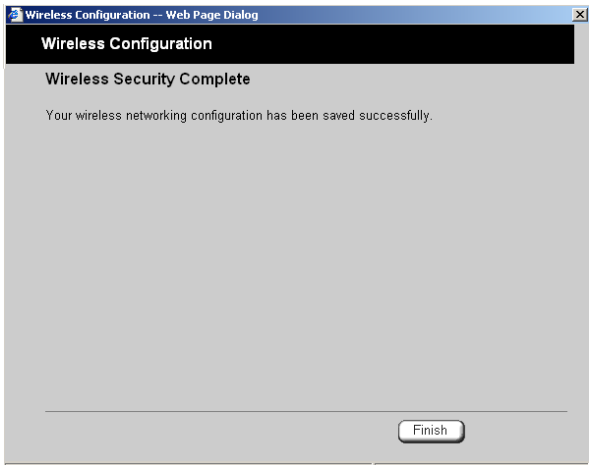
   This must be between 8 and 63 characters. It can contain spaces and special characters, and is case-sensitive.

2. Click Next.

The Wireless Security Confirmation dialog box appears.



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

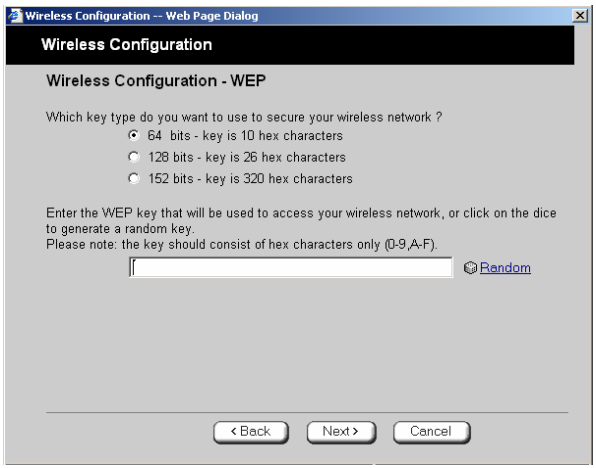


5. Click Finish.

   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 WLAN

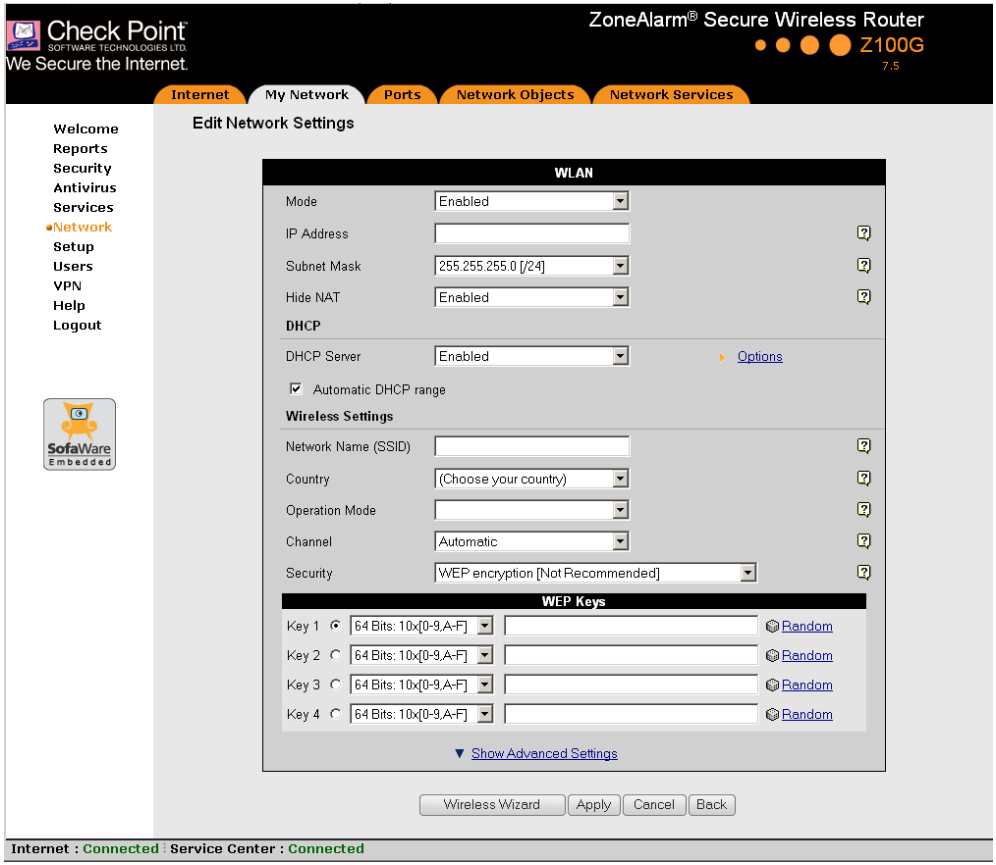
To manually configure a WLAN network

1. Prepare the router for a wireless connection as described in ***Preparing the Router for a Wireless Connection*** on page 38.
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. In the Mode drop-down list, select Enabled.

   The fields are enabled.

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

   The WLAN network must not overlap other networks.

6. In the Subnet Mask field, type the WLAN's internal network range.

7. If desired, enable or disable Hide NAT.

   See ***Enabling/Disabling Hide NAT*** on page 85.

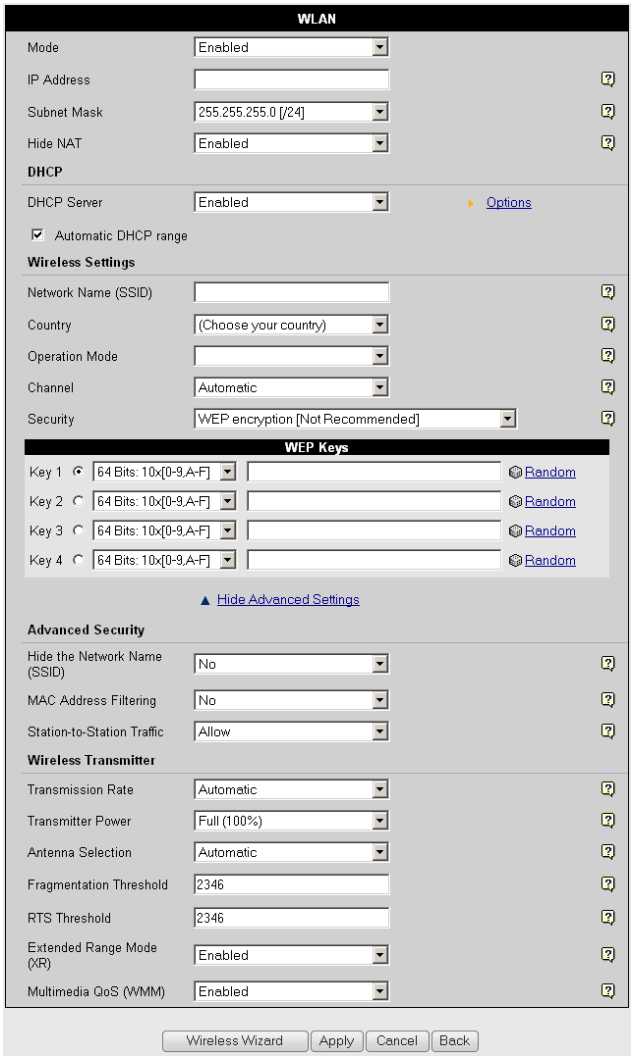
8. If desired, configure a DHCP server.

   See ***Configuring a DHCP Server*** on page 86.

9. Complete the fields using the information in ***Basic Wireless Settings Fields*** on page 126.

10. To configure advanced settings, click Show Advanced Settings and complete the fields using the information in ***Advanced Wireless Settings Fields*** on page 131.

New fields appear.



11. Click Apply.

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

12. 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 22: 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.

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

In this field…	Do this…
Channel	Select the radio frequency to use for the wireless connection: • Automatic. The ZoneAlarm router automatically selects a channel. This is the default. • A specific channel. The list of channels is dependent on the selected country and operation mode. Note: If there is another wireless network in the vicinity, the two networks may interfere with one another. To avoid this problem, the networks should be assigned channels that are at least 25 MHz (5 channels) apart. Alternatively, you can reduce the transmission power.
Security	Select the security protocol to use. For information on the supported security protocols, see ***Wireless Security Protocols*** on page 114. If you select WEP encryption, the WEP Keys area opens. If you select WPA-Personal, the Passphrase, Require WPA2 (802.11i), and WPA Encryption fields appear.
Passphrase	Type the passphrase for accessing the network, or click Random to randomly generate a passphrase. This must be between 8 and 63 characters. It can contain spaces and special characters, and is case-sensitive. For the highest security, choose a long passphrase that is hard to guess, or use the Random button. Note: The wireless stations must be configured with this passphrase as well.

In this field…	Do this…
Require WPA2 (802.11i)	Specify whether you want to require wireless stations to connect using WPA2, by selecting one of the following: • Enabled. Only wireless stations using WPA2 can access the WLAN network. • Disabled. Wireless stations using either WPA or WPA2 can access the WLAN network. This is the default.
WPA Encryption	Select the encryption method to use for authenticating and encrypting wireless data: • Auto. The ZoneAlarm router 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 23: 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 by 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 95. • 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 ZoneAlarm router automatically selects a rate. This is the default. • A specific rate
Transmitter Power	Select the transmitter power. Setting a higher transmitter power increases the access point's range. A lower power reduces interference with other access points in the vicinity. The default value is Full. It is not necessary to change this value, unless there are other access points in the vicinity.
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. ZoneAlarm routers avoid the problems of multipath distortion by using an antenna diversity system. To provide antenna diversity, each wireless security router has two antennas. Specify which antenna to use for communicating with wireless stations: • Automatic. The ZoneAlarm router 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 router.

In this field…	Do this…
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.
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.

In this field…	Do this…
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 Router*** on page 114.
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 ZoneAlarm router 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.

Troubleshooting Wireless Connectivity

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

- Check that the SSID configured on the station matches the ZoneAlarm router's SSID. The SSID is case-sensitive.
- Check that the encryption settings configured on the station (encryption mode and keys) match the ZoneAlarm router'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 104).
- Check that the wireless card region matches the access point region.
- Check the wireless card supports the wireless standard that you configured.

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 ZoneAlarm router, check that the Antenna Selection parameter in the WLAN's advanced settings is set to Automatic (see ***Manually Configuring a Wireless Network*** on page 122).
- Relocate the ZoneAlarm router to a place with better reception, and avoid obstructions, such as walls and electrical equipment. For example, try mounting the router in a high place with a direct line of sight to the wireless stations.
- Check for interference with nearby electrical equipment, such as microwave ovens and cordless or cellular phones.

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

Chapter 8

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 ZoneAlarm router allows you to connect the LAN and the WLAN network segments at the data-link layer, by configuring a bridge between them. A bridge allows you to choose whether to enable the firewall between the LAN and WLAN:

- If you enable the firewall, the WLAN and LAN will be assigned separate, isolated IP networks, and the gateway will operate as a regular firewall between the LAN and WLAN, inspecting traffic and dropping or blocking unauthorized or unsafe traffic according to the defined firewall policy.
- If you disable the firewall between the LAN and WLAN, they will appear as a single unified network; that is, the two network segments will share the same IP address range, and traffic will flow freely between them. Only traffic from the LAN and WLAN to the Internet will be inspected by the firewall.

The ZoneAlarm router allows you to configure anti-spoofing for the 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 LAN network segment, the following things happens:

- If a host with an IP address *outside of the allowed IP address range* tries to connect from the LAN 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 network segment *other than the LAN segment*, the connection will be blocked and logged as “Spoofed IP”.

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.

Note: The ZoneAlarm router license allows configuring one bridge; however, STP can be used in situations where multiple bridge devices exist on the same network.

Workflow

To use a bridge

1. Add a bridge.

   See ***Adding and Editing Bridges*** on page 141.

2. Add the LAN and WLAN networks to the bridge.

   See ***Adding Internal Networks to Bridges*** on page 145.

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

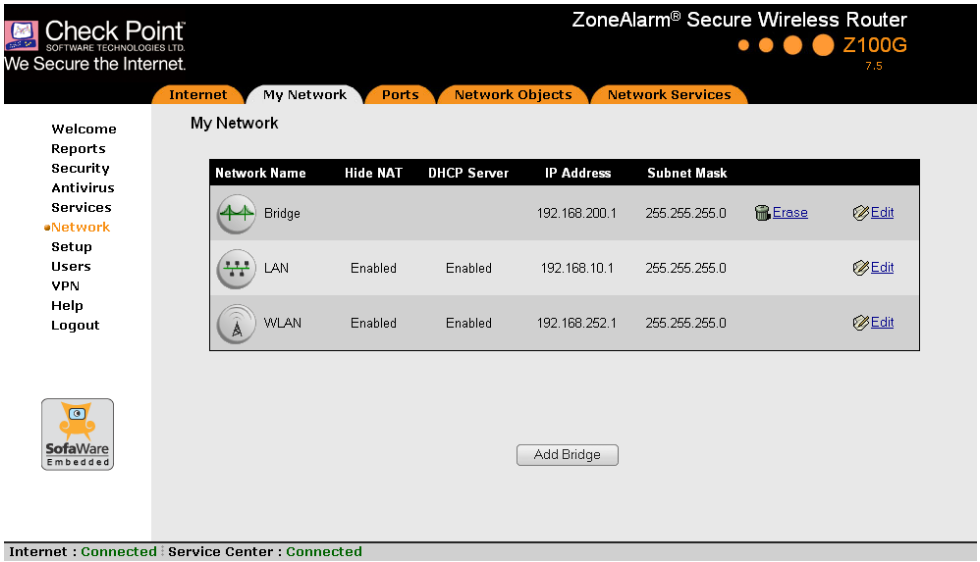
   For information on adding security rules, see ***Adding and Editing Rules*** on page 176. For information on adding VStream Antivirus rules, see ***Adding and Editing Vstream Antivirus Rules*** on page 252.

Adding and Editing Bridges

To add or edit a bridge

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

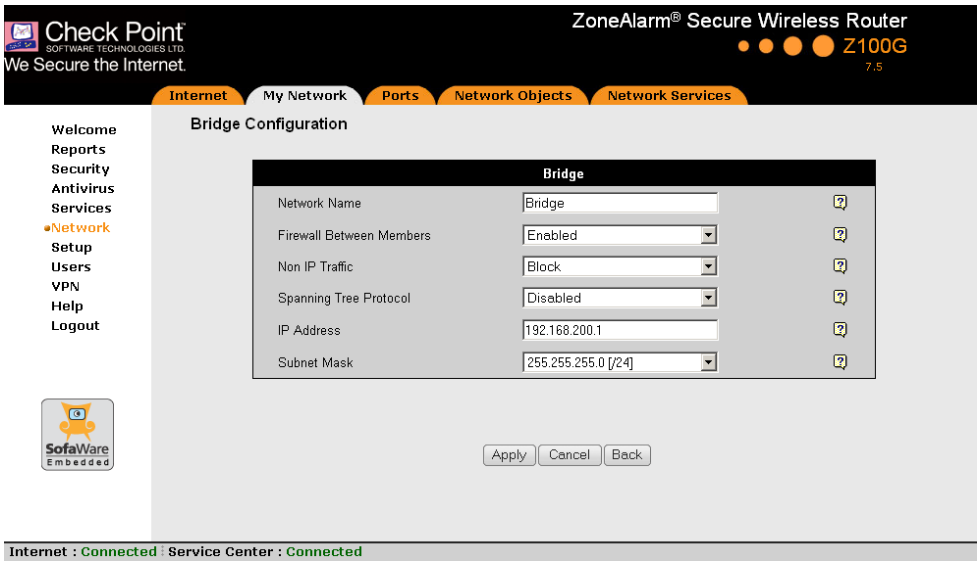
   The My Network page appears.



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 24: 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 139.
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

To add an internal network to a bridge

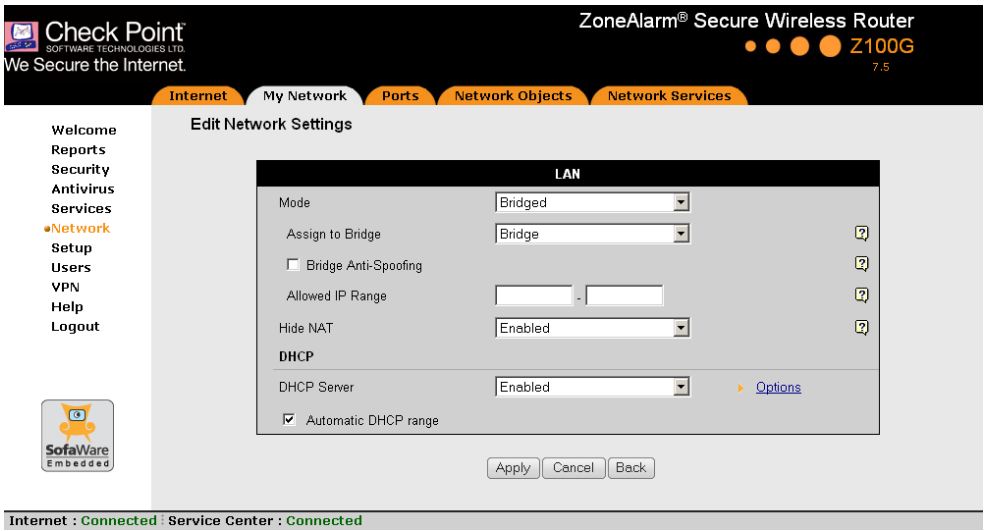
1. Click Network in the main menu, and click the My Network tab.

   The My Network page appears.

2. Click Edit in the desired network's row.

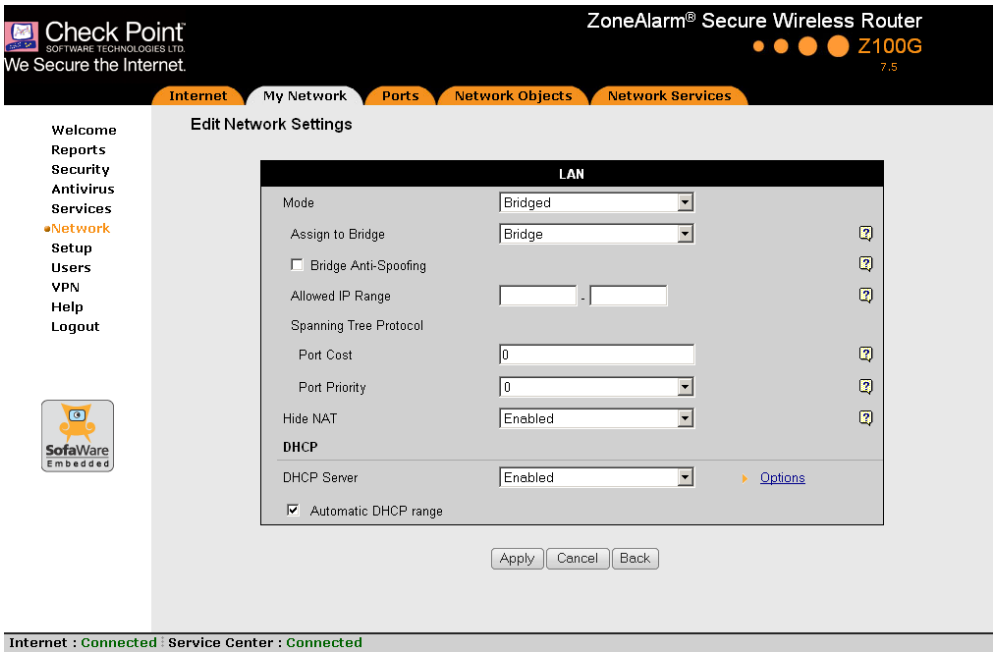
3. In the Mode drop-down list, select Bridged.

   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.

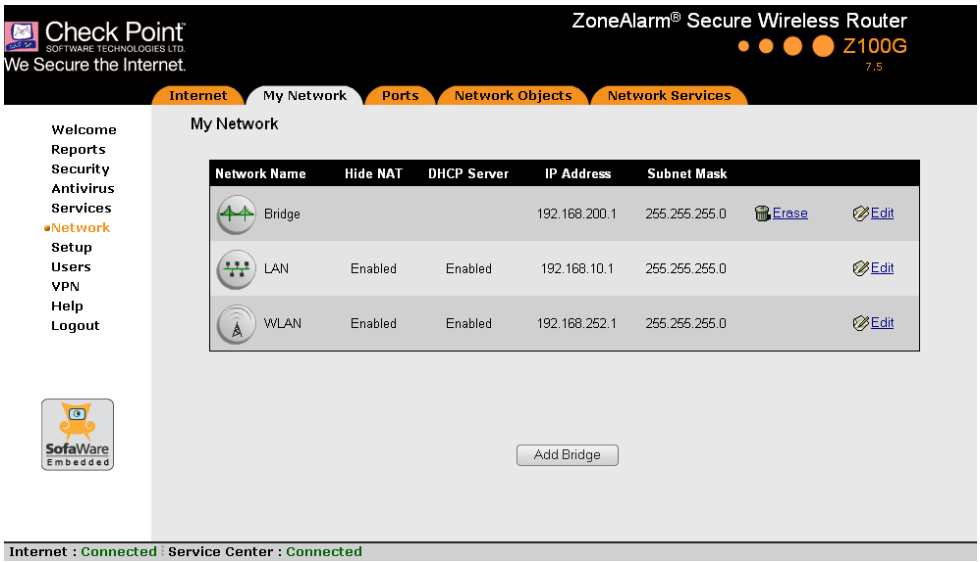


Table 25: Bridged Network Fields

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.

In this field...	Do this...
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 ZoneAlarm 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.

Deleting Bridges

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

   The My Network page appears.

3. In the desired bridge's row, click the Erase  icon.

   A confirmation message appears.

4. Click OK.

   The bridge is deleted.

Chapter 9

Viewing Reports

This chapter describes the ZoneAlarm Portal reports.

This chapter includes the following topics:

Viewing the Event Log

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

Table 26: Event Log Color Coding

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

An event marked in this color…	Indicates…
Green	Traffic accepted by the firewall. By default, accepted traffic is not logged. However, such traffic may be logged if specified by a security policy downloaded from your Service Center, or if specified in user-defined rules. In addition, accepted traffic may be logged if SmartDefense protections' Action field is set to "Track" instead of "Block".

You can create firewall rules specifying that certain types of connections should be logged, whether the connections are incoming or outgoing, blocked or accepted. For information, see ***Using Rules*** on page 172.

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

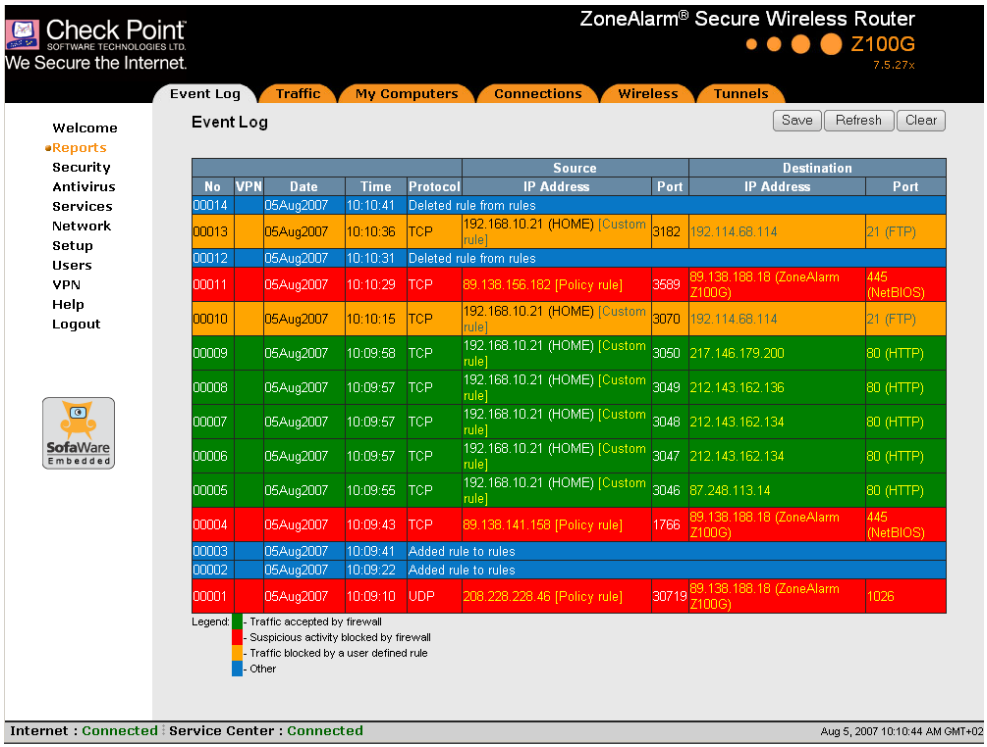
This information is useful for troubleshooting. You can export the logs to an *.xls (Microsoft Excel) file, and then store it for analysis purposes or send it to technical support.

Note: You can configure the ZoneAlarm router to send event logs to a Syslog server. For information, see ***Configuring Syslog Logging*** on page 336.

To view the event log

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

   The Event Log page appears.



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

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

3. To refresh the display, click Refresh.

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

   a. Click Save.

A standard File Download dialog box appears.

b. Click Save.

The Save As dialog box appears.

c. Browse to a destination directory of your choice.

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

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

5. To clear all displayed events:

a. Click Clear.

A confirmation message appears.

b. Click OK.

All events are cleared.

Using the Traffic Monitor

You can view incoming and outgoing traffic for selected network interfaces using the Traffic Monitor. This enables you to identify network traffic trends and anomalies.

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 156.

The traffic is color-coded as described in the following table.

Table 27: Traffic Monitor Color Coding for Networks

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

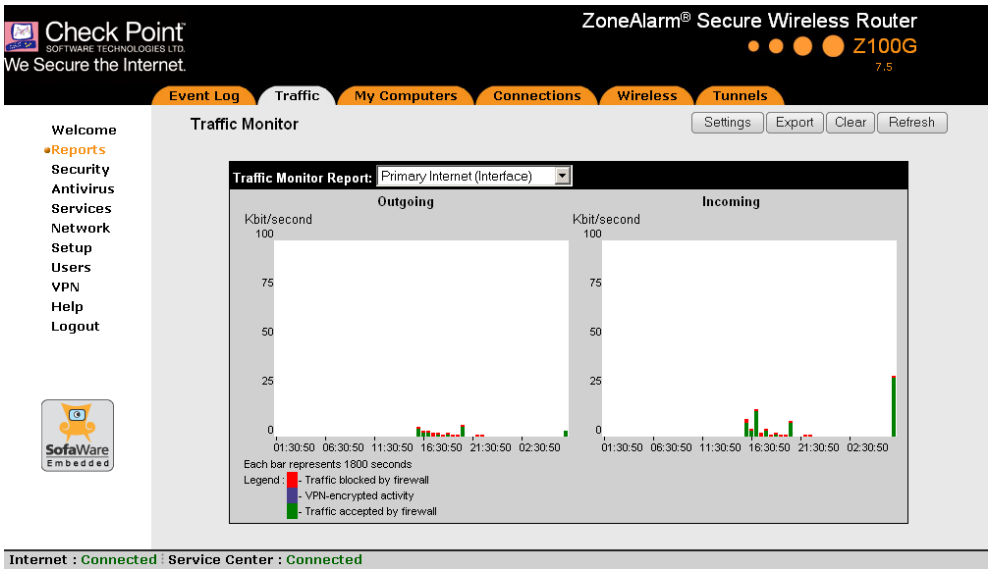
You can export a detailed traffic report for all enabled networks, using the procedure ***Exporting General Traffic Reports*** on page 157.

Viewing Traffic Reports

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 WLAN network is enabled, it will appear in the list.

   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

You can configure the interval at which the ZoneAlarm router should collect traffic data for network traffic reports.

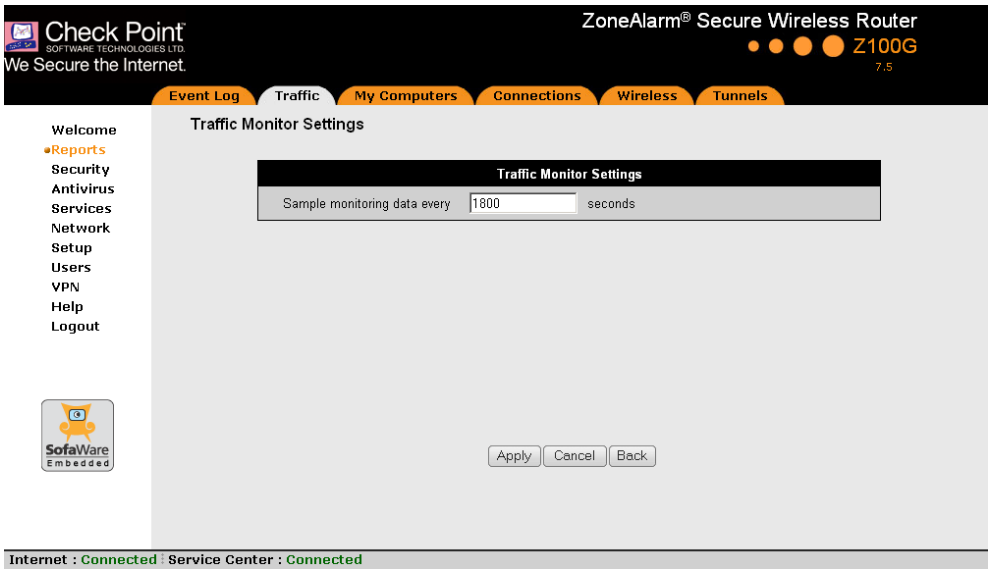
To configure Traffic Monitor settings

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 ZoneAlarm router should collect traffic data.

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

4. Click Apply.

Exporting General Traffic Reports

You can export a general traffic report that includes information for all enabled networks 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.

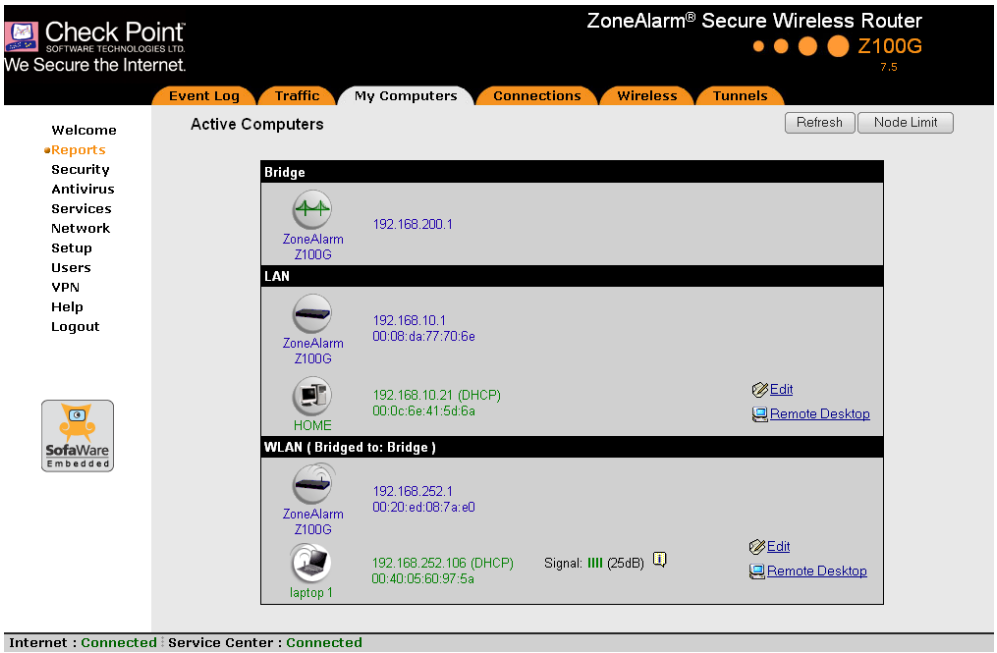
Viewing Computers

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 My Computers page appears.



If you enabled the wireless network, the wireless stations are shown under the WLAN. For information on viewing statistics for these computers, see ***Viewing Wireless Statistics*** on page 161. If a wireless station has been blocked from accessing the Internet through the ZoneAlarm router, the reason why it was blocked is shown in red.

If you are exceeding the maximum number of computers allowed by your license, a warning message appears, and the computers over the node limit are marked in red.

These computers are still protected, but they are blocked from accessing the Internet through the ZoneAlarm router.

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 My 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 335.

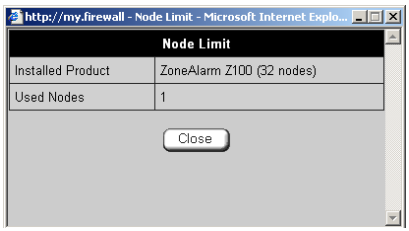
If Remote Desktop is enabled, a link appears next to each computer, enabling you to access its desktop remotely. For information on using Remote Desktop, see ***Using Remote Desktop*** on page 319.

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 97.

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.

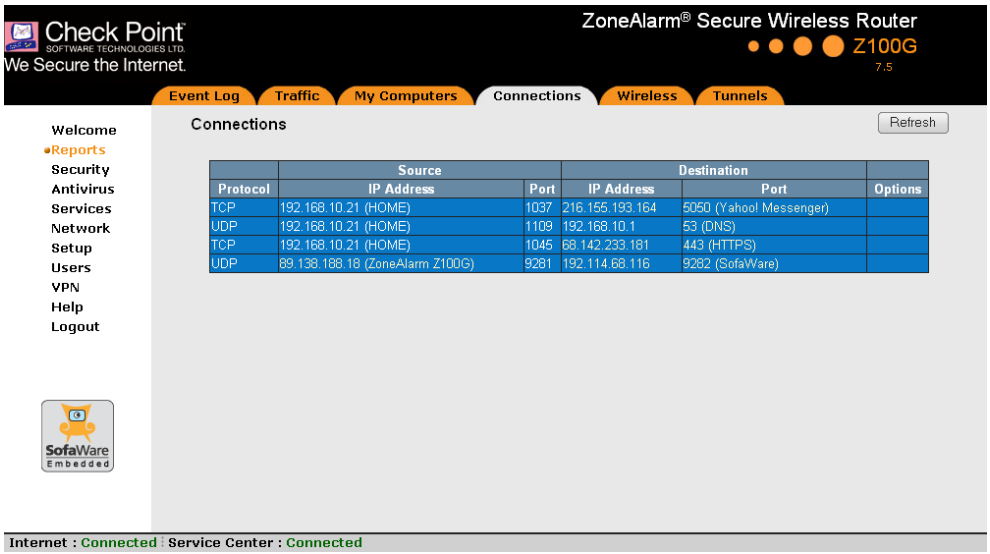
Viewing Connections

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

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 refresh the display, click Refresh.

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

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

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

   A window opens displaying information about the port.

Table 28: Connections Fields

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

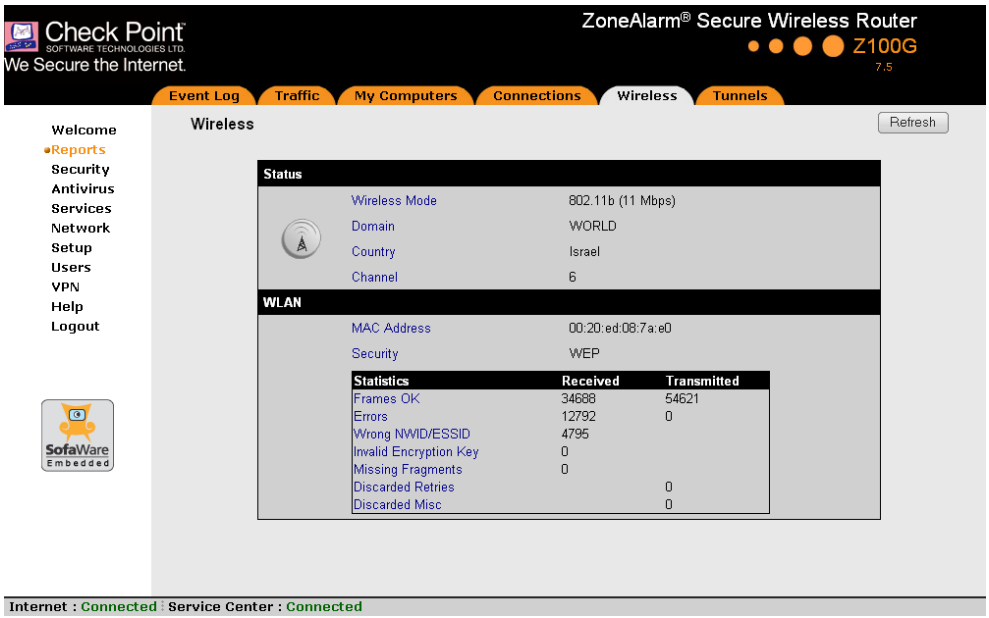
Viewing Wireless Statistics

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

To view statistics for the WLAN

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

The Wireless page appears.



The page displays the information in the following tables.

2. To refresh the display, click Refresh.

Table 29: Wireless Statistics

This field…	Displays…
Status	
Wireless Mode	The operation mode used by the WLAN, followed by the transmission rate in Mbps
Domain	The ZoneAlarm access point's region
Country	The country configured for the WLAN
Channel	The radio frequency used by the WLAN

This field…	Displays…
Statistics for WLAN	This information is displayed for the WLAN.
MAC Address	The MAC address of the wireless network interface
Security	The security mode used by the wireless network
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
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

To view statistics for a wireless station

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

   The My 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 30: Wireless Station Statistics

This field…	Displays…
Current Rate	The current reception and transmission rate in Mbps
Frames OK	The total number of frames that were successfully transmitted and received
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.
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.

This field…	Displays…
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 10

Setting Your Security Policy

This chapter describes how to set up your ZoneAlarm router 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 267.

This chapter includes the following topics:

The ZoneAlarm 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 ZoneAlarm router serves as the enforcement agent for your network security policy. Therefore, the ZoneAlarm router'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 ZoneAlarm router 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.

Default Security Policy

The ZoneAlarm default security policy includes the following rules:

- Access is blocked from the WAN (Internet) to the internal networks (LAN and WLAN).
- 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 WLAN.
- If you chose “Firewall Mode” during setup, either in the ZoneAlarm Setup Wizard or in the Wireless Configuration Wizard:
  - Access is blocked from the WLAN to the LAN.
  - HTTP access to the ZoneAlarm Portal (my.firewall and my.vpn) is allowed from the LAN, but not from the WLAN. You can allow HTTP access from the WLAN, by creating a specific user-defined firewall rule.
- When using the print server function (see ***Using Network Printers*** on page 367), 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 172.

Setting the Firewall Security Level

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 31: Firewall Security Levels

This level…	Does this…	Further Details
Low	Enforces basic control on incoming connections, while permitting all outgoing connections.	All inbound traffic is blocked to the external ZoneAlarm router 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 traffic from the Internet and all outbound traffic to the Internet is blocked. This does not affect traffic to and from the gateway itself.

The definitions of firewall security levels provided in this table represent the ZoneAlarm router'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 172.

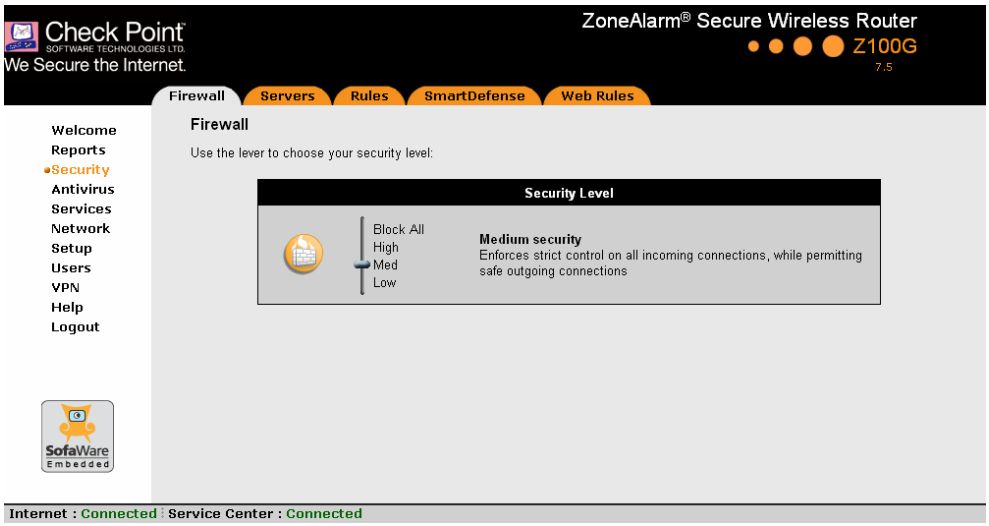
Note: If the security policy is remotely managed, this lever might be disabled.

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 ZoneAlarm router security level changes accordingly.

Using Firewall Rules

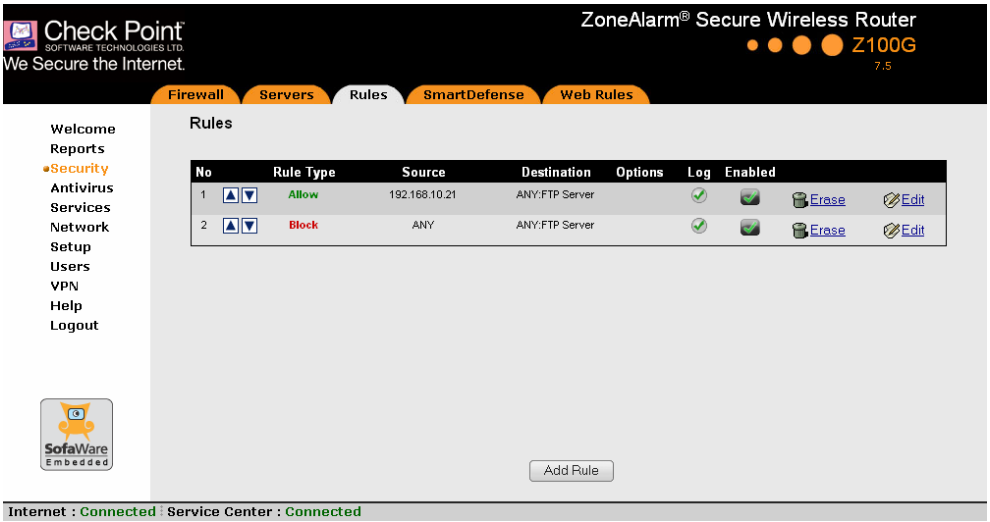
The ZoneAlarm router checks the protocol used, the ports range, and the destination IP address, when deciding whether to allow or block traffic.

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 your company computers are located on the LAN network, and guests are allowed to use the WLAN network, then as a result of the default security policy rules, employees on the LAN will be able to connect to guest computers, while guests will not be able to access any sensitive information on the company computers. You can override the default security policy rules, by creating firewall rules that allow specific WLAN computers (such a employee's laptop) to connect to the LAN network and company resources.

The ZoneAlarm router 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 ZoneAlarm router 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 32: 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 ZoneAlarm 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). Note: You must use this type of rule to allow incoming connections if your network uses Hide NAT.

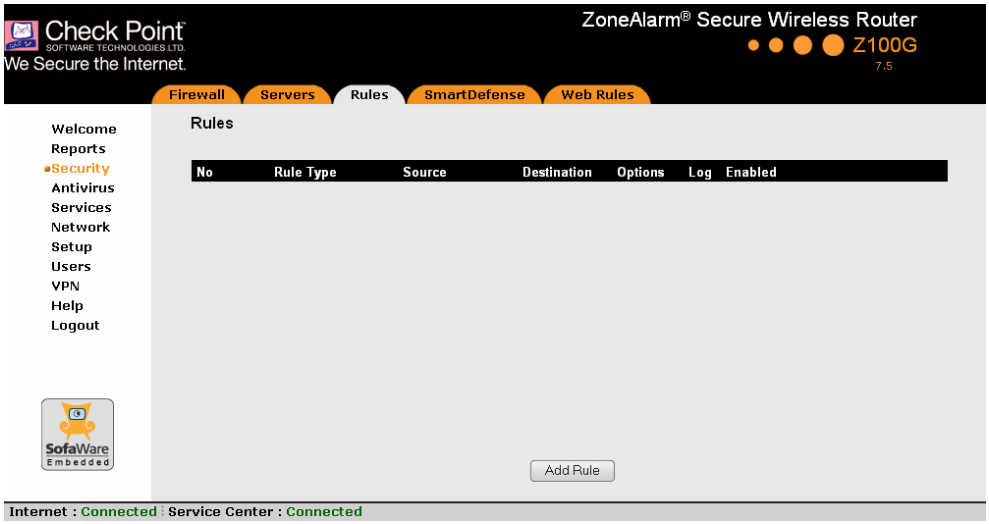
Rule	Description
Allow	This rule type enables you to do the following: • Permit outgoing access from your internal network to a specific service on the Internet. • Permit incoming access from the Internet to a specific service in your internal network. Note: You cannot use an Allow rule to permit incoming 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.

Adding and Editing Firewall Rules

To add or edit a firewall rule

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

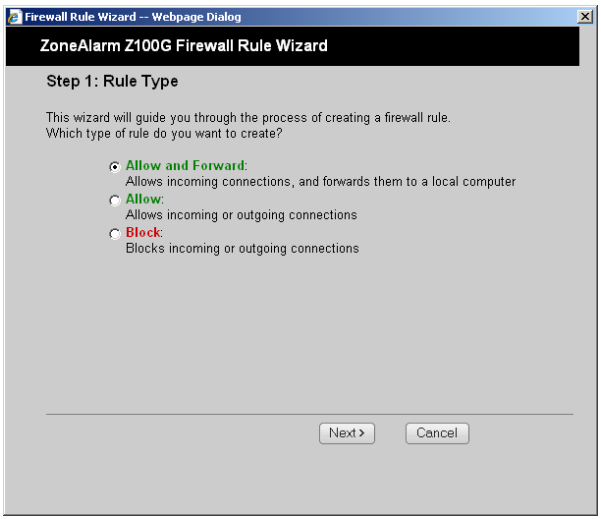
   The Rules page appears.



2. Do one of the following:

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

The ZoneAlarm 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**.

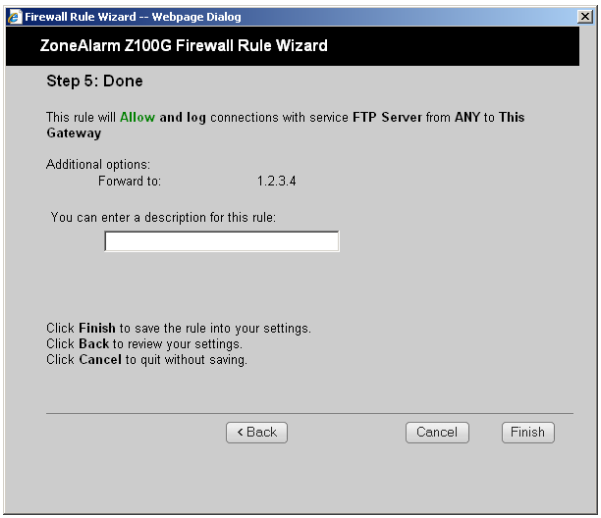
   New fields appear.

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 33: 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. 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.

In this field…	Do this…
Destination	Select the destination of the connections you want to allow or block. To specify an IP address, select Specified IP and type the desired IP address in the text box. To specify an IP address range, select Specified Range and type the desired IP address range in the fields provided. To specify the ZoneAlarm IP address, select This Gateway. To specify any destination *except* the ZoneAlarm Portal and network printers, 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.
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.

In this field…	Do this…
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

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, do one of the following:

   - To enable the rule, click  .

     The button changes to  and the rule is enabled.

   - To disable the rule, click  .

     The button changes to  and the rule is disabled.

Changing Firewall Rules' Priority

To change a firewall rule's priority

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

   The Rules page appears.

2. Do one of the following:

   - Click ▲ next to the desired rule, to move the rule up in the table.
   - Click ▼ next to the desired rule, to move the rule down in the table.

   The rule's priority changes accordingly.

Viewing and Deleting Firewall Rules

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 view a rule's description, mouse-over the information icon in the desired rule's row.

   A tooltip displays the rule's description.

3. To delete a rule, do the following.

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

      A confirmation message appears.

   b. Click OK.

      The rule is deleted.

Configuring Servers

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 ZoneAlarm router 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 172.

- Exposed host

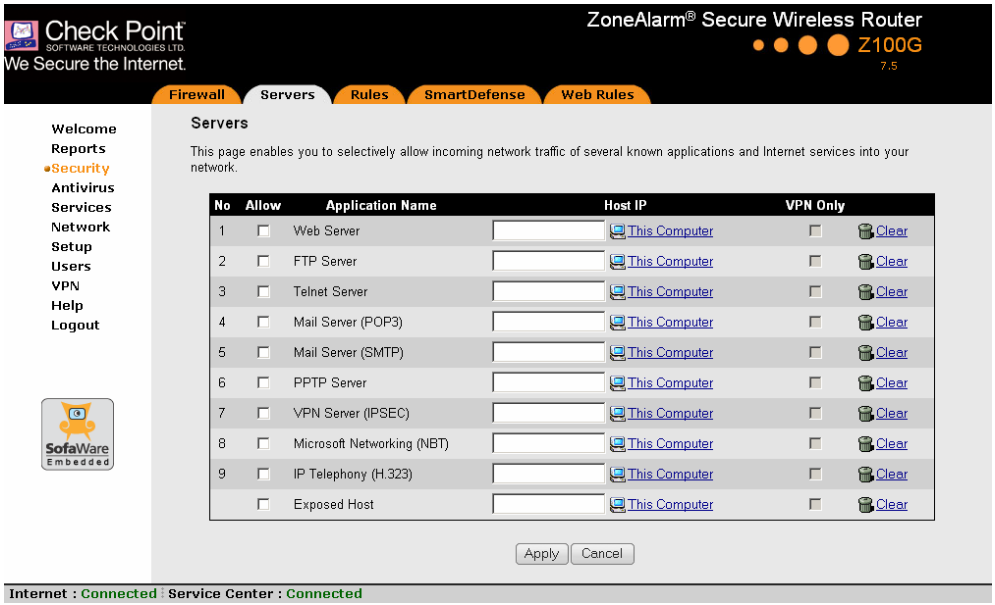
  If you need to allow unlimited incoming and outgoing connections between the Internet and a particular host, you can define an exposed host. An exposed host is not protected by the firewall, and it receives all traffic that was not forwarded to another computer by use of Allow and Forward rules.

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 34: 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 Web Rules

You can block or allow access to specific Web pages, by defining Web rules. If a user attempts to access a blocked page, the Access Denied page appears. For information on customizing this page, see ***Customizing the Access Denied Page*** on page 195.

If desired, you can permit specific users to override Web rules. Such users will be able to view Web pages without restriction, after they have provided their username password via the Access Denied page. For information on granting Web Filtering override permissions, see ***Adding and Editing Users*** on page 313.

In addition, you can choose to exclude specific network objects from Web rule enforcement. Users connecting from these network objects will be able to view Web pages without restriction, regardless of whether they have Web Filtering override permissions. For information on configuring network objects, see ***Using Network Objects*** on page 95.

Note: Web rules affect outgoing traffic only and cannot be used to allow or limit access from the Internet to internal Web servers.

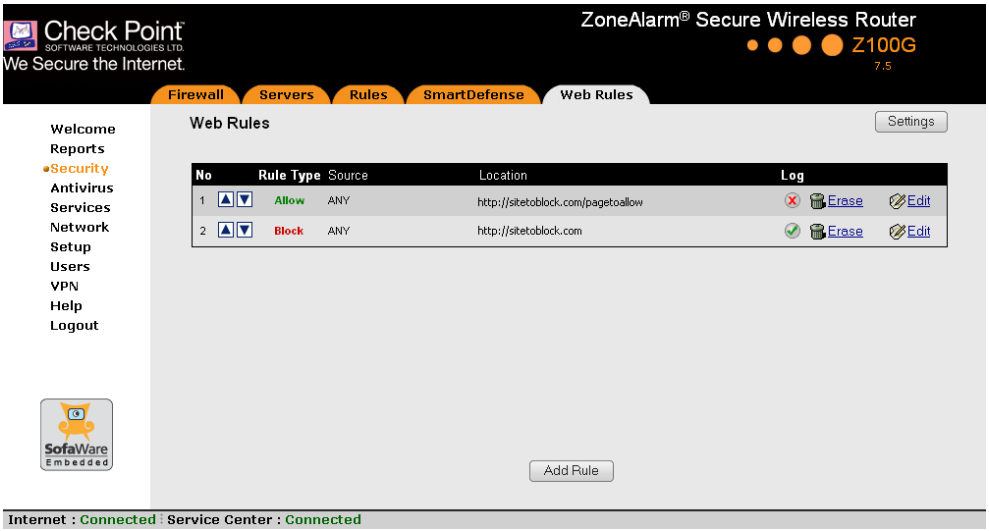
Note: Web rules differ from the Web Filtering subscription service in the following ways:

- The Web Filtering service is subscription-based and requires a connection to the Service Center, while Web rules are included with the ZoneAlarm router.
- The Web Filtering service is centralized, extracting URLs from HTTP requests and sending the URLs to the Service Center to determine whether they should be blocked or allowed. With Web rules, HTTP requests are analyzed in the gateway itself.
- The Web Filtering service is category based; that is, it filters Web sites based on the category to which they belong. In contrast, Web rules allow and block specific URLs.

You can use either content filtering solution or both in conjunction. When a user attempts to access a Web site, the ZoneAlarm router first evaluates the Web rules. If the site is not blocked by the Web rules, the Web Filtering service is then consulted. For information on the Web Filtering service, see ***Web Filtering*** on page 276.

The ZoneAlarm router processes Web rules in the order they appear in the Web 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 Web Rules table.

For example, if you want to block all the pages of a particular Web site, except a specific page, you can create a rule blocking access to all of the Web site's pages and move the rule down in the Web Rules table. Then create a rule allowing access to the desired page and move this rule to a higher location in the Web 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 ZoneAlarm router will process rule 1 first, allowing access to the desired page, and only then it will process rule 2, blocking access to the rest of the site.

The following rule types exist:

Table 35: Web Rule Types

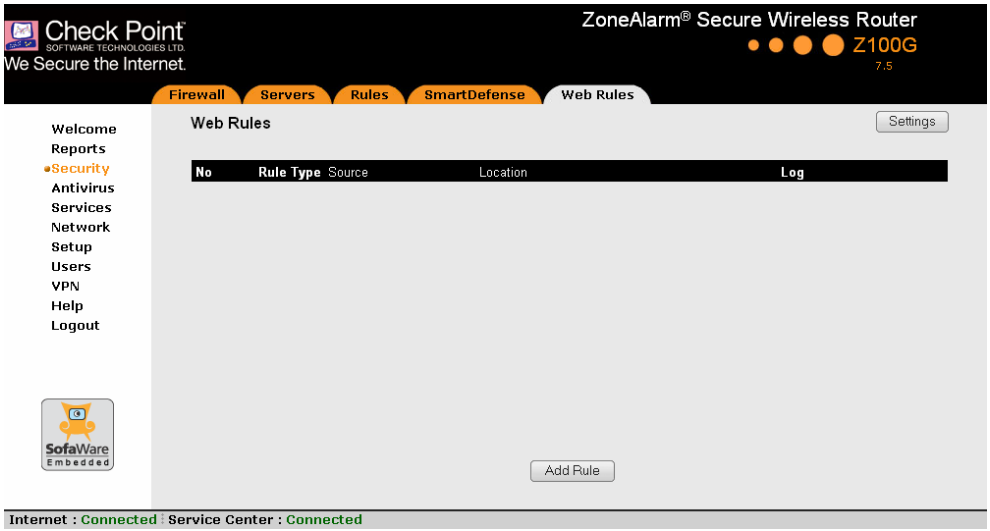
Rule	Description
Allow	This rule type enables you to specify that a specific Web page should be allowed.
Block	This rule type enables you to specify that a specific Web page should be blocked.

Adding and Editing Web Rules

To add or edit a Web rule

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

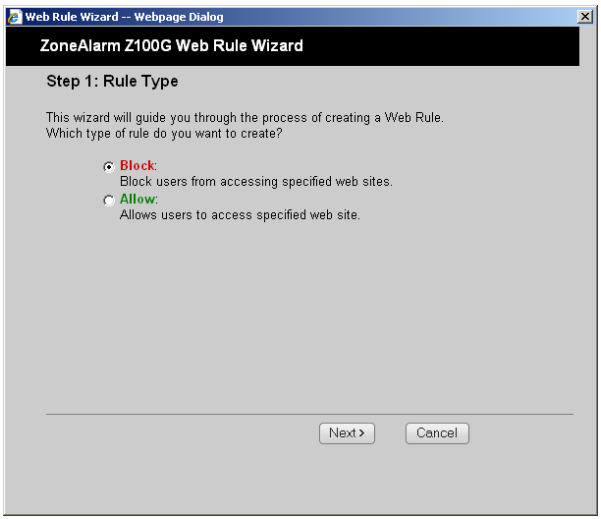
   The Web Rules page appears.



2. Do one of the following:

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

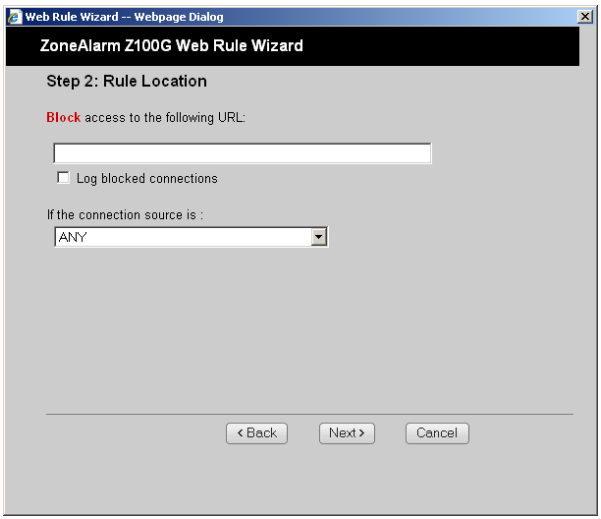
The ZoneAlarm Web Rule Wizard opens, with the Step 1: Rule Type dialog box displayed.



3. Select the type of rule you want to create.
4. Click Next.

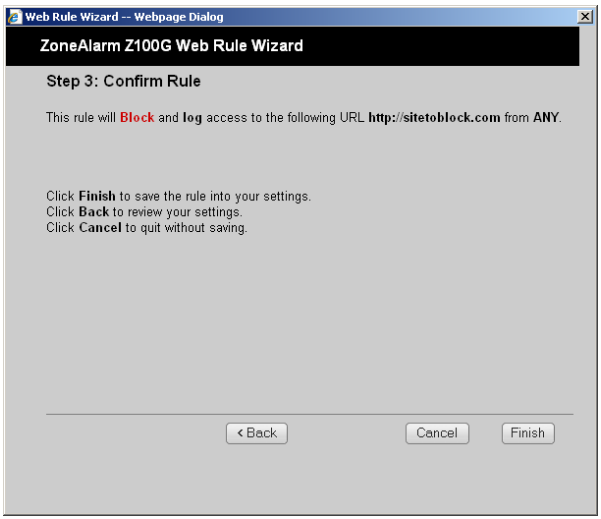
   The Step 2: Rule Location dialog box appears.

   The example below shows a Block rule.



5. Complete the fields using the relevant information in the following table.
6. Click Next.

   The Step 3: Confirm Rule dialog box appears.



7. Click Finish.

   The new rule appears in the Web Rules page.

Table 36: Web Rules Fields

In this field…	Do this…
Block/Allow access to the following URL	Type the URL or IP address to which the rule should apply. Wildcards (*) are supported. For example, to block all URLs that start with "http://www.casino-", set this field's value to: `http://www.casino-*` Note: If you block a Web site based on its domain name (http://<domain_name>), the Web site is not automatically blocked when surfing to the Web server's IP address (http://<IP_address>). Likewise, if you block a Web site based on its IP address, the Web site is not automatically blocked when surfing to the domain name. To prevent access to both the domain name and the IP address, you must block both.
Log allowed connections / Log blocked connections	Select this option to log the specified blocked or allowed connections. By default, allowed Web pages are not logged, and blocked Web pages are logged.
If the connection source is	Select the source of the connections you want to allow/block. To specify an IP address, select Specified IP and type the desired IP address in the field provided. To specify an IP address range, select Specified Range and type the desired IP address range in the fields provided.

Changing Web Rules' Priority

To change a Web rule's priority

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

   The Web Rules page appears.

2. Do one of the following:

   - Click ▲ next to the desired rule, to move the rule up in the table.
   - Click ▼ next to the desired rule, to move the rule down in the table.

   The rule's priority changes accordingly.

Viewing and Deleting Web Rules

To view or delete an existing Web rule

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

   The Web Rules page appears with a list of existing Web rules.

2. To delete a rule, do the following.

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

      A confirmation message appears.

   b. Click OK.

      The rule is deleted.

Customizing the Access Denied Page

The Access Denied page appears when a user attempts to access a page that is blocked either by a Web rule or by the Web Filtering service. You can customize this page using the following procedure.

For information on the Web Filtering service, see ***Web Filtering*** on page 276.

To customize the Access Denied page

1. Do one of the following:

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

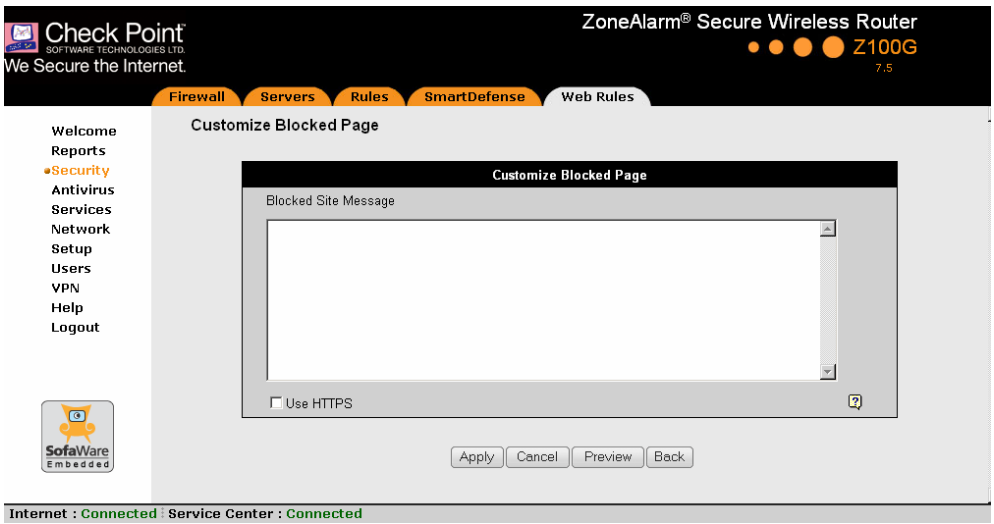
     The Web Rules page appears.

   - Click Services in the main menu, and click the Web Filtering tab.

     The Web Filtering page appears.

2. Click Settings.

   The Customize Blocked Page page appears. In the following example, this page was accessed via the Web Rules page.



3. In the text box, type the message that should appear when a user attempts to access a blocked Web page.

You can use HTML tags as needed.

4. To display the Access Denied page using HTTPS, select the Use HTTPS check box.
5. To preview the Access Denied page, click Preview.

   A browser window opens displaying the Access Denied page.
6. Click Apply.

   Your changes are saved.

Chapter 11

Using SmartDefense

This chapter explains how to use Check Point SmartDefense Services.

This chapter includes the following topics:

Overview

The ZoneAlarm router includes Check Point SmartDefense Services, based on Check Point Application Intelligence. SmartDefense provides a combination of attack safeguards and attack-blocking tools that protect your network in the following ways:

- Validating compliance to standards
- Validating expected usage of protocols (Protocol Anomaly Detection)
- Limiting application ability to carry malicious data
- Controlling application-layer operations

In addition, SmartDefense aids proper usage of Internet resources, such as FTP, instant messaging, Peer-to-Peer (P2P) file sharing, file-sharing operations, and File Transfer Protocol (FTP) uploading, among others.

Configuring SmartDefense

You can configure SmartDefense using the following tools:

- SmartDefense Wizard. Resets all SmartDefense settings to their defaults, and then creates a SmartDefense security policy according to your network and security preferences. See ***Using the SmartDefense Wizard*** on page 198.
- SmartDefense Tree. Enables you to fine tune individual settings in the SmartDefense policy. You can use the SmartDefense tree instead of, or in addition to, the wizard. See ***Using the SmartDefense Tree*** on page 203.

Using the SmartDefense Wizard

The SmartDefense Wizard allows you to configure your SmartDefense security policy quickly and easily through its user-friendly interface.

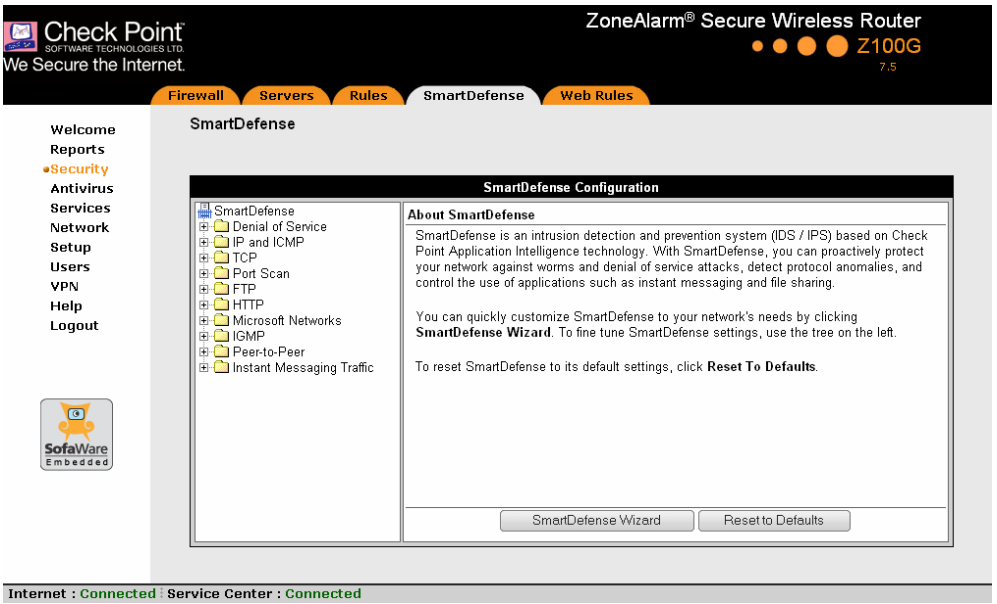
Note: The SmartDefense wizard clears any existing SmartDefense settings.

After using the wizard, you can fine tune the policy settings using the SmartDefense tree. See ***Using the SmartDefense Tree*** on page 203.

To configure the SmartDefense policy using the wizard

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

The SmartDefense page appears.



2. Click SmartDefense Wizard.

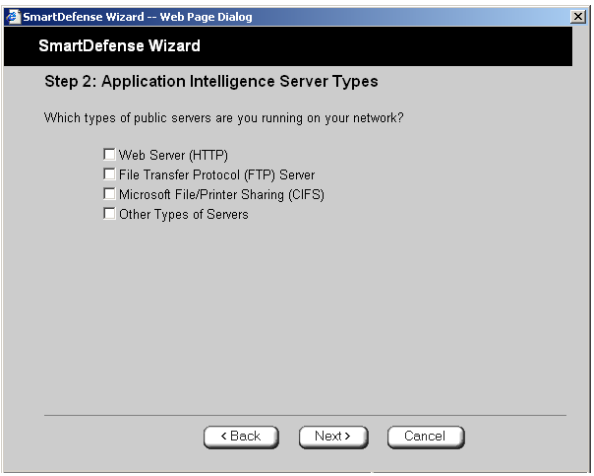
   The SmartDefense Wizard opens, with the Step 1: SmartDefense Level dialog box displayed.

3. Drag the lever to the desired level of SmartDefense enforcement.

For information on the levels, see the following table.

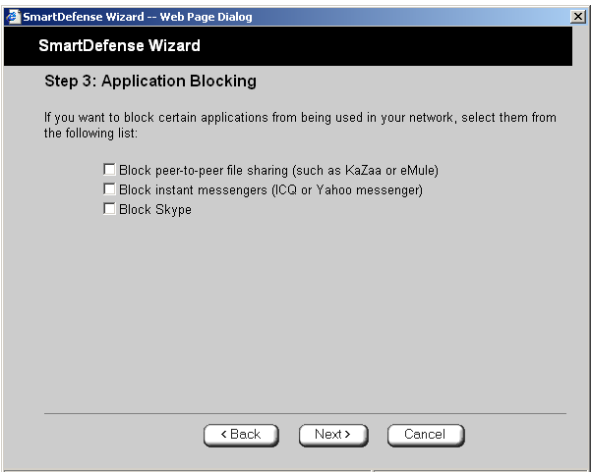
4. Click Next.

   The Step 2: Application Intelligence Server Types dialog box appears.



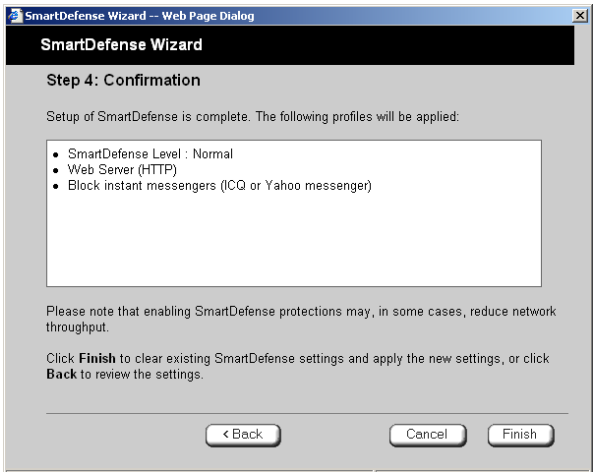
5. Select the check boxes next to the types of public servers that are running on your network.
6. Click Next.

   The Step 3: Application Blocking dialog box appears.



7. Select the check boxes next to the types of applications you want to block from running on your network.
8. Click Next.

   The Step 4: Confirmation dialog box appears.



9. Click Finish.

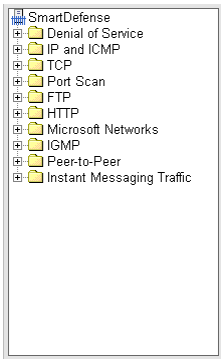
   Existing SmartDefense settings are cleared, and the security policy is applied.

Table 37: SmartDefense Security Levels

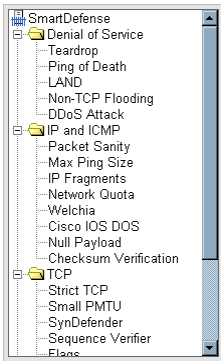
This level...	Does this...
Minimal	Disables all SmartDefense protections, except those that cannot be disabled.
Normal	Enables the following: • Teardrop • Ping of Death • LAND • Packet Sanity • Max Ping Size (set to 1500) • Welchia • Cisco IOS • Null Payload • IGMP • Small PMTU (Log Only) This level blocks the most common attacks.
High	Enables the same protections as Normal level, as well as the following: • Host Port Scan • Sweep Scan • HTTP Header Rejection • Strict TCP (Log Only)
Extra Strict	Enables the same protections as High level, as well as the following: • Strict TCP (Log + Block) • Small PMTU (Log + Block) • Max Ping Size (set to 512) • Network Quota

Using the SmartDefense Tree

For convenience, SmartDefense is organized as a tree, in which each branch represents a category of settings.



When a category is expanded, the settings it contains appear as nodes. For information on each category and the nodes it contains, see ***SmartDefense Categories*** on page 205.



Each node represents an attack type, a sanity check, or a protocol or service that is vulnerable to attacks. To control how SmartDefense handles a specific attack, you must configure the relevant node's settings.

To configure a SmartDefense node

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

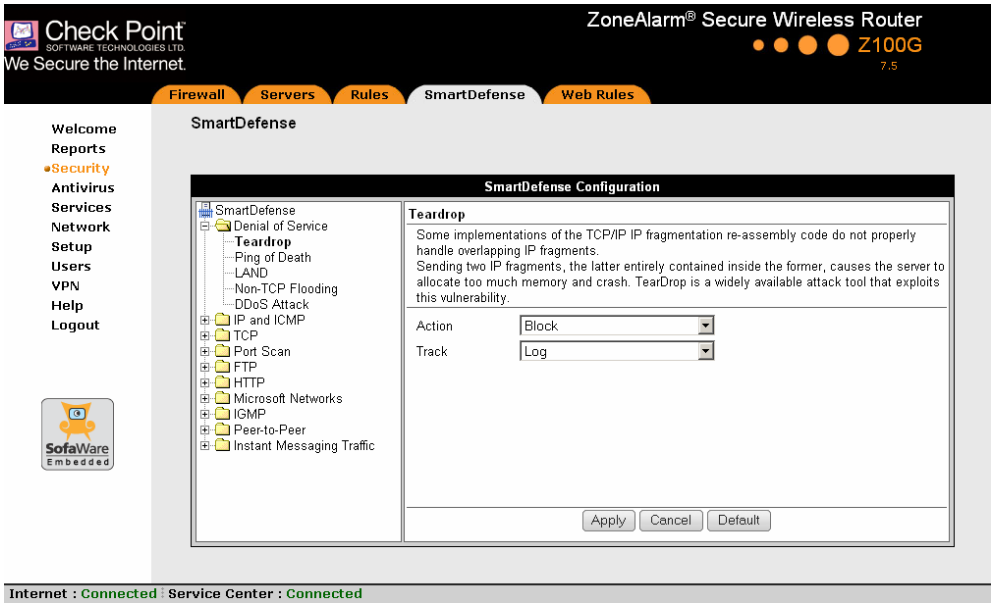
   The SmartDefense page appears.

   The left pane displays a tree containing SmartDefense categories.

   - To expand a category, click the ⊞ icon next to it.
   - To collapse a category, click the ⊟ icon next to it.

2. Expand the relevant category, and click on the desired node.

   The right pane displays a description of the node, followed by fields.



3. To modify the node's current settings, do the following:

   a) Complete the fields using the relevant information in ***SmartDefense Categories*** on page 205.

   b) Click Apply.

4. To reset the node to its default values:

a) Click Default.

A confirmation message appears.

b) Click OK.

The fields are reset to their default values, and your changes are saved.

SmartDefense Categories

SmartDefense includes the following categories:

- ***Denial of Service*** on page 205
- ***FTP*** on page 232
- ***HTTP*** on page 237
- ***IGMP*** on page 243
- ***Instant Messaging Traffic*** on page 244
- ***IP and ICMP*** on page 211
- ***Microsoft Networks*** on page 241
- ***Peer-to-Peer*** on page 239
- ***Port Scan*** on page 230
- ***TCP*** on page 223

Denial of Service

Denial of Service (DoS) attacks are aimed at overwhelming the target with spurious data, to the point where it is no longer able to respond to legitimate service requests.

This category includes the following attacks:

- ***DDoS Attack*** on page 210
- ***LAND*** on page 208
- ***Non-TCP Flooding*** on page 209
- ***Ping of Death*** on page 207
- ***Teardrop*** on page 206

Teardrop

In a Teardrop attack, the attacker sends two IP fragments, the latter entirely contained within the former. This causes some computers to allocate too much memory and crash.

You can configure how Teardrop attacks should be handled.

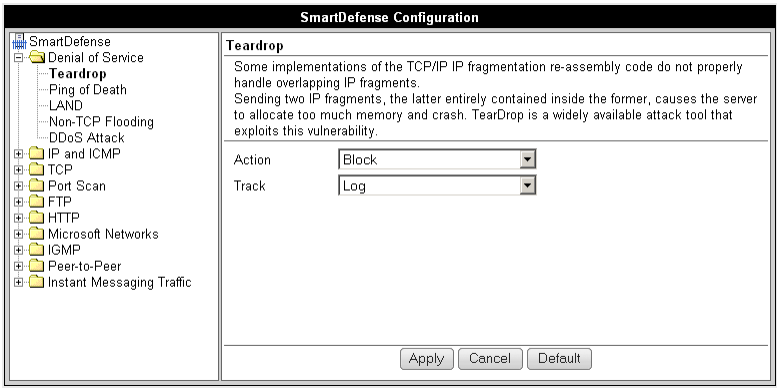


Table 38: Teardrop Fields

In this field…	Do this…
Action	Specify what action to take when a Teardrop attack occurs, by selecting one of the following: • Block. Block the attack. This is the default. • None. No action.
Track	Specify whether to log Teardrop attacks, by selecting one of the following: • Log. Log the attack. This is the default. • None. Do not log the attack.

Ping of Death

In a Ping of Death attack, the attacker sends a fragmented PING request that exceeds the maximum IP packet size (64KB). Some operating systems are unable to handle such requests and crash.

You can configure how Ping of Death attacks should be handled.

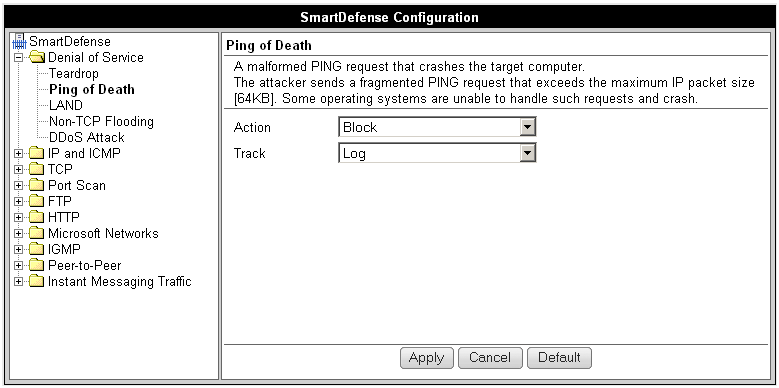


Table 39: Ping of Death Fields

In this field…	Do this…
Action	Specify what action to take when a Ping of Death attack occurs, by selecting one of the following: • Block. Block the attack. This is the default. • None. No action.
Track	Specify whether to log Ping of Death attacks, by selecting one of the following: • Log. Log the attack. This is the default. • None. Do not log the attack.

LAND

In a LAND attack, the attacker sends a SYN packet, in which the source address and port are the same as the destination (the victim computer). The victim computer then tries to reply to itself and either reboots or crashes.

You can configure how LAND attacks should be handled.

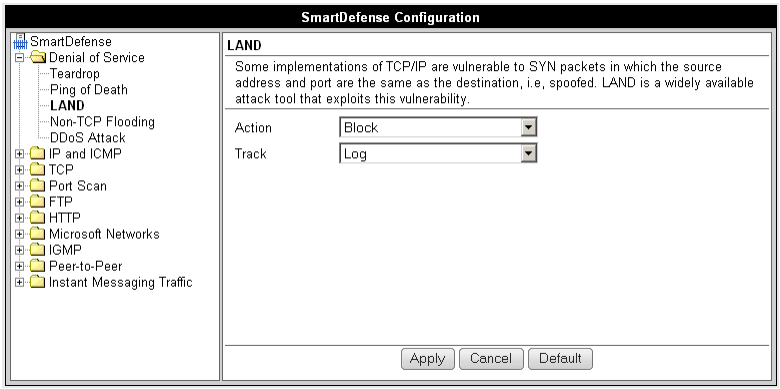


Table 40: LAND Fields

In this field...	Do this...
Action	Specify what action to take when a LAND attack occurs, by selecting one of the following: • Block. Block the attack. This is the default. • None. No action.
Track	Specify whether to log LAND attacks, by selecting one of the following: • Log. Log the attack. This is the default. • None. Do not log the attack.

Non-TCP Flooding

Advanced firewalls maintain state information about connections in a State table. In Non-TCP Flooding attacks, the attacker sends high volumes of non-TCP traffic. Since such traffic is connectionless, the related state information cannot be cleared or reset, and the firewall State table is quickly filled up. This prevents the firewall from accepting new connections and results in a Denial of Service (DoS).

You can protect against Non-TCP Flooding attacks by limiting the percentage of state table capacity used for non-TCP connections.

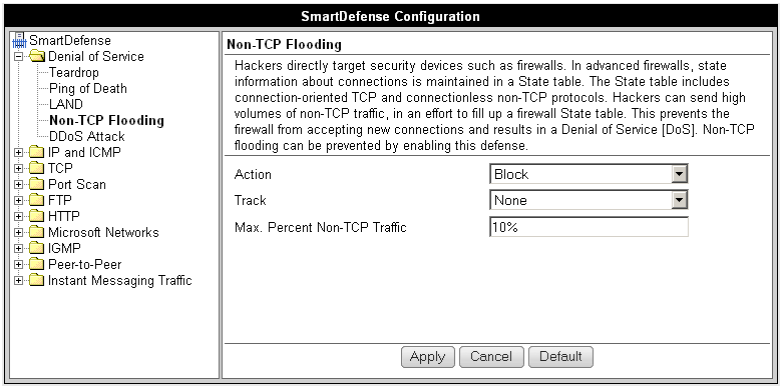


Table 41: Non-TCP Flooding Fields

In this field...	Do this...
Action	Specify what action to take when the percentage of state table capacity used for non-TCP connections reaches the Max. percent non TCP traffic threshold. Select one of the following: • Block. Block any additional non-TCP connections. • None. No action. This is the default.
Track	Specify whether to log non-TCP connections that exceed the Max. Percent Non-TCP Traffic threshold, by selecting one of the following: • Log. Log the connections. • None. Do not log the connections. This is the default.

In this field…	Do this…
Max. Percent Non-TCP Traffic	Type the maximum percentage of state table capacity allowed for non-TCP connections. The default value is 10%.

DDoS Attack

In a distributed denial-of-service attack (DDoS attack), the attacker directs multiple hosts in a coordinated attack on a victim computer or network. The attacking hosts send large amounts of spurious data to the victim, so that the victim is no longer able to respond to legitimate service requests.

You can configure how DDoS attacks should be handled.

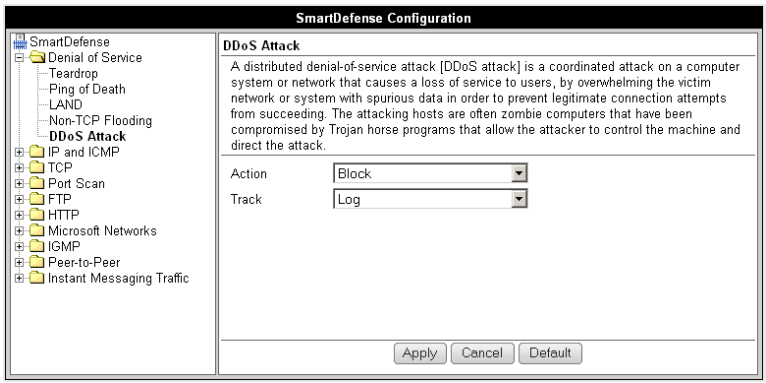


Table 42: Distributed Denial of Service Fields

In this field...	Do this...
Action	Specify what action to take when a DDoS attack occurs, by selecting one of the following: • Block. Block the attack. This is the default. • None. No action.
Track	Specify whether to log DDoS attacks, by selecting one of the following: • Log. Log the attack. This is the default. • None. Do not log the attack.

IP and ICMP

This category allows you to enable various IP and ICMP protocol tests, and to configure various protections against IP and ICMP-related attacks. It includes the following:

- ***Checksum Verification*** on page 222
- ***Cisco IOS DOS*** on page 219
- ***IP Fragments*** on page 215
- ***Max Ping Size*** on page 214
- ***Network Quota*** on page 217
- ***Null Payload*** on page 221
- ***Packet Sanity*** on page 212
- ***Welchia*** on page 218

Packet Sanity

Packet Sanity performs several Layer 3 and Layer 4 sanity checks. These include verifying packet size, UDP and TCP header lengths, dropping IP options, and verifying the TCP flags.

You can configure whether logs should be issued for offending packets.

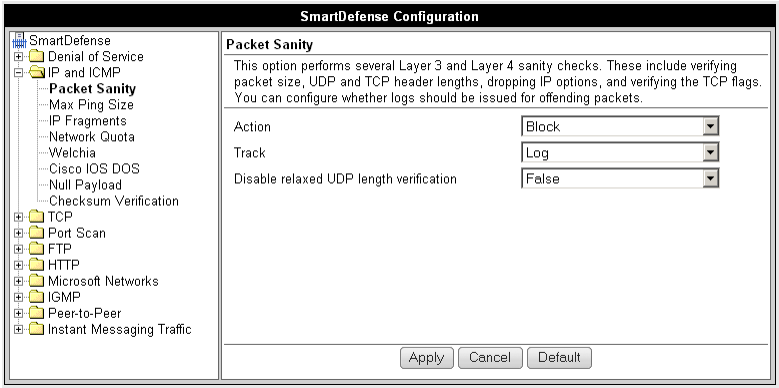


Table 43: Packet Sanity Fields

In this field…	Do this…
Action	Specify what action to take when a packet fails a sanity test, by selecting one of the following: • Block. Block the packet. This is the default. • None. No action.
Track	Specify whether to issue logs for packets that fail the packet sanity tests, by selecting one of the following: • Log. Issue logs. This is the default. • None. Do not issue logs.

In this field…	Do this…
Disable relaxed UDP length verification	The UDP length verification sanity check measures the UDP header length and compares it to the UDP header length specified in the UDP header. If the two values differ, the packet may be corrupted. However, since different applications may measure UDP header length differently, the ZoneAlarm router relaxes the UDP length verification sanity check by default, performing the check but not dropping offending packets. This is called relaxed UDP length verification. Specify whether the ZoneAlarm router should relax the UDP length verification sanity check or not, by selecting one of the following: • True. Disable relaxed UDP length verification. The ZoneAlarm router will drop packets that fail the UDP length verification check. • False. Do not disable relaxed UDP length verification. The ZoneAlarm router will not drop packets that fail the UDP length verification check. This is the default.

Max Ping Size

PING (ICMP echo request) is a program that uses ICMP protocol to check whether a remote machine is up. A request is sent by the client, and the server responds with a reply echoing the client's data.

An attacker can echo the client with a large amount of data, causing a buffer overflow. You can protect against such attacks by limiting the allowed size for ICMP echo requests.

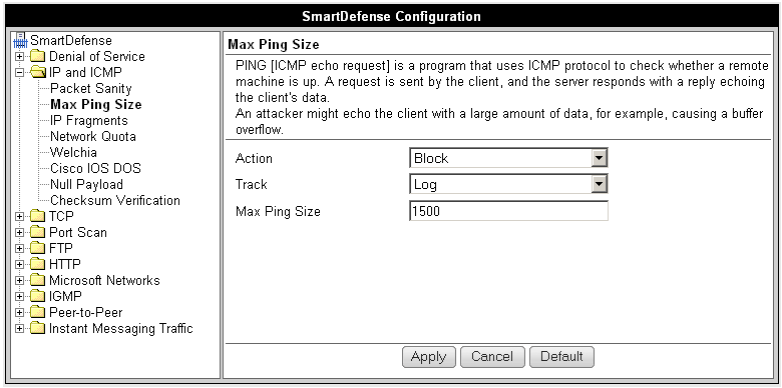


Table 44: Max Ping Size Fields

In this field…	Do this…
Action	Specify what action to take when an ICMP echo response exceeds the Max Ping Size threshold, by selecting one of the following: • Block. Block the request. This is the default. • None. No action.
Track	Specify whether to log ICMP echo responses that exceed the Max Ping Size threshold, by selecting one of the following: • Log. Log the responses. This is the default. • None. Do not log the responses.

In this field…	Do this…
Max Ping Size	Specify the maximum data size for ICMP echo response. The default value is 1500.

IP Fragments

When an IP packet is too big to be transported by a network link, it is split into several smaller IP packets and transmitted in fragments. To conceal a known attack or exploit, an attacker might imitate this common behavior and break the data section of a single packet into several fragmented packets. Without reassembling the fragments, it is not always possible to detect such an attack. Therefore, the ZoneAlarm router always reassembles all the fragments of a given IP packet, before inspecting it to make sure there are no attacks or exploits in the packet.

You can configure how fragmented packets should be handled.

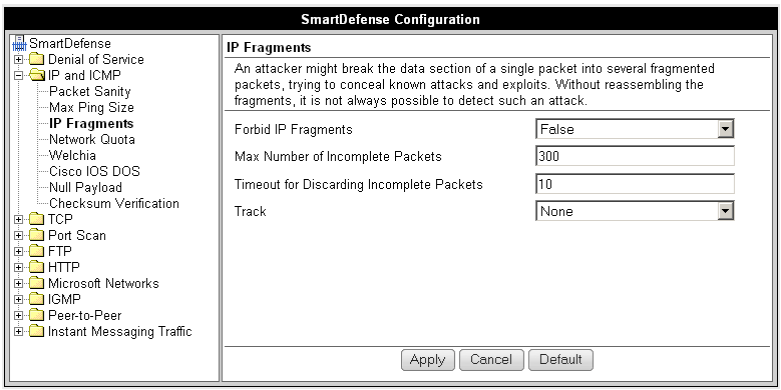


Table 45: IP Fragments Fields

In this field…	Do this…
Forbid IP Fragments	Specify whether all fragmented packets should be dropped, by selecting one of the following: • True. Drop all fragmented packets. • False. No action. This is the default. Under normal circumstances, it is recommended to leave this field set to False. Setting this field to True may disrupt Internet connectivity, because it does not allow any fragmented packets.
Max Number of Incomplete Packets	Type the maximum number of fragmented packets allowed. Packets exceeding this threshold will be dropped. The default value is 300.
Timeout for Discarding Incomplete Packets	When the ZoneAlarm router receives packet fragments, it waits for additional fragments to arrive, so that it can reassemble the packet. Type the number of seconds to wait before discarding incomplete packets. The default value is 10.
Track	Specify whether to log fragmented packets, by selecting one of the following: • Log. Log all fragmented packets. • None. Do not log the fragmented packets. This is the default.

Network Quota

An attacker may try to overload a server in your network by establishing a very large number of connections per second. To protect against Denial Of Service (DoS) attacks, Network Quota enforces a limit upon the number of connections per second that are allowed from the same source IP address.

You can configure how connections that exceed that limit should be handled.

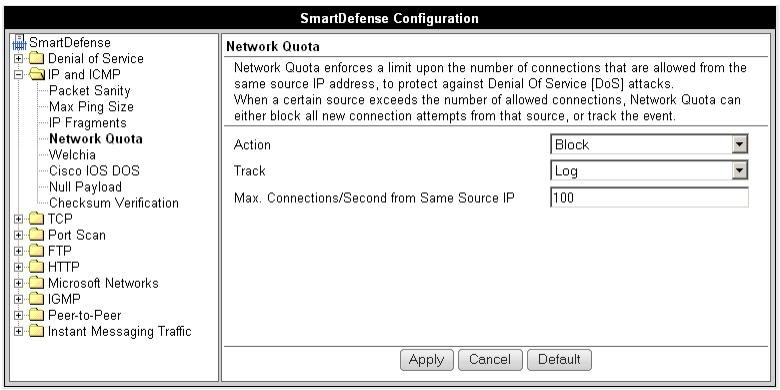


Table 46: Network Quota Fields

In this field...	Do this...
Action	Specify what action to take when the number of network connections from the same source reaches the Max. Connections/Second per Source IP threshold. Select one of the following: • Block. Block all new connections from the source. Existing connections will not be blocked. This is the default. • None. No action.
Track	Specify whether to log connections from a specific source that exceed the Max. Connections/Second per Source IP threshold, by selecting one of the following: • Log. Log the connections. This is the default. • None. Do not log the connections.

In this field…	Do this…
Max. Connections/Second from Same Source IP	Type the maximum number of network connections allowed per second from the same source IP address. The default value is 100. Set a lower threshold for stronger protection against DoS attacks. Note: Setting this value too low can lead to false alarms.

Welchia

The Welchia worm uses the MS DCOM vulnerability or a WebDAV vulnerability. After infecting a computer, the worm begins searching for other live computers to infect. It does so by sending a specific ping packet to a target and waiting for the reply that signals that the target is alive. This flood of pings may disrupt network connectivity.

You can configure how the Welchia worm should be handled.

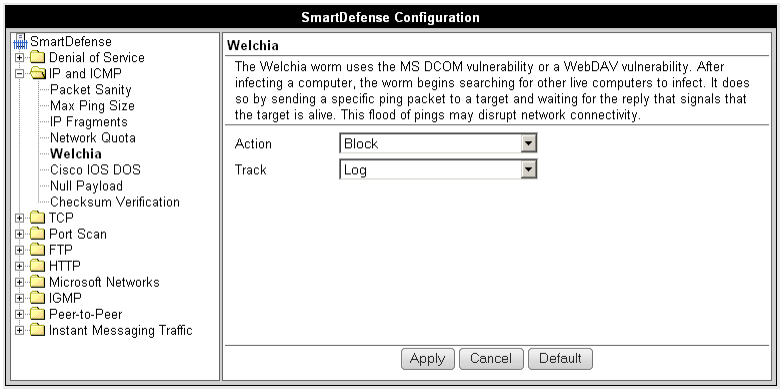


Table 47: Welchia Fields

In this field…	Do this…
Action	Specify what action to take when the Welchia worm is detected, by selecting one of the following: • Block. Block the attack. This is the default. • None. No action.
Track	Specify whether to log Welchia worm attacks, by selecting one of the following: • Log. Log the attack. This is the default. • None. Do not log the attack.

Cisco IOS DOS

Cisco routers are configured to process and accept Internet Protocol version 4 (IPv4) packets by default. When a Cisco IOS device is sent a specially crafted sequence of IPv4 packets (with protocol type 53 - SWIPE, 55 - IP Mobility, 77 - Sun ND, or 103 - Protocol Independent Multicast - PIM), the router will stop processing inbound traffic on that interface.

You can configure how Cisco IOS DOS attacks should be handled.

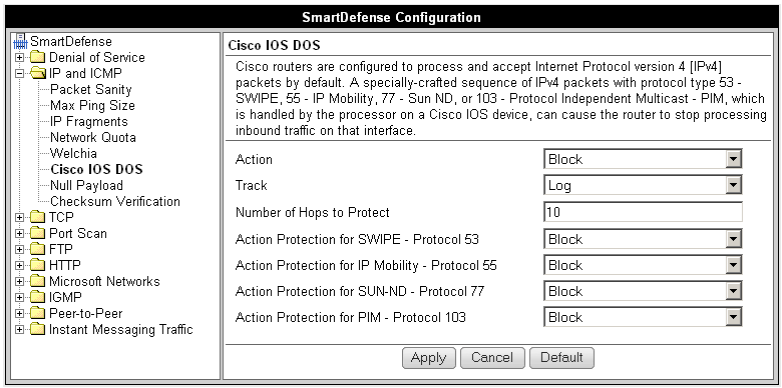


Table 48: Cisco IOS DOS

In this field…	Do this…
Action	Specify what action to take when a Cisco IOS DOS attack occurs, by selecting one of the following: • Block. Block the attack. This is the default. • None. No action.
Track	Specify whether to log Cisco IOS DOS attacks, by selecting one of the following: • Log. Log the attack. This is the default. • None. Do not log the attack.
Number of Hops to Protect	Type the number of hops from the enforcement module that Cisco routers should be protected. The default value is 10.
Action Protection for SWIPE - Protocol 53 / IP Mobility - Protocol 55 / SUN-ND - Protocol 77 / PIM - Protocol 103	Specify what action to take when an IPv4 packet of the specific protocol type is received, by selecting one of the following: • Block. Drop the packet. This is the default. • None. No action.

Null Payload

Some worms, such as Sasser, use ICMP echo request packets with null payload to detect potentially vulnerable hosts.

You can configure how null payload ping packets should be handled.

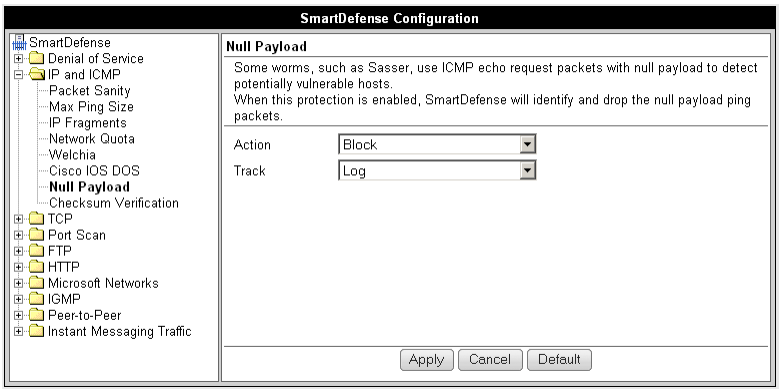


Table 49: Null Payload Fields

In this field…	Do this…
Action	Specify what action to take when null payload ping packets are detected, by selecting one of the following: • Block. Block the packets. This is the default. • None. No action.
Track	Specify whether to log null payload ping packets, by selecting one of the following: • Log. Log the packets. This is the default. • None. Do not log the packets.

Checksum Verification

SmartDefense identifies any IP, TCP, or UDP packets with incorrect checksums. You can configure how these packets should be handled.

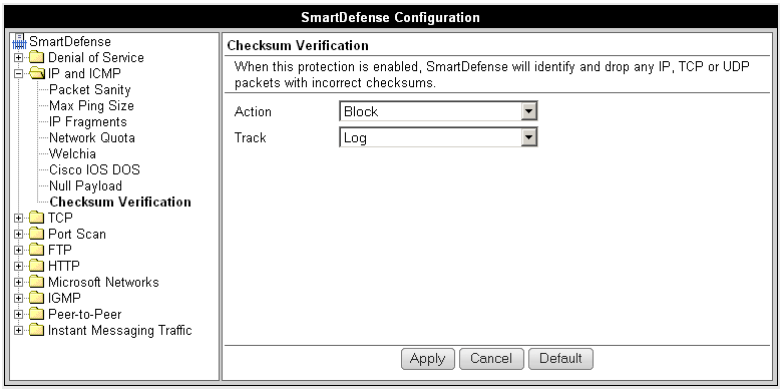


Table 50: Checksum Verification Fields

In this field…	Do this…
Action	Specify what action to take when packets with incorrect checksums are detected, by selecting one of the following: • Block. Block the packets. This is the default. • None. No action.
Track	Specify whether to log packets with incorrect checksums, by selecting one of the following: • Log. Log the packets. • None. Do not log the packets. This is the default.

TCP

This category allows you to configure various protections related to the TCP protocol. It includes the following:

- ***Flags*** on page 229
- ***Sequence Verifier*** on page 228
- ***Small PMTU*** on page 224
- ***Strict TCP*** on page 223
- ***SynDefender*** on page 226

Strict TCP

Out-of-state TCP packets are SYN-ACK or data packets that arrive out of order, before the TCP SYN packet.

Note: In normal conditions, out-of-state TCP packets can occur after the ZoneAlarm restarts, since connections which were established prior to the reboot are unknown. This is normal and does not indicate an attack.

You can configure how out-of-state TCP packets should be handled.

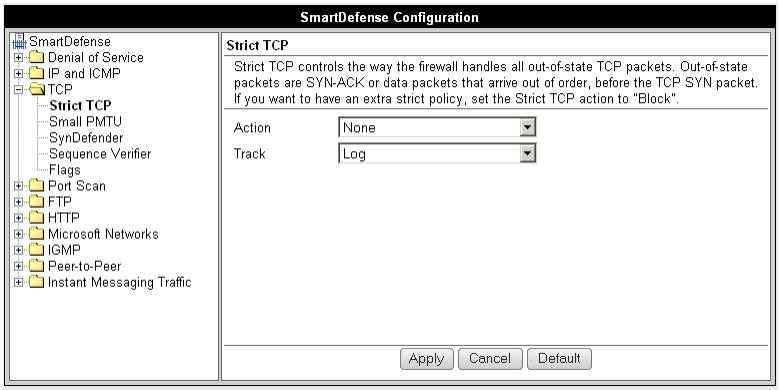


Table 51: Strict TCP

In this field…	Do this…
Action	Specify what action to take when an out-of-state TCP packet arrives, by selecting one of the following: • Block. Block the packets. • None. No action. This is the default.
Track	Specify whether to log null payload ping packets, by selecting one of the following: • Log. Log the packets. This is the default. • None. Do not log the packets.

Small PMTU

Small PMTU (Packet MTU) is a bandwidth attack in which the client fools the server into sending large amounts of data using small packets. Each packet has a large overhead that creates a "bottleneck" on the server.

You can protect against this attack by specifying a minimum packet size for data sent over the Internet.

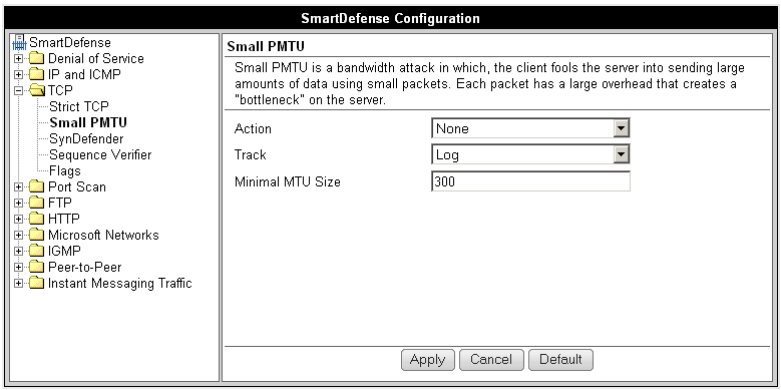


Table 52: Small PMTU Fields

In this field…	Do this…
Action	Specify what action to take when a packet is smaller than the Minimal MTU Size threshold, by selecting one of the following: • Block. Block the packet. • None. No action. This is the default.
Track	Specify whether to issue logs for packets are smaller than the Minimal MTU Size threshold, by selecting one of the following: • Log. Issue logs. This is the default. • None. Do not issue logs.
Minimal MTU Size	Type the minimum value allowed for the MTU field in IP packets sent by a client. An overly small value will not prevent an attack, while an overly large value might degrade performance and cause legitimate requests to be dropped. The default value is 300.

SynDefender

In a SYN attack, the attacker sends many SYN packets without finishing the three-way handshake. This causes the attacked host to be unable to accept new connections.

You can protect against this attack by specifying a maximum amount of time for completing handshakes.

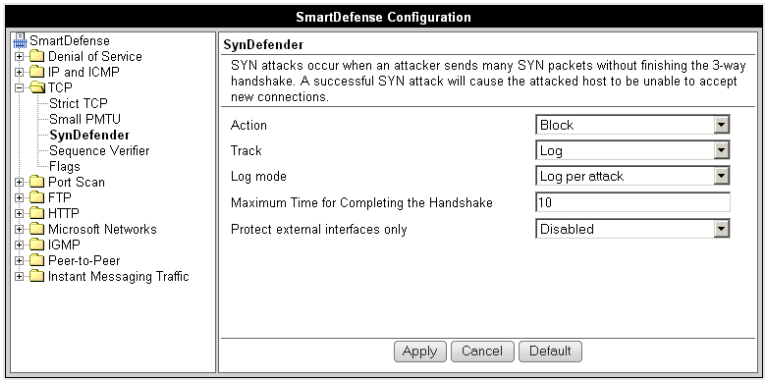


Table 53: SynDefender Fields

In this field…	Do this…
Action	Specify what action to take when a SYN attack occurs, by selecting one of the following: • Block. Block the packet. This is the default. • None. No action. A SYN attack is when more than 5 incomplete TCP handshakes are detected within 10 seconds. A handshake is considered incomplete when it exceeds the Maximum time for completing the handshake threshold.
Track	Specify whether to issue logs for the events specified by the Log Mode parameter, by selecting one of the following: • Log. Issue logs. This is the default. • None. Do not issue logs.

In this field…	Do this…
Log Mode	Specify upon which events logs should be issued, by selecting one of the following: • None. Do not issue logs. • Log per attack. Issue logs for each SYN attack. This is the default. • Log individual unfinished handshakes. Issue logs for each incomplete handshake. This field is only relevant if the Track field is set to Log.
Maximum time for completing the handshake	Type the maximum amount of time in seconds after which a TCP handshake is considered incomplete. The default value is 10 seconds.
Protect external interfaces only	Specify whether SynDefender should be enabled for external (WAN) interfaces only, by selecting one of the following: • Disabled. Enable SynDefender for all the firewall interfaces. This is the default. • Enabled. Enable SynDefender for external interfaces only.

Sequence Verifier

The ZoneAlarm router examines each TCP packet's sequence number and checks whether it matches a TCP connection state. You can configure how the router handles packets that match a TCP connection in terms of the TCP session but have incorrect sequence numbers.

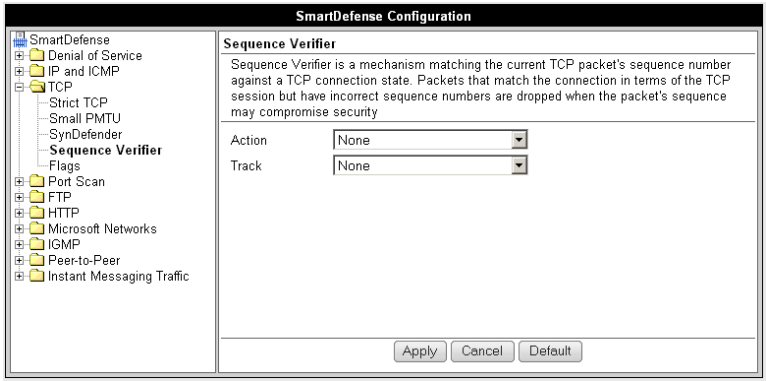


Table 54: Strict TCP

In this field…	Do this…
Action	Specify what action to take when TCP packets with incorrect sequence numbers arrive, by selecting one of the following: • Block. Block the packets. • None. No action. This is the default.
Track	Specify whether to log TCP packets with incorrect sequence numbers, by selecting one of the following: • Log. Log the packets. This is the default. • None. Do not log the packets.

Flags

The URG flag is used to indicate that there is urgent data in the TCP stream, and that the data should be delivered with high priority. Since handling of the URG flag is inconsistent between different operating systems, an attacker can use the URG flag to conceal certain attacks.

You can configure how the URG flag should be handled.

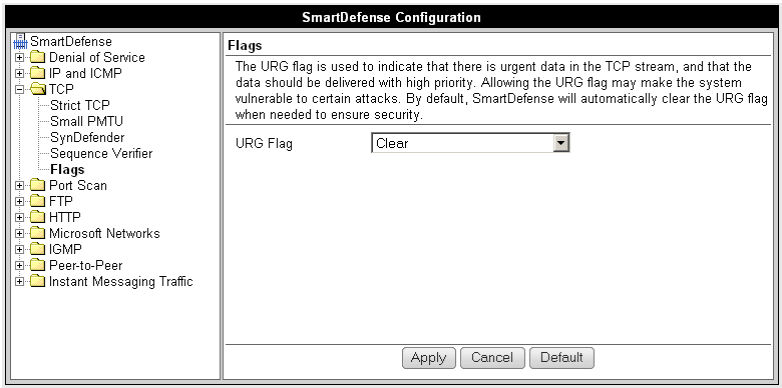


Table 55: Flags Fields

In this field…	Do this…
URG Flag	Specify whether to clear or allow the URG flag, by selecting one of the following: • Clear. Clear the URG flag on all incoming packets. This is the default. • Allow. Allow the URG flag.

Port Scan

An attacker can perform a port scan to determine whether ports are open and vulnerable to an attack. This is most commonly done by attempting to access a port and waiting for a response. The response indicates whether or not the port is open.

This category includes the following types of port scans:

- Host Port Scan. The attacker scans a specific host's ports to determine which of the ports are open.
- Sweep Scan. The attacker scans various hosts to determine where a specific port is open.

You can configure how the ZoneAlarm router should react when a port scan is detected.

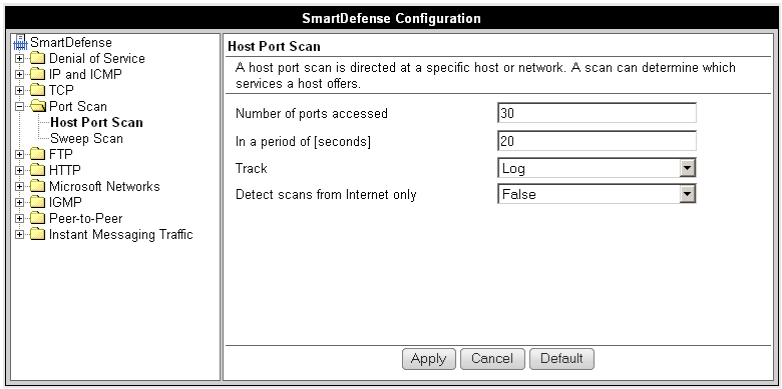


Table 56: Port Scan Fields

In this field…	Do this…
Number of ports accessed	SmartDefense detects ports scans by measuring the number of ports accessed over a period of time. The number of ports accessed must exceed the Number of ports accessed value, within the number of seconds specified by the In a period of [seconds] value, in order for SmartDefense to consider the activity a scan. Type the minimum number of ports that must be accessed within the In a period of [seconds] period, in order for SmartDefense to detect the activity as a port scan. For example, if this value is 30, and 40 ports are accessed within a specified period of time, SmartDefense will detect the activity as a port scan. For Host Port Scan, the default value is 30. For Sweep Scan, the default value is 50.
In a period of [seconds]	SmartDefense detects ports scans by measuring the number of ports accessed over a period of time. The number of ports accessed must exceed the Number of ports accessed value, within the number of seconds specified by the In a period of [seconds] value, in order for SmartDefense to consider the activity a scan. Type the maximum number of seconds that can elapse, during which the Number of ports accessed threshold is exceeded, in order for SmartDefense to detect the activity as a port scan. For example, if this value is 20, and the Number of ports accessed threshold is exceeded for 15 seconds, SmartDefense will detect the activity as a port scan. If the threshold is exceeded for 30 seconds, SmartDefense will not detect the activity as a port scan. The default value is 20 seconds.

In this field…	Do this…
Track	Specify whether to issue logs for scans, by selecting one of the following: • Log. Issue logs. This is the default. • None. Do not issue logs. This is the default.
Detect scans from Internet only	Specify whether to detect only scans originating from the Internet, by selecting one of the following: • False. Do not detect only scans from the Internet. This is the default. • True. Detect only scans from the Internet.

FTP

This category allows you to configure various protections related to the FTP protocol. It includes the following:

- ***Block Known Ports*** on page 234
- ***Block Port Overflow*** on page 235
- ***Blocked FTP Commands*** on page 236
- ***FTP Bounce*** on page 233

FTP Bounce

When connecting to an FTP server, the client sends a PORT command specifying the IP address and port to which the FTP server should connect and send data. An FTP Bounce attack is when an attacker sends a PORT command specifying the IP address of a third party instead of the attacker's own IP address. The FTP server then sends data to the victim machine.

You can configure how FTP bounce attacks should be handled.

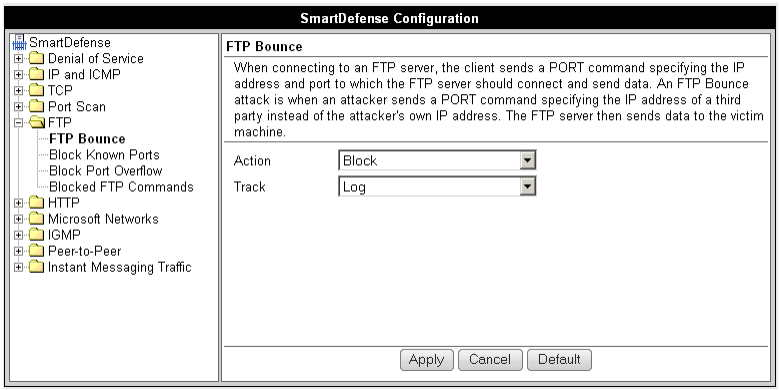


Table 57: FTP Bounce Fields

In this field...	Do this...
Action	Specify what action to take when an FTP Bounce attack occurs, by selecting one of the following: • Block. Block the attack. This is the default. • None. No action.
Track	Specify whether to log FTP Bounce attacks, by selecting one of the following: • Log. Log the attack. This is the default. • None. Do not log the attack.

Block Known Ports

You can choose to block the FTP server from connecting to well-known ports.

Note: Known ports are published ports associated with services (for example, SMTP is port 25).

This provides a second layer of protection against FTP bounce attacks, by preventing such attacks from reaching well-known ports.

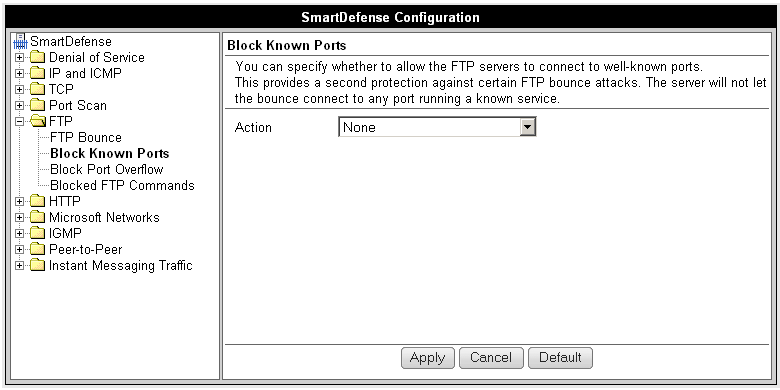


Table 58: Block Known Ports Fields

In this field…	Do this…
Action	Specify what action to take when the FTP server attempts to connect to a well-known port, by selecting one of the following: • Block. Block the connection. • None. No action. This is the default.

Block Port Overflow

FTP clients send PORT commands when connecting to the FTP sever. A PORT command consists of a series of numbers between 0 and 255, separated by commas.

To enforce compliance to the FTP standard and prevent potential attacks against the FTP server, you can block PORT commands that contain a number greater than 255.

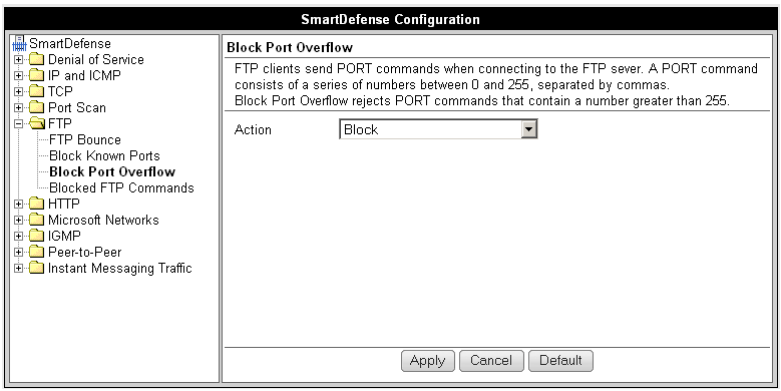
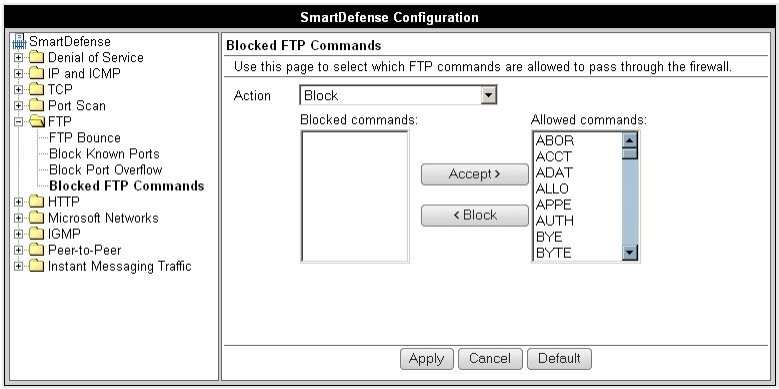


Table 59: Block Port Overflow

In this field…	Do this…
Action	Specify what action to take for PORT commands containing a number greater than 255, by selecting one of the following: • Block. Block the PORT command. This is the default. • None. No action.

Blocked FTP Commands

Some seldom-used FTP commands may compromise FTP server security and integrity. You can specify which FTP commands should be allowed to pass through the security server, and which should be blocked.



To enable FTP command blocking

- In the Action drop-down list, select Block.

  The FTP commands listed in the Blocked Commands box will be blocked.

  FTP command blocking is enabled by default.

To disable FTP command blocking

- In the Action drop-down list, select None.

  All FTP commands are allowed, including those in the Blocked Commands box.

To block a specific FTP command

1. In the Allowed Commands box, select the desired FTP command.
2. Click Block.

   The FTP command appears in the Blocked Commands box.
3. Click Apply.

   When FTP command blocking is enabled, the FTP command will be blocked.

To allow a specific FTP command

1. In the Blocked Commands box, select the desired FTP command.
2. Click Accept.

   The FTP command appears in the Allowed Commands box.
3. Click Apply.

   The FTP command will be allowed, regardless of whether FTP command blocking is enabled or disabled.

HTTP

This category allows you to configure various protections related to the HTTP protocol. It includes the following:

- ***Header Rejection*** on page 237
- ***Worm Catcher*** on page 238

Header Rejection

Some exploits are carried in standard HTTP headers with custom values (for example, in the Host header), or in custom HTTP headers. You can protect against such exploits by rejecting HTTP requests that contain specific headers and header values.

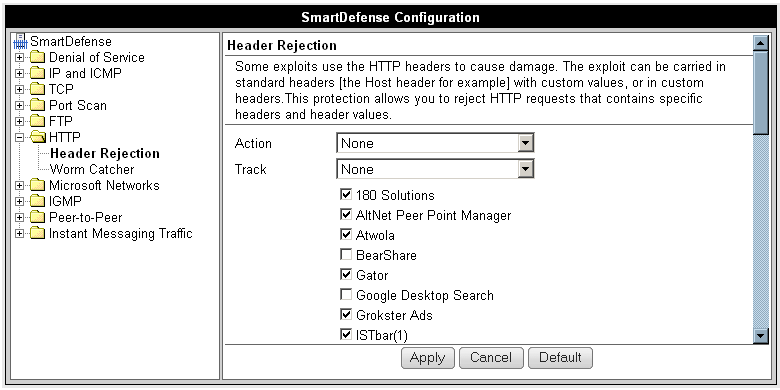


Table 60: Header Rejection Fields

In this field…	Do this…
Action	Specify what action to take when an HTTP header-based exploit is detected, by selecting one of the following: • Block. Block the attack. • None. No action. This is the default.
Track	Specify whether to log HTTP header-based exploits, by selecting one of the following: • Log. Log the attack. • None. Do not log the attack. This is the default.
HTTP header values list	Select the HTTP header values to detect.

Worm Catcher

A worm is a self-replicating malware (malicious software) that propagates by actively sending itself to new machines. Some worms propagate by using security vulnerabilities in the HTTP protocol.

You can specify how HTTP-based worm attacks should be handled.

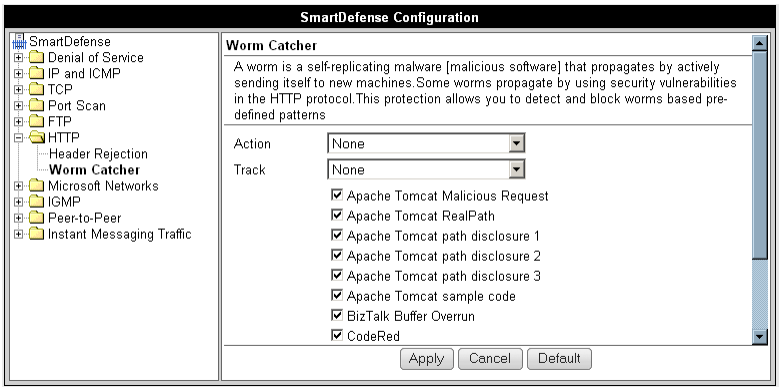


Table 61: Worm Catcher Fields

In this field…	Do this…
Action	Specify what action to take when an HTTP-based worm attack is detected, by selecting one of the following: • Block. Block the attack. • None. No action. This is the default.
Track	Specify whether to log HTTP-based worm attacks, by selecting one of the following: • Log. Log the attack. • None. Do not log the attack. This is the default.
HTTP-based worm patterns list	Select the worm patterns to detect.

Peer-to-Peer

SmartDefense can block peer-to-peer file-sharing traffic, by identifying the proprietary protocols and preventing the initial connection to the peer-to-peer networks. This prevents not only downloads, but also search operations.

This category includes the following nodes:

- BitTorrent
- eMule
- Gnutella
- KaZaA
- Winny

Note: SmartDefense can detect peer-to-peer traffic regardless of the TCP port being used to initiate the session.

In each node, you can configure how peer-to-peer connections of the selected type should be handled, using the following table.

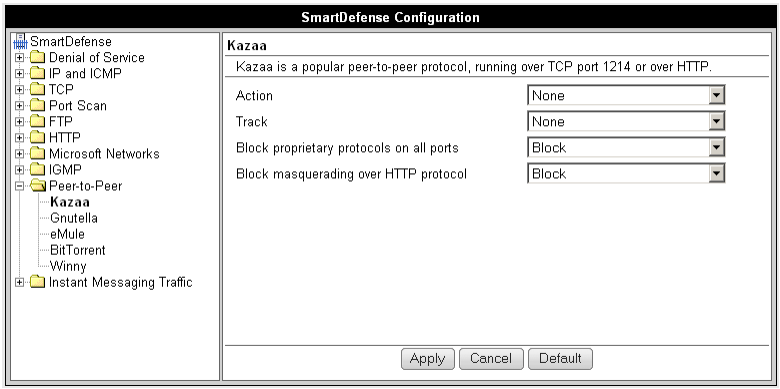


Table 62: Peer to Peer Fields

In this field…	Do this…
Action	Specify what action to take when a connection is attempted, by selecting one of the following: • Block. Block the connection. • None. No action. This is the default.
Track	Specify whether to log peer-to-peer connections, by selecting one of the following: • Log. Log the connection. • None. Do not log the connection. This is the default.
Block proprietary protocols on all ports	Specify whether proprietary protocols should be blocked on all ports, by selecting one of the following: • Block. Block the proprietary protocol on all ports. This in effect prevents all communication using this peer-to-peer application. This is the default. • None. Do not block the proprietary protocol on all ports.

In this field…	Do this…
Block masquerading over HTTP protocol	Specify whether to block using the peer-to-peer application over HTTP, by selecting one of the following: • Block. Block using the application over HTTP. This is the default. • None. Do not block using the application over HTTP. This field is not relevant for eMule and Winny.

Microsoft Networks

This category includes File and Print Sharing.

Microsoft operating systems and Samba clients rely on Common Internet File System (CIFS), a protocol for sharing files and printers. However, this protocol is also widely used by worms as a means of propagation.

You can configure how CIFS worms should be handled.

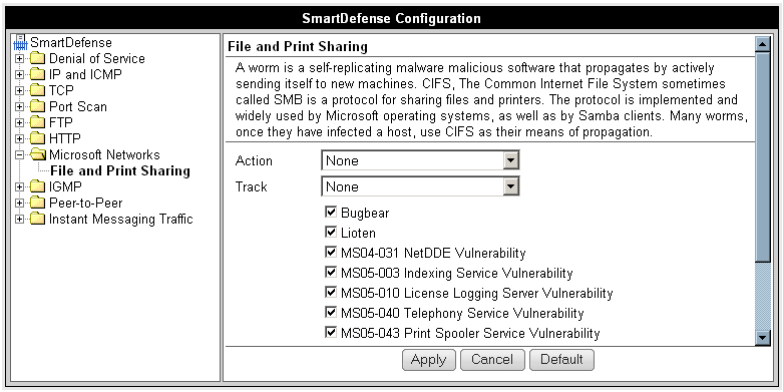


Table 63: File Print and Sharing Fields

In this field…	Do this…
Action	Specify what action to take when a CIFS worm attack is detected, by selecting one of the following: • Block. Block the attack. • None. No action. This is the default.
Track	Specify whether to log CIFS worm attacks, by selecting one of the following: • Log. Log the attack. • None. Do not log the attack. This is the default.
CIFS worm patterns list	Select the worm patterns to detect. Patterns are matched against file names (including file paths but excluding the disk share name) that the client is trying to read or write from the server.

IGMP

This category includes the IGMP protocol.

IGMP is used by hosts and routers to dynamically register and discover multicast group membership. Attacks on the IGMP protocol usually target a vulnerability in the multicast routing software/hardware used, by sending specially crafted IGMP packets.

You can configure how IGMP attacks should be handled.

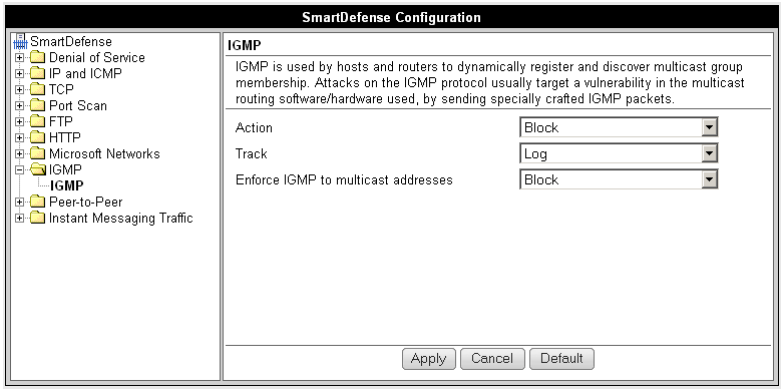


Table 64: IGMP Fields

In this field...	Do this...
Action	Specify what action to take when an IGMP attack occurs, by selecting one of the following: • Block. Block the attack. This is the default. • None. No action.
Track	Specify whether to log IGMP attacks, by selecting one of the following: • Log. Log the attack. This is the default. • None. Do not log the attack.

In this field…	Do this…
Enforce IGMP to multicast addresses	According to the IGMP specification, IGMP packets must be sent to multicast addresses. Sending IGMP packets to a unicast or broadcast address might constitute and attack; therefore the ZoneAlarm router blocks such packets. Specify whether to allow or block IGMP packets that are sent to non-multicast addresses, by selecting one of the following: • Block. Block IGMP packets that are sent to non-multicast addresses. This is the default. • None. No action.

Instant Messaging Traffic

SmartDefense can block instant messaging applications that use VoIP protocols, by identifying the messaging application's fingerprints and HTTP headers.

This category includes the following nodes:

- ICQ
- MSN Messenger
- Skype
- Yahoo

Note: SmartDefense can detect instant messaging traffic regardless of the TCP port being used to initiate the session.

Note: Skype versions up to 2.0.0.103 are supported.

In each node, you can configure how instant messaging connections of the selected type should be handled, using the following table.

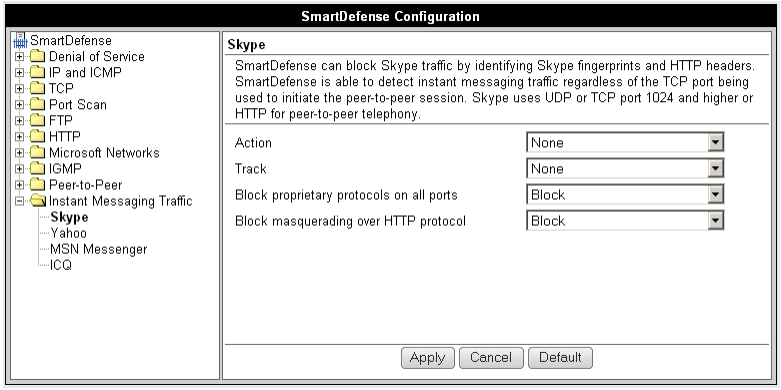


Table 65: Instant Messengers Fields

In this field…	Do this…
Action	Specify what action to take when a connection is attempted, by selecting one of the following: • Block. Block the connection. • None. No action. This is the default.
Track	Specify whether to log instant messenger connections, by selecting one of the following: • Log. Log the connection. • None. Do not log the connection. This is the default.

In this field…	Do this…
Block proprietary protocol / Block proprietary protocols on all ports	Specify whether proprietary protocols should be blocked on all ports, by selecting one of the following: • Block. Block the proprietary protocol on all ports. This in effect prevents all communication using this instant messenger application. This is the default. • None. Do not block the proprietary protocol on all ports.
Block masquerading over HTTP protocol	Specify whether to block using the instant messenger application over HTTP, by selecting one of the following: • Block. Block using the application over HTTP. This is the default. • None. Do not block using the application over HTTP.

Resetting SmartDefense to its Defaults

If desired, you can reset the SmartDefense security policy to its default settings. For information on the default value of each SmartDefense setting, see ***SmartDefense Categories*** on page 205.

For information on resetting individual nodes in the SmartDefense tree to their default settings, see ***Using the SmartDefense Tree*** on page 203.

To reset SmartDefense to its defaults

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

   The SmartDefense page appears.

2. Click Reset to Defaults.

   A confirmation message appears.

3. Click OK.

   The SmartDefense policy is reset to its default settings.

Chapter 12

Using VStream Antivirus

This chapter explains how to use the VStream Antivirus engine to block security threats before they reach your network.

This chapter includes the following topics:

Overview

The ZoneAlarm router includes VStream Antivirus, an embedded stream-based antivirus engine based on Check Point Stateful Inspection and Application Intelligence technologies, that performs virus scanning at the kernel level.

VStream Antivirus scans files for malicious content on the fly, without downloading the files into intermediate storage. This means minimal added latency and support for unlimited file sizes; and since VStream Antivirus stores only minimal state information per connection, it can scan thousands of connections concurrently. In order to scan archive files on the fly, VStream Antivirus performs real-time decompression and scanning of ZIP, TAR, and GZ archive files, with support for nested archive files.

When VStream Antivirus detects malicious content, the action it takes depends on the protocol in which the virus was found. See the following table. In each case, VStream Antivirus blocks the file and writes a log to the Event Log.

Table 66: VStream Antivirus Actions

If a virus if found in this protocol...	VStream Antivirus does this...	The protocol is detected on this port...
HTTP	• Terminates the connection	All ports on which VStream Antivirus is enabled by the policy, not only port 80
POP3	• Terminates the connection • Deletes the virus-infected email from the server	The standard TCP port 110.
IMAP	• Terminates the connection • Replaces the virus-infected email with a message notifying the user that a virus was found	The standard TCP port 143
SMTP	• Rejects the virus-infected email with error code 554 • Sends a "Virus detected" message to the sender	The standard TCP port 25
FTP	• Terminates the data connection • Sends a "Virus detected" message to the FTP client	The standard TCP port 21
TCP and UDP	• Terminates the connection	Generic TCP and UDP ports, other than those listed above

Note: In protocols that are not listed in this table, VStream Antivirus uses a "best effort" approach to detect viruses. In such cases, detection of viruses is not guaranteed and depends on the specific encoding used by the protocol.

If you are subscribed to the VStream Antivirus subscription service, VStream Antivirus virus signatures are automatically updated, so that security is always up-to-date, and your network is always protected.

Note: VStream Antivirus differs from the Email Antivirus subscription service (part of the Email Filtering service) in the following ways:

- Email Antivirus is centralized, redirecting traffic through the Service Center for scanning, while VStream Antivirus scans for viruses in the ZoneAlarm gateway itself.
- Email Antivirus is specific to email, scanning incoming POP3 and outgoing SMTP connections only, while VStream Antivirus supports additional protocols, including incoming SMTP and outgoing POP3 connections.

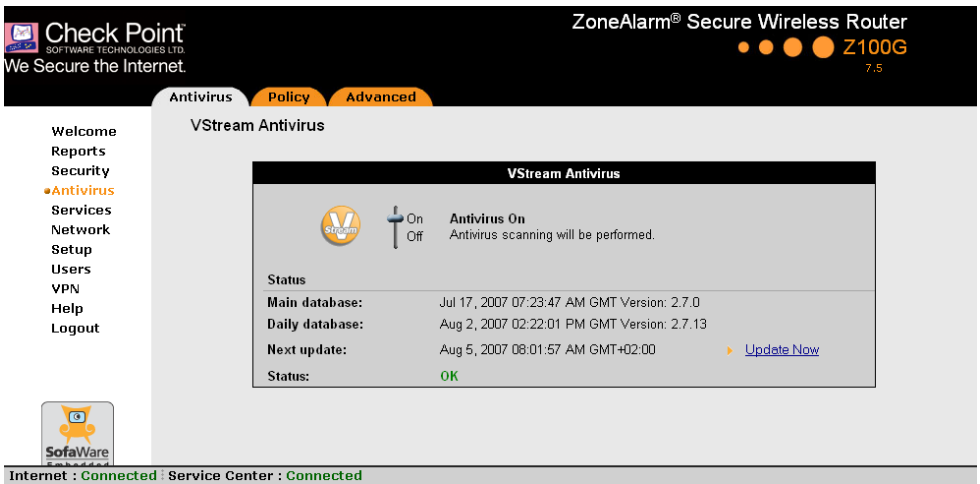
You can use either antivirus solution or both in conjunction. For information on Email Antivirus, see ***Email Filtering*** on page 282.

Enabling/Disabling VStream Antivirus

To enable/disable VStream Antivirus

1. Click Antivirus in the main menu, and click the Antivirus tab.

   The VStream Antivirus page appears.



2. Drag the On/Off lever upwards or downwards.

   VStream Antivirus is enabled/disabled for all internal network computers.

Viewing VStream Antivirus Signature Database Information

VStream Antivirus maintains two databases: a daily database and a main database. The daily database is updated frequently with the newest virus signatures. Periodically, the contents of the daily database are moved to the main database, leaving the daily database empty. This system of incremental updates to the main database allows for quicker updates and saves on network bandwidth.

You can view information about the VStream Antivirus signature databases currently in use, in the VStream Antivirus page.

Table 67: VStream Antivirus Page Fields

This field…	Displays…
Main database	The date and time at which the main database was last updated, followed by the version number.
Daily database	The date and time at which the daily database was last updated, followed by the version number.
Next update	The next date and time at which the ZoneAlarm router will check for updates.
Status	The current status of the database. This includes the following statuses: • Database Not Installed • OK

Configuring VStream Antivirus

You can configure VStream Antivirus in the following ways:

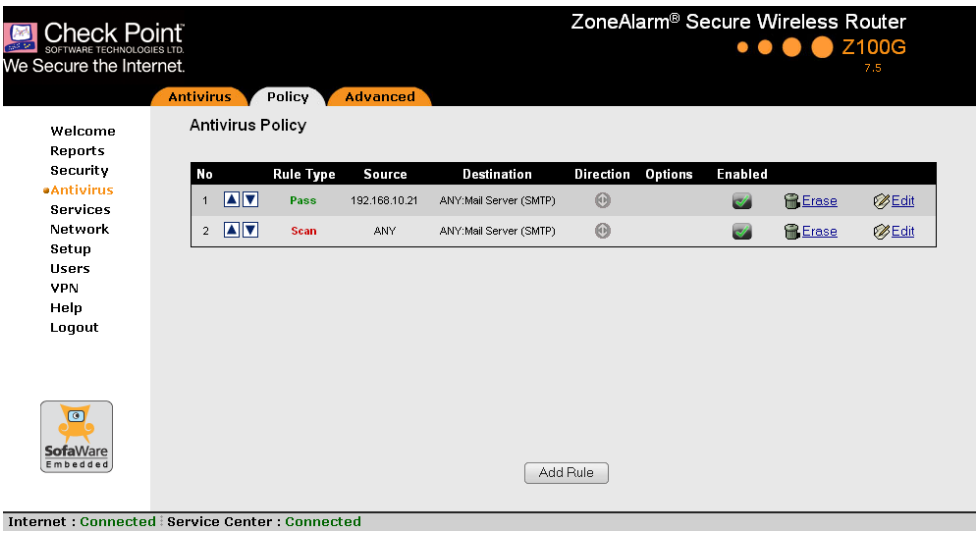
- ***Configuring the VStream Antivirus Policy*** on page 251
- ***Configuring VStream Antivirus Advanced Settings*** on page 261

Configuring the VStream Antivirus Policy

VStream Antivirus includes a flexible mechanism that allows the user to define exactly which traffic should be scanned, by specifying the protocol, ports, and source and destination IP addresses.

VStream Antivirus processes policy rules in the order they appear in the Antivirus Policy 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 scan all outgoing SMTP traffic, except traffic from a specific IP address, you can create a rule scanning all outgoing SMTP traffic and move the rule down in the Antivirus Policy table. Then create a rule passing SMTP traffic from the desired IP address and move this rule to a higher location in the Antivirus Policy table than the first rule. In the figure below, the general rule is rule number 2, and the exception is rule number 1.



The ZoneAlarm router will process rule 1 first, passing outgoing SMTP traffic from the specified IP address, and only then it will process rule 2, scanning all outgoing SMTP traffic.

The following rule types exist:

Table 68: VStream Antivirus Rule Types

Rule	Description
Pass	This rule type enables you to specify that VStream Antivirus should not scan traffic matching the rule.
Scan	This rule type enables you to specify that VStream Antivirus should scan traffic matching the rule. If a virus is found, it is blocked and logged.

Adding and Editing VStream Antivirus Rules

To add or edit a VStream Antivirus rule

1. Click Antivirus in the main menu, and click the Policy tab.

The Antivirus Policy page appears.

2. Do one of the following:

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

The VStream Policy Rule Wizard opens, with the Step 1: Rule Type dialog box displayed.

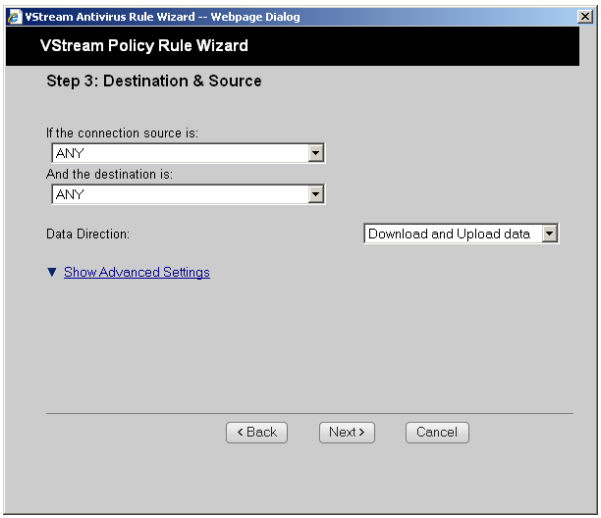
3. Select the type of rule you want to create.
4. Click Next.

   The Step 2: Service dialog box appears.

   The example below shows a Scan rule.

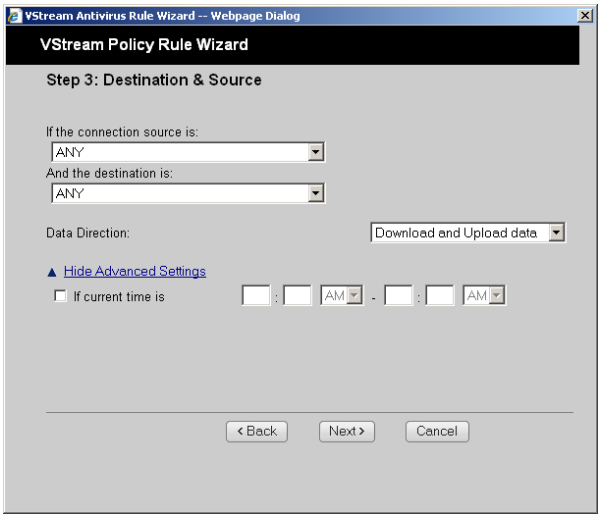
5. Complete the fields using the relevant information in the following table.
6. Click Next.

The Step 3: Destination & Source dialog box appears.



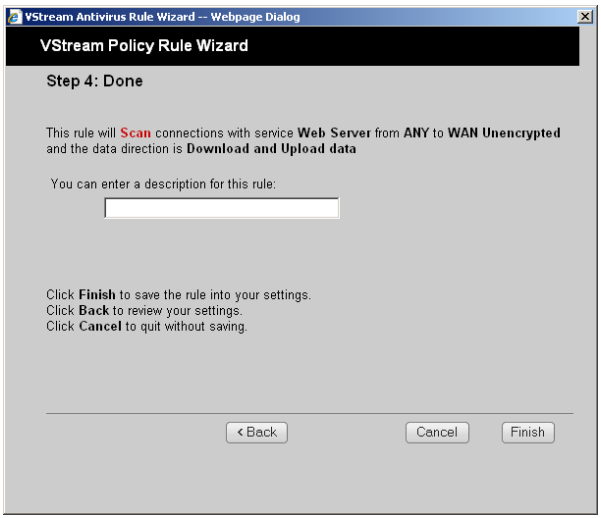
7. To configure advanced settings, click Show Advanced Settings.

   New fields appear.



8. Complete the fields using the relevant information in the following table.
9. Click Next.

The Step 4: Done dialog box appears.



10. If desired, type a description of the rule in the field provided.
11. Click Finish.

    The new rule appears in the Antivirus Policy page.

Table 69: VStream Antivirus 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 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 (TCP, UDP, or ANY) for which the rule should apply.
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.
If the connection source is	Select the source of the connections you want to allow/block. To specify an IP address, select Specified IP and type the desired IP address in the field provided. To specify an IP address range, select Specified Range and type the desired IP address range in the fields provided.
And the destination is	Select the destination of the connections you want to allow or block. To specify an IP address, select Specified IP and type the desired IP address in the text box. To specify an IP address range, select Specified Range and type the desired IP address range in the fields provided. To specify the ZoneAlarm Portal and network printers, select This Gateway. To specify any destination *except* the ZoneAlarm Portal and network printers, select ANY.

In this field…	Do this…
Data Direction	Select the direction of connections to which the rule should apply: • Download and Upload data. The rule applies to downloaded and uploaded data. This is the default. • Download data. The rule applies to downloaded data, that is, data flowing from the destination of the connection to the source of the connection. • Upload data. The rule applies to uploaded data, that is, data flowing from the source of the connection to the destination of the connection.
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.

Enabling/Disabling VStream Antivirus Rules

You can temporarily disable a VStream Antivirus rule.

To enable/disable a VStream Antivirus rule

1. Click Antivirus in the main menu, and click the Policy tab.

   The Antivirus Policy page appears.
2. Next to the desired rule, do one of the following:

   - To enable the rule, click  .

     The button changes to  and the rule is enabled.
   - To disable the rule, click  .

     The button changes to  and the rule is disabled.

Changing VStream Antivirus Rules' Priority

To change a VStream Antivirus rule's priority

1. Click Antivirus in the main menu, and click the Policy tab.

   The Antivirus Policy page appears.
2. Do one of the following:

   - Click  next to the desired rule, to move the rule up in the table.
   - Click  next to the desired rule, to move the rule down in the table.

   The rule's priority changes accordingly.

Viewing and Deleting VStream Antivirus Rules

To view or delete an existing VStream Antivirus rule

1. Click Antivirus in the main menu, and click the Policy tab.

   The Antivirus Policy page appears with a list of existing VStream Antivirus rules.

2. To view a rule's description, mouse-over the information icon in the desired rule's row.

   A tooltip displays the rule's description.

3. To delete a rule, do the following.

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

      A confirmation message appears.

   b. Click OK.

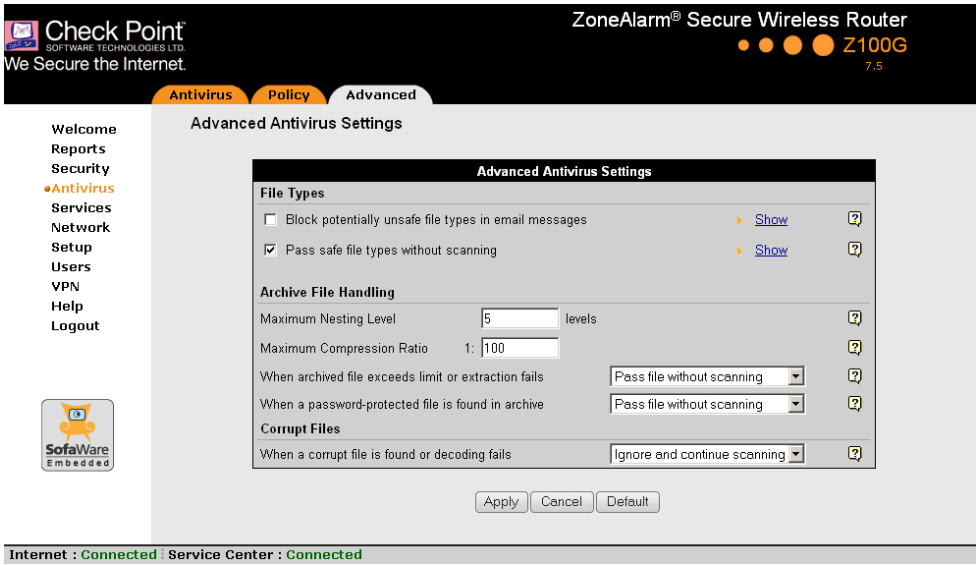
      The rule is deleted.

Configuring VStream Antivirus Advanced Settings

To configure VStream Antivirus advanced settings

1. Click Antivirus in the main menu, and click the Advanced tab.

   The Advanced Antivirus Settings page appears.



2. Complete the fields using the following table.
3. Click Apply.
4. To restore the default VStream Antivirus settings, do the following:

   a) Click Default.

      A confirmation message appears.

   b) Click OK.

      The VStream Antivirus settings are reset to their defaults. For information on the default values, refer to the following table.

Table 70: Advanced Antivirus Settings Fields

In this field…	Do this…
File Types	
Block potentially unsafe file types in email messages	Select this option to block all emails containing potentially unsafe attachments. Unsafe file types are: • DOS/Windows executables, libraries and drivers • Compiled HTML Help files • VBScript encoded files • Files with {CLSID} in their name • The following file extensions: ade, adp, bas, bat, chm, cmd,com, cpl, crt, exe, hlp, hta, inf, ins, isp, js, jse, lnk, mdb, mde, msc, msi, msp, mst, pcd, pif, reg, scr, sct, shs,shb, url, vb, vbe, vbs, wsc, wsf, wsh. To view a list of unsafe file types and their descriptions, click Show next to this option.

In this field…	Do this…
Pass safe file types without scanning	Select this option to accept common file types that are known to be safe, without scanning them. Safe files types are: • GIF • BMP • JFIF standard • EXIF standard • PNG • RIFF • RIFX • MPEG video stream • MPEG sys stream • Ogg Stream • MP3 file with ID3 version 2 • MP3 • PDF • PostScript • WMA/WMV/ASF • RealMedia file • JPEG - only the header is scanned, and the rest of the file is skipped To view a list of safe file types, click Show next to this option. Selecting this option reduces the load on the gateway by skipping safe file types. This option is selected by default.

In this field…	Do this…
Archive File Handling	
Maximum Nesting Level	Type the maximum number of nested content levels that VStream Antivirus should scan. Setting a higher number increases security. Setting a lower number prevents attackers from overloading the gateway by sending extremely nested archive files. The default value is 5 levels.
Maximum Compression Ratio 1:x	Fill in the field to complete the maximum compression ratio of files that VStream Antivirus should scan. For example, to specify a 1:80 maximum compression ratio, type 80. Setting a higher number allows the scanning of highly compressed files, but creates a potential for highly compressible files to create a heavy load on the router. Setting a lower number prevents attackers from overloading the gateway by sending extremely compressible files. The default value is 100.
When archived file exceeds limit or extraction fails	Specify how VStream Antivirus should handle files that exceed the Maximum nesting level or the Maximum compression ratio, and files for which scanning fails. Select one of the following: • Pass file without scanning. Scan only the number of levels specified, and skip the scanning of more deeply nested archives. Furthermore, skip scanning highly compressible files, and skip scanning archives that cannot be extracted because they are corrupt. This is the default. • Block file. Block the file.

In this field…	Do this…
When a password-protected file is found in archive	VStream Antivirus cannot extract and scan password-protected files inside archives. Specify how VStream Antivirus should handle such files, by selecting one of the following: • Pass file without scanning. Accept the file without scanning it. This is the default. • Block file. Block the file.
Corrupt Files	
When a corrupt file is found or decoding fails	Specify how VStream Antivirus should handle corrupt files and protocol anomalies, by selecting one of the following: • Ignore and continue scanning. Log the corrupt file or protocol anomaly, and scan the information on a best-effort basis. This is the default. • Block file. Block and log the corrupt file or protocol anomaly.

Updating VStream Antivirus

When you are subscribed to the VStream Antivirus updates service, VStream Antivirus virus signatures are automatically updated, keeping security up-to-date with no need for user intervention. However, you can still check for updates manually, if needed.

To update the VStream Antivirus virus signature database

1. Click Antivirus in the main menu, and click the Antivirus tab.

   The VStream Antivirus page appears.

2. Click Update Now.

   The VStream Antivirus database is updated with the latest virus signatures.

Chapter 13

Using Subscription Services

This chapter explains how to start subscription services, and how to use Software Updates, Web Filtering, and Email Filtering services.

Note: Check with your reseller regarding availability of subscription services, or surf to www.sofaware.com/servicecenters to locate a Service Center in your area.

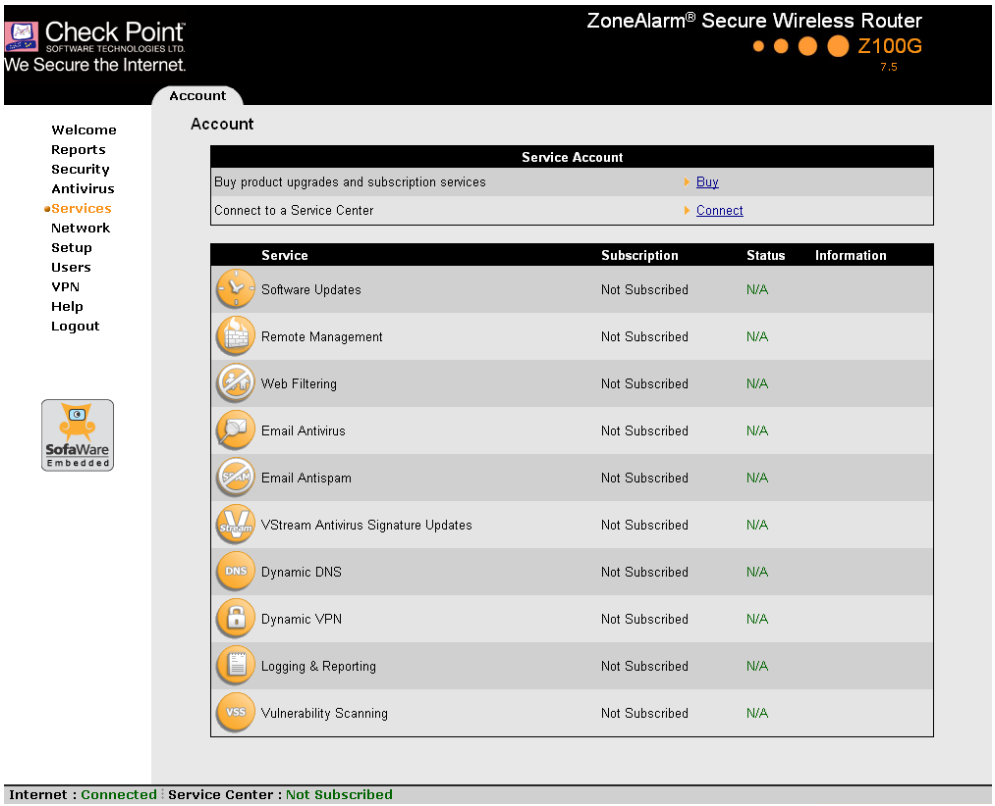
This chapter includes the following topics:

Connecting to a Service Center

To connect to a Service Center

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

The Account page appears.



2. In the Service Account area, click Connect.

The ZoneAlarm Services Wizard opens, with the Service Center dialog box displayed.

3. Make sure the Connect to a Service Center check box is selected.
4. Do one of the following:
   - To connect to the SofaWare Service Center, choose usercenter.sofaware.com.
   - To specify a Service Center, choose Specified IP and then in the Specified IP field, enter the desired Service Center's IP address, as given to you by your system administrator.
5. Click Next.
   - The Connecting screen appears.

- If the Service Center requires authentication, the Service Center Login dialog box appears.

Enter your gateway ID and registration key in the appropriate fields, as given to you by your service provider, then click Next.

- The Connecting screen appears.
- The Confirmation dialog box appears with a list of services to which you are subscribed.

6. Click Next.

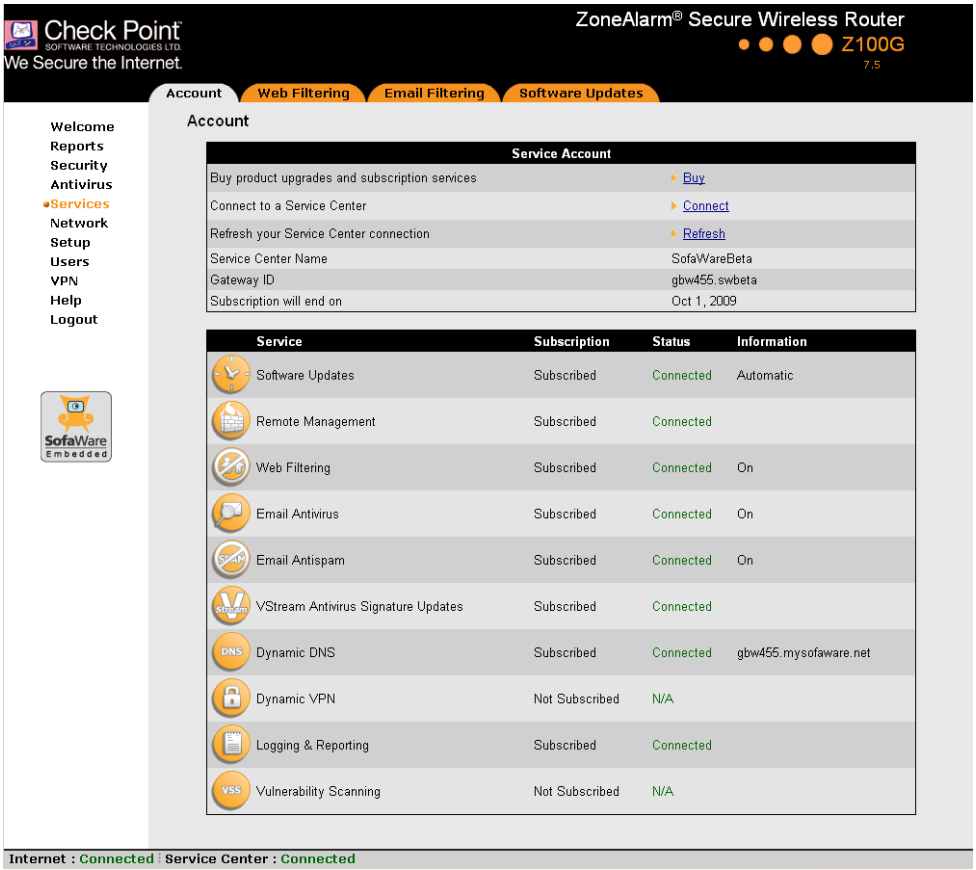
   The Done screen appears with a success message.

7. Click Finish.

   The following things happen:

   - If a new firmware is available, the ZoneAlarm router may start downloading it. This may take several minutes. Once the download is complete, the ZoneAlarm router restarts using the new firmware.
   - The Welcome page appears.

- The services to which you are subscribed are now available on your ZoneAlarm router and listed as such on the Account page. See ***Viewing Services Information*** on page 273 for further information.



- The Services submenu includes the services to which you are subscribed.

Viewing Services Information

The Account page displays the following information about your subscription.

Table 71: Account Page Fields

This field…	Displays…
Service Center Name	The name of the Service Center to which you are connected (if known).
Gateway ID	Your gateway ID.
Subscription will end on	The date on which your subscription to services will end.
Service	The services available in your service plan.
Subscription	The status of your subscription to each service: • Subscribed • Not Subscribed
Status	The status of each service: • Connected. You are connected to the service through the Service Center. • Connecting. Connecting to the Service Center. • N/A. The service is not available.
Information	The mode to which each service is set. If you are subscribed to Dynamic DNS, this field displays your gateway's domain name. For further information, see ***Web Filtering*** on page 276, ***Virus Scanning*** on page 282, and ***Automatic and Manual Updates*** on page 287.

Refreshing Your Service Center Connection

This option restarts your ZoneAlarm router's connection to the Service Center and refreshes your ZoneAlarm router's service settings.

To refresh your Service Center connection

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

   The Account page appears.

2. In the Service Account area, click Refresh.

   The ZoneAlarm router reconnects to the Service Center.

   Your service settings are refreshed.

Configuring Your Account

This option allows you to access your Service Center's Web site, which may offer additional configuration options for your account. Contact your Service Center for a user ID and password.

To configure your account

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

   The Account page appears.

2. In the Service Account area, click Configure.

Note: If no additional settings are available from your Service Center, this button will not appear.

   Your Service Center's Web site opens.

3. Follow the on-screen instructions.

Disconnecting from Your Service Center

If desired, you can disconnect from your Service Center.

To disconnect from your Service Center

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

   The Account page appears.

2. In the Service Account area, click Connect.

   The ZoneAlarm Services Wizard opens, with the first Subscription Services dialog box displayed.

3. Clear the Connect to a Service Center check box.

4. Click Next.

   The Done screen appears with a success message.

5. Click Finish.

   The following things happen:

   - You are disconnected from the Service Center.
   - The services to which you were subscribed are no longer available on your ZoneAlarm router.

Web Filtering

When the Web Filtering service is enabled, access to Web content is restricted according to the categories specified under Allow Categories. If a user attempts to access a blocked page, the Access Denied page appears. For information on customizing this page, see ***Customizing the Access Denied Page*** on page 195.

If desired, you can permit specific users to override Web Filtering. Such users will be able to view Web pages without restriction, after they have provided their username password via the Access Denied page. For information on granting Web Filtering override permissions, see ***Adding and Editing Users*** on page 313.

In addition, you can choose to exclude specific network objects from Web Filtering enforcement. Users connecting from these network objects will be able to view Web pages without restriction, regardless of whether they have Web Filtering override permissions. For information on configuring network objects, see ***Using Network Objects*** on page 95.

Note: The Web Filtering service is only available if you are connected to a Service Center and subscribed to this service.

Note: The Web Filtering subscription service differs from Web rules in the following ways:

- The category-based Web Filtering service is subscription-based and requires a connection to the Service Center, while Web rules are included with the ZoneAlarm router.
- The category-based Web Filtering service is centralized, extracting URLs from HTTP requests and sending the URLs to the Service Center to determine whether they should be blocked or allowed. With Web rules, HTTP requests are analyzed in the gateway itself.
- The Web Filtering service is category based; that is, it filters Web sites based on the category to which they belong. In contrast, Web rules allow and block specific URLs.

You can use either content filtering solution or both in conjunction. When a user attempts to access a Web site, the ZoneAlarm router first evaluates the Web rules. If the site is not blocked by the Web rules, the Web Filtering service is then consulted. For information on Web rules, see ***Using Web Rules*** on page 187.

Enabling/Disabling Web Filtering

To enable/disable Web Filtering

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

The Web Filtering page appears.

2. Drag the On/Off lever upwards or downwards.

   Web Filtering is enabled/disabled.

Selecting Categories for Blocking

You can define which types of Web sites should be considered appropriate for your family or office members, by selecting the categories. Categories marked with  will remain visible, while categories marked with  will be blocked and will require the administrator password for viewing.

Note: If the ZoneAlarm router is remotely managed, contact your Service Center administrator to change these settings.

Note: The list of supported categories may vary, depending on the Service Center to which the ZoneAlarm router is connected.

To allow/block a category

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

   The Web Filtering page appears.

2. In the Allow Categories area, click  or  next to the desired category.

Configuring Web Filtering Advanced Settings

Note: If the ZoneAlarm router is remotely managed, contact your Service Center administrator to change these settings.

To configure Web Filtering advanced settings

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

   The Web Filtering page appears.

2. Next to the Bypass scanning if Service Center is unavailable option, specify how the gateway should handle Web Filtering when the service is enabled and the Service Center is unavailable, by doing do one of the following:

   - To temporarily block all connections to the Internet, click  .

This ensures that users will not gain access to undesirable Web sites, even when the Service Center is unavailable.

The button changes to  .

- To temporarily allow all connections to the Internet, click  .

  This ensures continuous access to the Internet.

  The button changes to  .

When the Service Center is available again, the gateway will enforce the configured Web Filtering policy.

Temporarily Disabling Web Filtering

If desired, you can temporarily disable the Web Filtering service.

To temporarily disable Web Filtering

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

   The Web Filtering page appears.

2. Click Snooze.

   - Web Filtering is temporarily disabled for all internal network computers.

- The Snooze button changes to Resume.

- The Web Filtering Off popup window opens.

3. To re-enable the service, click Resume, either in the popup window, or on the Web Filtering page.

   - The service is re-enabled for all internal network computers.
   - If you clicked Resume in the Web Filtering page, the button changes to Snooze.

- If you clicked Resume in the Web Filtering Off popup window, the popup window closes.

Email Filtering

There are two Email Filtering services:

- Email Antivirus

  When the Email Antivirus service is enabled, your email is automatically scanned for the detection and elimination of all known viruses and vandals. If a virus is detected, it is removed and replaced with a warning message.

Note: The Email Antivirus subscription service differs from VStream Antivirus in the following ways:

- Email Antivirus is centralized, redirecting traffic through the Service Center for scanning, while VStream Antivirus scans for viruses in the ZoneAlarm gateway itself.
- Email Antivirus is specific to email, scanning incoming POP3 and outgoing SMTP connections only, while VStream Antivirus supports additional protocols, including incoming SMTP and outgoing POP3 connections.

You can use either antivirus solution or both in conjunction. For information on VStream Antivirus, see ***Using VStream Antivirus*** on page 247.

- Email Antispam

  When the Email Antispam service is enabled, your email is automatically scanned for the detection of spam. If spam is detected, the email's Subject line is modified to indicate that it is suspected spam. You can create rules to divert such messages to a special folder.

Note: Email Filtering services are only available if you are connected to a Service Center and subscribed to the services.

Enabling/Disabling Email Filtering

To enable/disable Email Filtering

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

   The Email Filtering page appears.

2. Next to Email Antivirus, drag the On/Off lever upwards or downwards.

   Email Antivirus is enabled/disabled.

Selecting Protocols for Scanning

If you are locally managed, you can define which protocols should be scanned for viruses and spam:

- Email retrieving (POP3). If enabled, all incoming email in the POP3 protocol will be scanned.
- Email sending (SMTP). If enabled, all outgoing email will be scanned.

Protocols marked with  will be scanned, while those marked with  will not.

Note: If the ZoneAlarm router is remotely managed, contact your Service Center administrator to change these settings.

To enable virus and spam scanning for a protocol

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

   The Email Filtering page appears.

2. In the Options area, click  or  next to the desired protocol.

Configuring Email Filtering Advanced Settings

Note: If the ZoneAlarm router is remotely managed, contact your Service Center administrator to change these settings.

To configure Email Filtering advanced settings

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

   The Email Filtering page appears.

2. Next to the Bypass scanning if Service Center is unavailable option, specify how the gateway should handle Email Filtering when the service is enabled and the Service Center is unavailable, by doing do one of the following:

   - To temporarily block all email traffic, click  .

     This ensures constant protection from spam and viruses.

     The button changes to  .

   - To temporarily allow all email traffic, click  .

     This ensures continuous access to email; however, it does not protect against viruses and spam, so use this option cautiously.

     The button changes to  .

   When the Service Center is available again, the gateway will enforce the configured Email Filtering policy.

Temporarily Disabling Email Filtering

If you are having problems sending or receiving email you can temporarily disable the Email Filtering services.

To temporarily disable Email Filtering

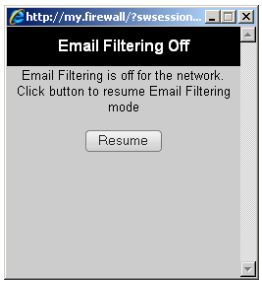
1. Click Services in the main menu, and click the Email Filtering tab.

   The Email Filtering page appears.

2. Click Snooze.

   - Email Antivirus and Email Antispam are temporarily disabled for all internal network computers.
   - The Snooze button changes to Resume.

- The Email Filtering Off popup window opens.



3. To re-enable Email Antivirus and Email Antispam, click Resume, either in the popup window, or on the Email Filtering page.

   - The services are re-enabled for all internal network computers.
   - If you clicked Resume in the Email Filtering page, the button changes to Snooze.
   - If you clicked Resume in the Email Filtering Off popup window, the popup window closes.

Automatic and Manual Updates

The Software Updates service enables you to check for new security and software updates.

Note: Software Updates are only available if you are connected to a Service Center and subscribed to this service.

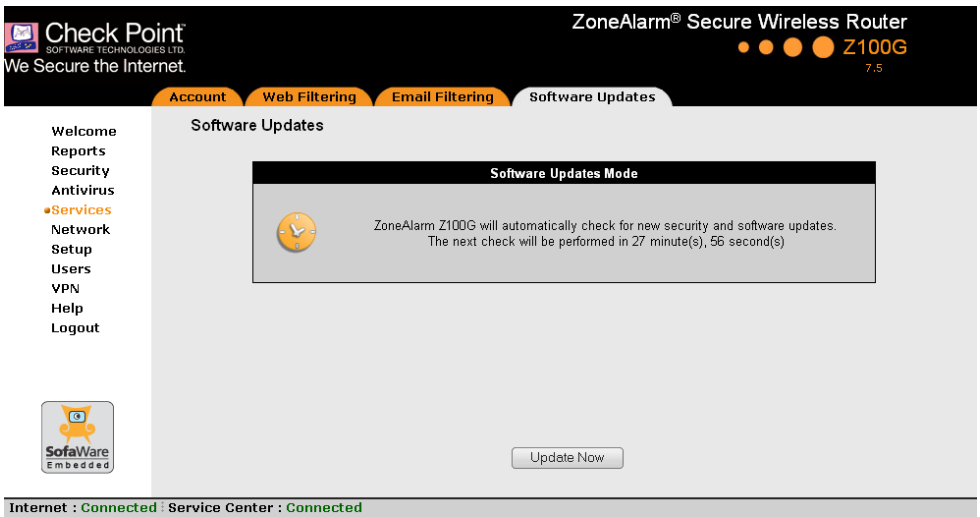
Checking for Software Updates when Remotely Managed

If your ZoneAlarm router is remotely managed, it automatically checks for software updates and installs them without user intervention. However, you can still check for updates manually, if needed.

To manually check for security and software updates

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

   The Software Updates page appears.



2. Click Update Now.

   The system checks for new updates and installs them.

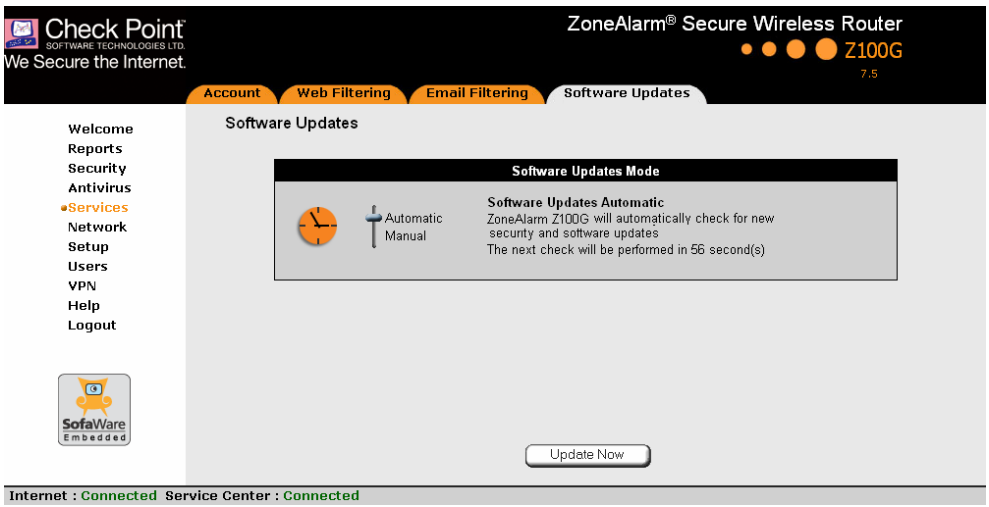
Checking for Software Updates when Locally Managed

If your ZoneAlarm router is locally managed, you can set it to automatically check for software updates, or you can set it so that software updates must be checked for manually.

To configure software updates when locally managed

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

   The Software Updates page appears.



2. To set the ZoneAlarm router to automatically check for and install new software updates, drag the Automatic/Manual lever upwards.

   The ZoneAlarm router checks for new updates and installs them according to its schedule.

Note: When the Software Updates service is set to Automatic, you can still manually check for updates.

3. To set the ZoneAlarm router so that software updates must be checked for manually, drag the Automatic/Manual lever downwards.

   The ZoneAlarm router does not check for software updates automatically.

4. To manually check for software updates, click Update Now.

   The system checks for new updates and installs them.

Chapter 14

Secure Remote Access

This chapter describes how to use your ZoneAlarm router as a Remote Access VPN Server.

This chapter includes the following topics:

Overview

You can configure your ZoneAlarm router as a Remote Access VPN Server. A Remote Access VPN (virtual private network) Server allows you to connect to your home or home office network from a remote location, while securing the traffic with data encryption and strong authentication.

The ZoneAlarm VPN Server accepts connections from devices installed with Check Point SecureClient/SecuRemote VPN Client software, or from other Check Point security appliances which include a built-in SecuRemote VPN Client, such as Check Point Safe@Office.

ZoneAlarm allows a single VPN user to connect. If you need to allow VPN remote access to multiple users, consider purchasing a Check Point Safe@Office gateway.

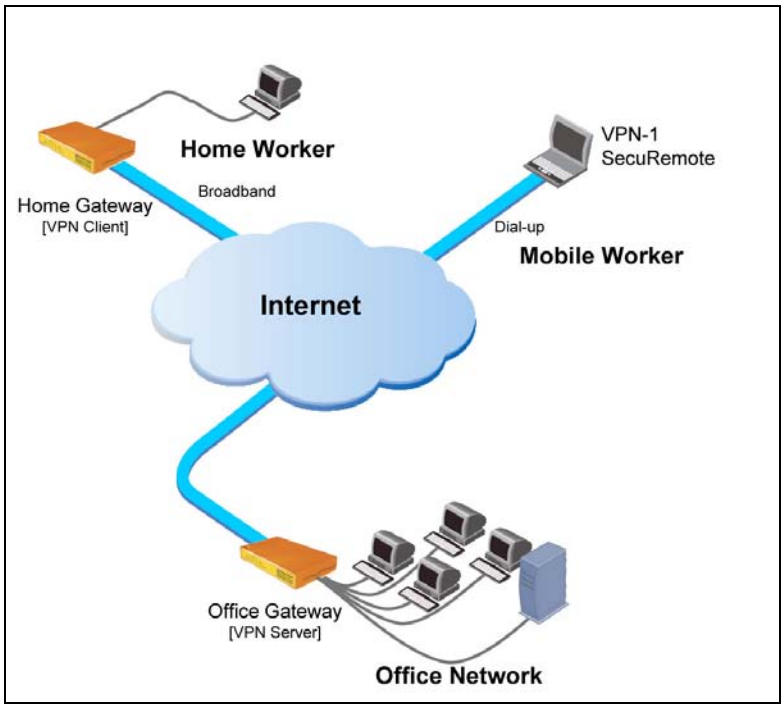


Figure 8: Remote Access VPN

Note: A locally managed Remote Access VPN Server must have a static IP address. If you need a Remote Access VPN Server with a dynamic IP address, you must use SofaWare Security Management Portal (SMP) management.

Note: SecureClient/SecuRemote supports split tunneling, which means that VPN Clients can connect directly to the Internet, while traffic to and from VPN sites passes through the VPN Server.

Note: This chapter explains how to define a VPN locally. However, if your router is centrally managed by a Service Center, then the Service Center can automatically deploy VPN configuration for your router.

Configuring a Remote Access VPN

To create a Remote Access VPN with one user

1. On the ZoneAlarm router, enable the SecuRemote Remote Access VPN Server.

   See ***Configuring the SecuRemote Remote Access VPN Server*** on page 294.

2. Set up remote VPN access for users.

   See ***Setting Up Remote VPN Access for Users*** on page 318.

3. On the remote user's computer, do *one* of the following:

   - Install SecureClient/SecuRemote VPN Client software (provided for free with your ZoneAlarm)

     For information on installing SecureClient/SecuRemote software, see ***Installing SecuRemote*** on page 296.

   - Install a Check Point security appliance with a built-in SecuRemote VPN Client (for example, Check Point Safe@Office) at the user's premises.

4. On the remote user's VPN Client, add the ZoneAlarm Remote Access VPN Server as a Remote Access VPN site.

   For information on configuring SecureClient/SecuRemote software, see the User Help. To access SecureClient/SecuRemote User Help, right-click on the VPN Client icon in the taskbar, select Settings, and then click Help.

   For information on configuring a Check Point security appliance with a built-in SecuRemote VPN Client, refer to the appliance's user guide.

Configuring the SecuRemote Remote Access VPN Server

To configure the SecuRemote Remote Access VPN Server

1. Click VPN in the main menu, and click the VPN Server tab.

   The VPN Server page appears.

2. Select the Allow SecuRemote users to connect from the Internet check box.

New check boxes appear.

3. To allow authenticated users connecting from the Internet to bypass NAT when connecting to your internal network, select the Bypass NAT check box.
4. To allow authenticated users connecting from the Internet to bypass the default firewall policy and access your internal network without restriction, select the Bypass default firewall policy check box.

   User-defined rules will still apply to the authenticated users.
5. Click Apply.

   The SecuRemote Remote Access VPN Server is enabled for the specified connection types.

Installing SecuRemote

If you configured the ZoneAlarm SecuRemote VPN Server, then authorized remote access users can connect to your network using SecureClient/SecuRemote VPN Client software.

Users can download the necessary software from http://www.checkpoint.com. Alternatively, authorized ZoneAlarm users can use the following procedure to download and install SecureClient/SecuRemote software.

To install SecureClient/SecuRemote

1. Connect to the ZoneAlarm Portal using HTTPS.

   See ***Accessing the ZoneAlarm Portal Remotely Using HTTPS*** on page 47.

2. Click VPN in the main menu, and click the VPN Server tab.

   The VPN Server page appears.

3. Click the Download link.

   The VPN-1 SecuRemote for ZoneAlarm page opens in a new window.

4. Follow the online instructions to complete installation.

   SecureClient/SecuRemote is installed.

   For information on using SecureClient/SecuRemote, see the User Help. To access SecureClient/SecuRemote User Help, right-click on the VPN Client icon in the taskbar, select Settings, and then click Help.

Installing a Certificate

A digital certificate is a secure means of authenticating the ZoneAlarm router to Remote Access VPN Clients. The certificate is issued by the Certificate Authority (CA) to entities such as gateways, users, or computers. The entity then uses the certificate to identify itself and provide verifiable information.

For instance, the certificate includes the Distinguished Name (DN) (identifying information) of the entity, as well as the public key (information about itself). After two entities exchange and validate each other's certificates, they can begin encrypting information between themselves using the public keys in the certificates.

The certificate also includes a fingerprint, a unique text used to identify the certificate. You can email your certificate's fingerprint to the remote user. Upon connecting to the ZoneAlarm VPN Server for the first time, the entity should check that the VPN peer's fingerprint displayed in the SecureClient/SecuRemote VPN Client is identical to the fingerprint received.

A certificate is required for the correct functioning of the ZoneAlarm VPN Server. When the gateway is started for the first time, a self-signed certificate is automatically generated for your gateway; therefore, you usually do not need to install a certificate and can skip this section.

In the event that you need to install a certificate, you must use a certificate encoded in the PKCS#12 (Personal Information Exchange Syntax Standard) format. Your ZoneAlarm router enables you to install such certificates in the following ways:

- By generating a self-signed certificate.

  See ***Generating a Self-Signed Certificate*** on page 298.

- By importing a certificate.

  The PKCS#12 file you import must have a ".p12" file extension. If you do not have such a PKCS#12 file, obtain one from your network security administrator.

  See ***Importing a Certificate*** on page 302.

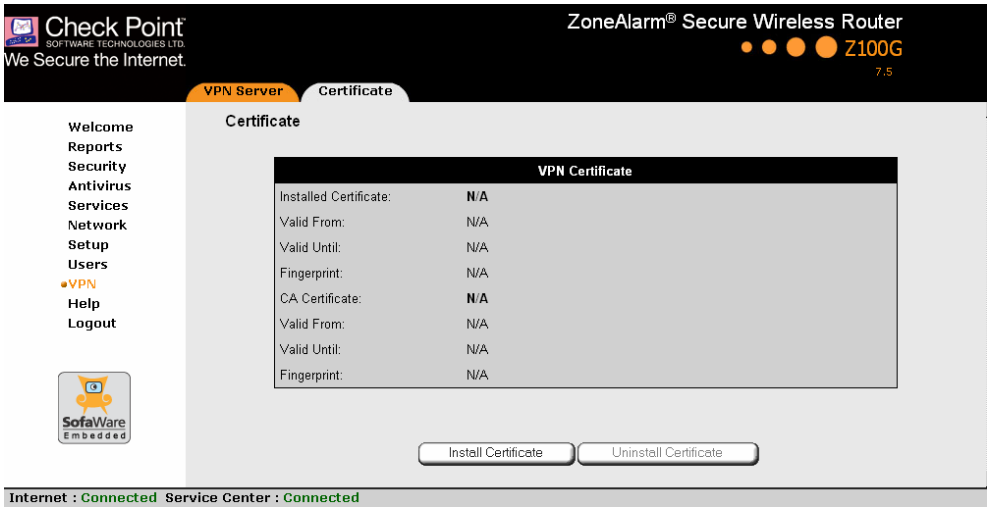
Note: To use certificates authentication, each ZoneAlarm router should have a unique certificate. Do not use the same certificate for more than one gateway.

Generating a Self-Signed Certificate

To generate a self-signed certificate

1. Click VPN in the main menu, and click the Certificate tab.

   The Certificate page appears.



2. Click Install Certificate.

The ZoneAlarm Certificate Wizard opens, with the Certificate Wizard dialog box displayed.

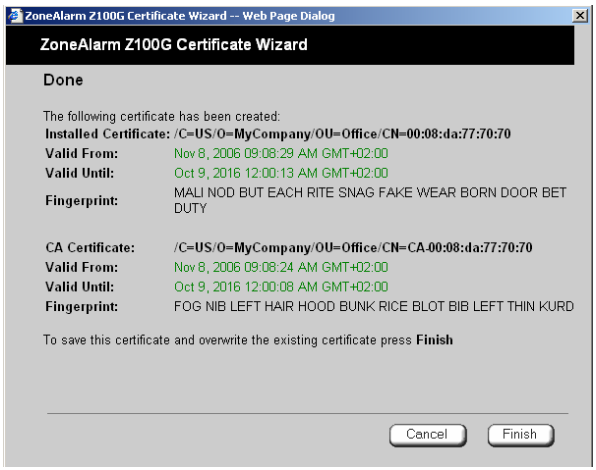
3. Click Generate a self-signed security certificate for this gateway.

   The Create Self-Signed Certificate dialog box appears.

4. Complete the fields using the information in the following table.
5. Click Next.

   The ZoneAlarm router generates the certificate. This may take a few seconds.

The Done dialog box appears, displaying the certificate's details.



6. Click Finish.

   The ZoneAlarm router installs the certificate. If a certificate is already installed, it is overwritten.

   The Certificate Wizard closes.

   The Certificates page displays the following information:

   - The gateway's certificate
   - The gateway's name
   - The gateway certificate's fingerprint
   - The CA's certificate
   - The name of the CA that issued the certificate (in this case, the ZoneAlarm gateway)
   - The CA certificate's fingerprint

- The starting and ending dates between which the gateway's certificate and the CA's certificate are valid

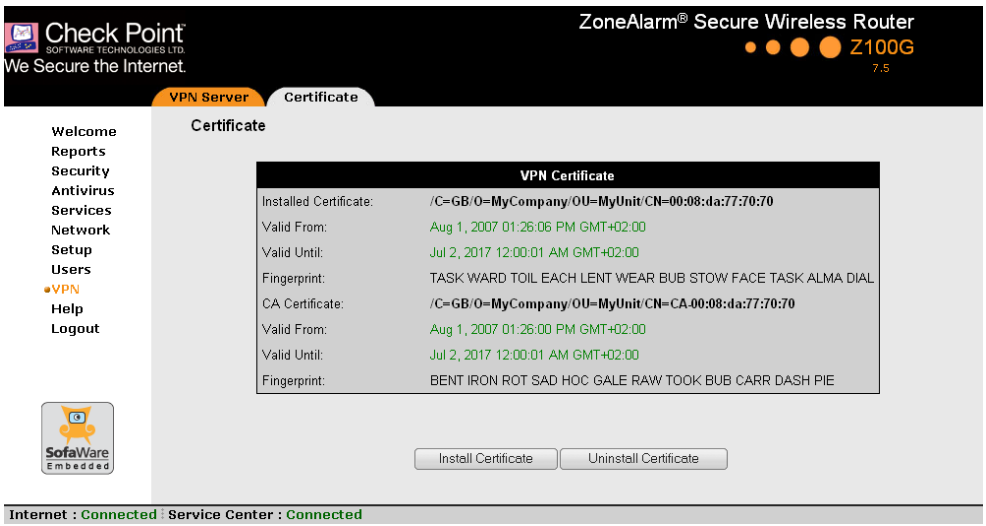


Table 72: Certificate Fields

In this field…	Do this…
Country	Select your country from the drop-down list.
Organization Name	Type the name of your organization.
Organizational Unit	Type the name of your division.
Gateway Name	Type the gateway's name. This name will appear on the certificate, and will be visible to remote users inspecting the certificate. This field is filled in automatically with the gateway's MAC address. If desired, you can change this to a more descriptive name.

In this field…	Do this…
Valid Until	Use the drop-down lists to specify the month, day, and year when this certificate should expire. Note: You must renew the certificate when it expires.

Importing a Certificate

To install a certificate

1. Click VPN in the main menu, and click the Certificate tab.

   The Certificate page appears.

2. Click Install Certificate.

   The ZoneAlarm Certificate Wizard opens, with the Certificate Wizard dialog box displayed.

3. Click Import a security certificate in PKCS#12 format.

   The Import Certificate dialog box appears.

4. Click Browse to open a file browser from which to locate and select the file.

   The filename that you selected is displayed.

5. Click Next.

   The Import-Certificate Passphrase dialog box appears. This may take a few moments.

6. Type the pass-phrase you received from the network security administrator.
7. Click Next.

   The Done dialog box appears, displaying the certificate's details.

8. Click Finish.

   The ZoneAlarm router installs the certificate. If a certificate is already installed, it is overwritten.

   The Certificate Wizard closes.

   The Certificates page displays the following information:

   - The gateway's certificate
   - The gateway's name
   - The gateway certificate's fingerprint
   - The CA's certificate
   - The name of the CA that issued the certificate
   - The CA certificate's fingerprint

- The starting and ending dates between which the gateway's certificate and the CA's certificate are valid

Uninstalling a Certificate

A certificate is required for the correct functioning of the VPN Server. If you uninstall the certificate, VPN Clients configured for certificate authentication will not be able to connect to the VPN Server.

Note: If you want to replace a currently-installed certificate, there is no need to uninstall the certificate first. When you install the new certificate, the old certificate will be overwritten.

To uninstall a certificate

1. Click VPN in the main menu, and click the Certificate tab.

   The Certificate page appears with the name of the currently installed certificate.

2. Click Uninstall.

   A confirmation message appears.

3. Click OK.

   The certificate is uninstalled.

   A success message appears.

4. Click OK.

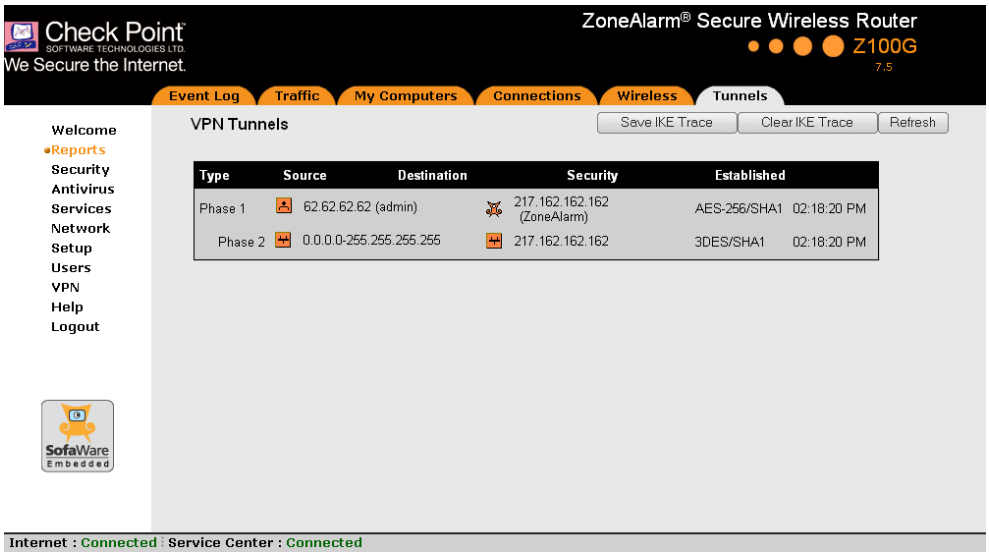
Viewing VPN Tunnels

You can view a list of currently established VPN tunnels.

To view VPN tunnels

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

   The VPN Tunnels page appears with a table of open VPN tunnels.



   The VPN Tunnels page includes the information described in the following table.

2. To refresh the table, click Refresh.

Table 73: VPN Tunnels Page Fields

This field...	Displays...
Type	The currently active security protocol (IPSEC).
Source	The IP address or address range of the entity from which the tunnel originates. The entity's type is indicated by an icon. See ***VPN Tunnel Icons*** on page 307.
Destination	The IP address or address range of the entity to which the tunnel is connected. The entity's type is indicated by an icon. See ***VPN Tunnel Icons*** on page 307.
Security	The type of encryption used to secure the connection, and the type of Message Authentication Code (MAC) used to verify the integrity of the message. This information is presented in the following format: Encryption type/Authentication type. In addition, if IPSec compression is enabled for the tunnel, this field displays the  icon. Note: All VPN settings are automatically negotiated between the two sites. The encryption and authentication schemes used for the connection are the strongest of those used at the two sites. Your ZoneAlarm router supports AES, 3DES, and DES encryption schemes, and MD5 and SHA authentication schemes.

This field…	Displays…
Established	The time at which the tunnel was established. This information is presented in the format hh:mm:ss, where: hh=hours mm=minutes ss=seconds

Table 74: VPN Tunnels Icons

This icon…	Represents…
	This gateway
	A network for which an IKE Phase-2 tunnel was negotiated
	A remote access VPN user

Viewing IKE Traces for VPN Connections

If you are experiencing VPN connection problems, you can save a trace of IKE (Internet Key Exchange) negotiations to a file, and then use the free IKE View tool to view the file.

The IKE View tool is available for the Windows platform.

Note: Before viewing IKE traces, it is recommended to do the following:

- The ZoneAlarm router stores traces for all recent IKE negotiations. If you want to view only new IKE trace data, clear all IKE trace data currently stored on the ZoneAlarm router.
- Close all existing VPN tunnels except for the problematic tunnel, so as to make it easier to locate the problematic tunnel's IKE negotiation trace in the exported file.

To clear all currently-stored IKE traces

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

   The VPN Tunnels page appears with a table of open tunnels to VPN sites.

2. Click Clear IKE Trace.

   All IKE trace data currently stored on the ZoneAlarm router is cleared.

To view the IKE trace for a connection

1. Ask the administrator of the VPN site with which you are experiencing connection problems to establish a VPN tunnel to the ZoneAlarm VPN Server.

   For information on when and how VPN tunnels are established, see ***Viewing VPN Tunnels*** on page 305.

2. Click Reports in the main menu, and click the Tunnels tab.

   The VPN Tunnels page appears with a table of open VPN tunnels.

3. Click Save IKE Trace.

   A standard File Download dialog box appears.

4. Click Save.

   The Save As dialog box appears.

5. Browse to a destination directory of your choice.
6. Type a name for the *.elg file and click Save.

   The *.elg file is created and saved to the specified directory. This file contains the IKE traces of all currently-established VPN tunnels.
7. Use the IKE View tool to open and view the *.elg file, or send the file to technical support.

Chapter 15

Managing Users

This chapter describes how to manage ZoneAlarm router users. You can define multiple users, set their passwords, and assign them various permissions.

This chapter includes the following topics:

Changing Your Login Credentials

You can change your username and password at any time.

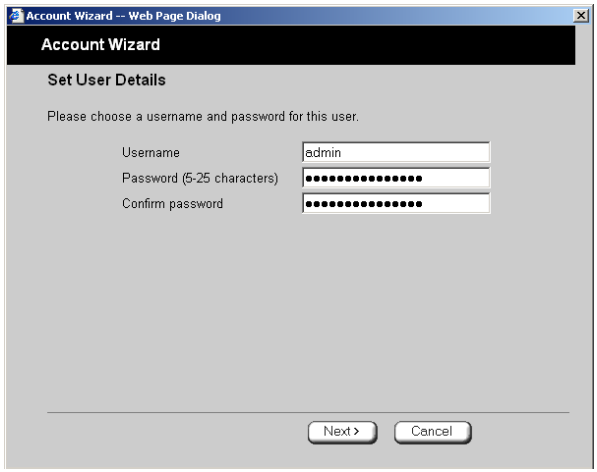
To change your login credentials

1. Click Users in the main menu, and click the Internal Users tab.

The Internal Users page appears.

2. In the row of your username, click Edit.

   The Account Wizard opens displaying the Set User Details dialog box.



3. Edit the Username field.
4. Edit the Password and Confirm password fields.

Note: Use 5 to 25 characters (letters or numbers) for the new password.

5. Click Next.

   The Set User Permissions dialog box appears.

6. Click Finish.

   Your changes are saved.

Adding and Editing Users

This procedure explains how to add and edit users.

To add or edit a user

1. Click Users in the main menu, and click the Internal Users tab.

   The Internal Users page appears.

2. Do one of the following:

   - To create a new user, click New User.

- To edit an existing user, click Edit next to the desired user.

The Account Wizard opens displaying the Set User Details dialog box.

3. Complete the fields using the information in ***Set User Details Fields*** on page 315.
4. Click Next.

   The Set User Permissions dialog box appears.

The options that appear on the page are dependant on the software and services you are using.

5. Complete the fields using the information in ***Set User Permissions Fields*** on page 316.
6. Click Finish.

   The user is saved.

Table 75: Set User Details Fields

In this field…	Do this…
Username	Enter a username for the user.
Password	Enter a password for the user. Use five to 25 characters (letters or numbers) for the new password.
Confirm Password	Re-enter the user's password.
Expires On	To specify an expiration time for the user, select this option and specify the expiration date and time in the fields provided. When the user account expires, it is locked, and the user can no longer log on to the ZoneAlarm router. If you do not select this option, the user will not expire.

Table 76: Set User Permissions Fields

In this field...	Do this...
Administrator Level	Select the user's level of access to the ZoneAlarm Portal. The levels are: • No Access: The user cannot access the ZoneAlarm Portal. • Read Only: The user can log on to the ZoneAlarm Portal, but cannot modify system settings or export the router configuration via the Setup>Tools page. For example, you could assign this administrator level to technical support personnel who need to view the Event Log. • Users Manager. The user can log on to the ZoneAlarm Portal and add, edit, or delete "No Access"-level users. However, the user cannot modify other system settings. For example, you could assign this administrator level to company clerk who needs to manage network users. • Read/Write: The user can log on to the ZoneAlarm Portal and modify system settings. The default level is No Access. The "admin" user's Administrator Level (Read/Write) cannot be changed.
VPN Remote Access	Select this option to allow the user to connect to this ZoneAlarm router using their VPN Client. For further information on setting up VPN remote access, see ***Setting Up Remote VPN Access for Users*** on page 318.
Web Filtering Override	Select this option to allow the user to override the Web Filtering service and Web rules. This option cannot be changed for the "admin" user.

Remote Desktop Access	Select this option to allow the user to log on to the my.firewall portal, view the Active Computers page, and remotely access computers' desktops, using the Remote Desktop feature. Note: The user can perform these actions, even if their level of administrative access is "No Access". For information on Remote Desktop, see ***Using Remote Desktop*** on page 319.

Viewing and Deleting Users

Note: The “admin” user cannot be deleted.

To view or delete users

1. Click Users in the main menu, and click the Internal Users tab.

   The Internal Users page appears with a list of all users and their permissions.

   The expiration time of expired users appears in red.
2. To delete a user, do the following:

   a) In the desired user’s row, click the Erase  icon.

   A confirmation message appears.

   b) Click OK.

   The user is deleted.
3. To delete all expired users, do the following:

   a) Click Clear Expired.

   A confirmation message appears.

   b) Click OK.

   The expired users are deleted.

Setting Up Remote VPN Access for Users

If you are using your ZoneAlarm router as a SecuRemote Remote Access VPN Server, you can allow users to access it remotely through their Remote Access VPN Clients (a Check Point SecureClient, Check Point SecuRemote, or a Check Point appliance with a built-in SecuRemote VPN Client).

Note: ZoneAlarm Z100G allows defining a single VPN user.

To set up remote VPN access for a user

1. Enable your VPN Server, using the procedure ***Configuring the SecuRemote Remote Access VPN Server*** on page 294.
2. Add or edit the user, using the procedure ***Adding and Editing Users*** on page 313.

   You must select the VPN Remote Access option.

Chapter 16

Using Remote Desktop

This chapter describes how to remotely access the desktop of each of your computers, using the ZoneAlarm router's Remote Desktop feature.

This chapter includes the following topics:

Overview

Your ZoneAlarm router includes an integrated client for Microsoft Terminal Services, allowing you to remotely access the desktop of each of your computers from anywhere, via the ZoneAlarm Portal. You can even redirect your printers or ports to a remote computer, so that you can print and transfer files with ease.

Remote Desktop sessions use the Microsoft Remote Desktop Protocol (RDP) on TCP port 3389. This port is opened dynamically between the Remote Desktop client and the Remote Desktop server as needed, meaning that the port is not exposed to the Internet, and your constant security is ensured.

Note: By default, the Microsoft RDP protocol is secured with 128-bit RC4 encryption. For the strongest possible security, it is recommended to use Remote Desktop over an IPSec VPN connection. For information on VPNs, see ***Working With VPNs*** on page 291.

Workflow

To use Remote Desktop

1. Configure Remote Desktop.

   See ***Configuring Remote Desktop*** on page 321.

2. Enable the Remote Desktop server on computers that authorized users should be allowed to remotely access.

   See ***Configuring the Host Computer*** on page 324.

3. Grant Remote Desktop Access permissions to users who should be allowed to remotely access desktops.

   See ***Adding and Editing Users*** on page 313.

4. The authorized users can access remote computers' desktops as desired.

   See ***Accessing a Remote Computer's Desktop*** on page 327.

Configuring Remote Desktop

To configure Remote Desktop

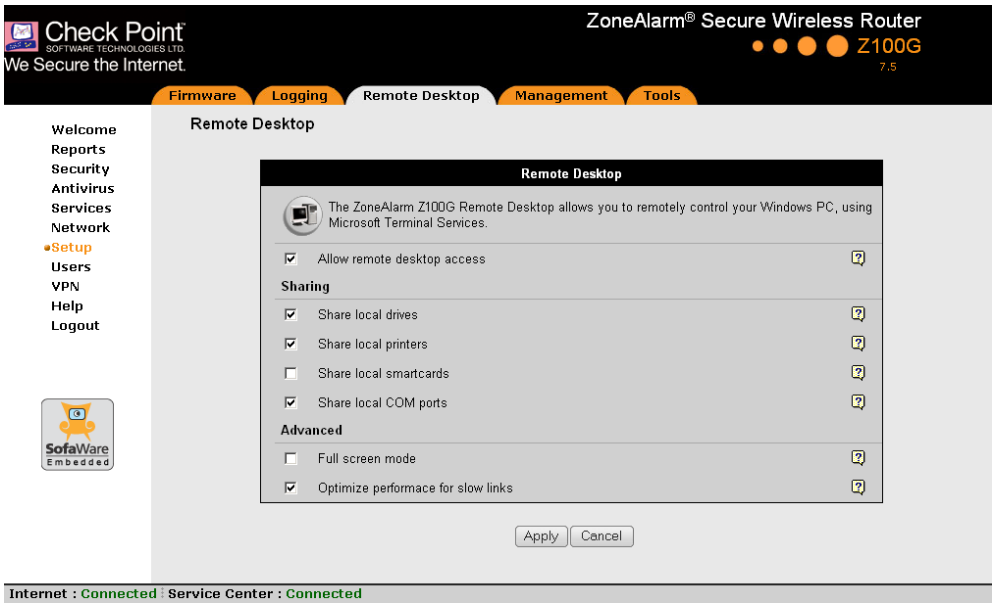
1. Click Setup in the main menu, and click the Remote Desktop tab.

   The Remote Desktop page appears.

2. Do one of the following:

   - To enable Remote Desktop, select the Allow remote desktop access check box.

New fields appear.



- To disable Remote Desktop, clear the Allow remote desktop access check box.

  Fields disappear.

3. Complete the fields using the information in the following table.
4. Click Apply.

Table 77: Remote Desktop Options

In this field...	Do this...
Sharing	
Share local drives	Select this option to allow the host computer to access hard drives on the client computer. This enables remote users to access their local hard drives when logged on to the host computer.

In this field…	Do this…
Share local printers	Select this option to allow the host computer to access printers on the client computer. This enables remote users to access their local printer when logged on to the host computer.
Share local smartcards	Select this option to allow the host computer to access smartcards on the client computer. This enables remote users to access their local smartcards when logged on to the host computer.
Share local COM ports	Select this option to allow the host computer to access COM ports on the client computer. This enables remote users to access their local COM ports when logged on to the host computer.
Advanced	
Full screen mode	Select this option to open Remote Desktop sessions on the whole screen.
Optimize performance for slow links	Select this option to optimize Remote Desktop sessions for slow links. Bandwidth-consuming options, such as wallpaper and menu animations, will be disabled.

Configuring the Host Computer

To enable remote users to connect to a computer, you must enable the Remote Desktop server on that computer.

Note: The host computer must have one of the following operating systems installed:

- Microsoft Windows Server 2003
- Microsoft Windows XP Professional
- Microsoft Windows XP Media Center
- Microsoft Windows XP Tablet PC 2005

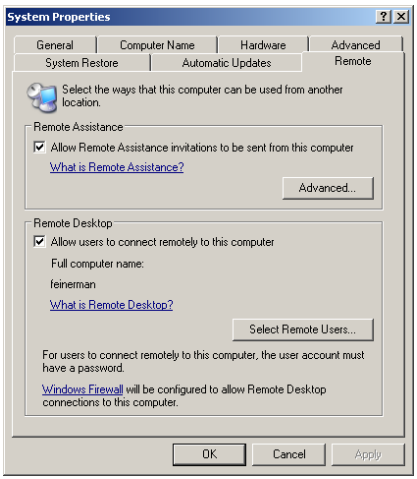
To enable users to remotely connect to a computer

1. Log on to the desired computer as an administrator.
2. For each remote user who should be allowed to access this computer, create a user account with a password.

   For information, refer to Microsoft documentation.
3. On the desktop, right-click on My Computer, and select Properties in the pop-up menu that appears.

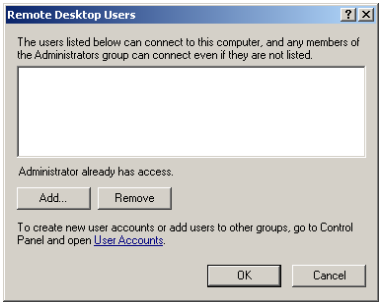
   The System Properties dialog box appears displaying the General tab.
4. Click the Remote tab.

The Remote tab appears.



5. Select the Allow users to connect remotely to this computer check box.
6. Click Select Remote Users.

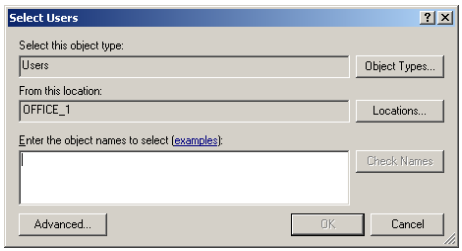
   The Remote Desktop Users dialog box appears.



7. Do the following for each remote user who should be allowed to access this computer:

   a. Click Add.

The Select Users dialog box appears.



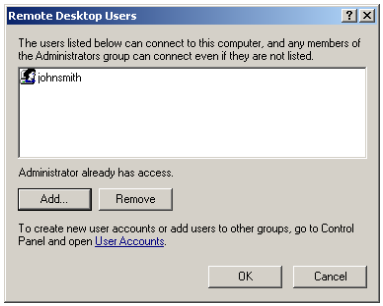
b. Type the desired user's username in the text box.

   The Check Names button is enabled.

c. Click Check Names.

d. Click OK.

   The Remote Desktop Users dialog box reappears with the desired user's username.



8. Click OK.
9. Click OK.

Accessing a Remote Computer's Desktop

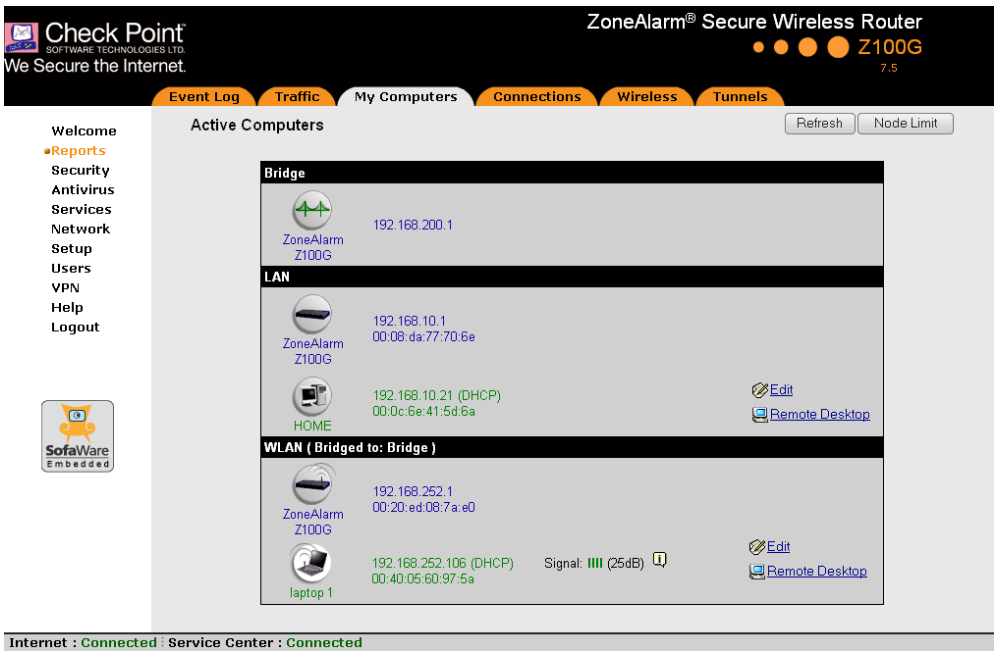
Note: The client computer must meet the following requirements:

- Microsoft Internet Explorer 6.0 or later
- A working Internet connection

To access a remote computer's desktop

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

   The My Computers page appears.

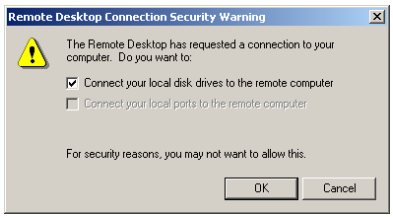


2. Next to the desired computer, click Remote Desktop.

   The following things happen:

   - If you are prompted to install the Remote Desktop Active X Control, then install it.

- The Remote Desktop Connection Security Warning dialog box appears.

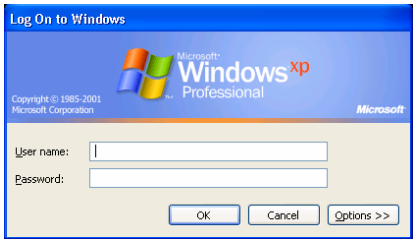


3. Select the desired connection options.

   The available options depend on your Remote Desktop configuration. See ***Configuring Remote Desktop*** on page 321.

4. Click OK.

   The Log On to Windows dialog box appears.



5. Type your username and password for the remote computer.

   These are the credentials configured for your user account in ***Enabling the Remote Desktop Server*** on page 324.

6. Click OK.

   The remote computer's desktop appears onscreen.

   You can use the following keyboard shortcuts during the Remote Desktop session:

Table 78: Remote Desktop Keyboard Shortcuts

This shortcut…	Does this…
ALT+INSERT	Cycles through running programs in the order that they were started
ALT+HOME	Displays the Start menu
CTRL+ALT+BREAK	Toggles between displaying the session in a window and on the full screen
CTRL+ALT+END	Opens the Windows Security dialog box

Chapter 17

Maintenance

This chapter describes the tasks required for maintenance and diagnosis of your ZoneAlarm router.

This chapter includes the following topics:

Viewing Firmware Status

The firmware is the software program embedded in the ZoneAlarm router.

You can view your current firmware version and additional details.

To view the firmware status

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

  The Firmware page appears.

The Firmware page displays the following information:

Table 79: Firmware Status Fields

This field…	Displays…	For example…
WAN MAC Address	The MAC address used for the Internet connection	00:80:11:22:33:44
Firmware Version	The current version of the firmware	7.5

This field…	Displays…	For example…
Installed Product	The licensed software and the number of allowed nodes	ZoneAlarm Z100G (5 nodes)
Uptime	The time that elapsed from the moment the unit was turned on	01:21:15
Hardware Type	The type of the current ZoneAlarm router hardware	SBox-200
Hardware Version	The current hardware version of the ZoneAlarm router	1.0

Updating the Firmware

If you are subscribed to Software Updates, firmware updates are performed automatically. These updates include new product features and protection against new security threats. Check with your reseller for the availability of Software Updates and other services. For information on subscribing to services, see ***Connecting to a Service Center*** on page 267.

If you are not subscribed to the Software Updates service, you must update your firmware manually.

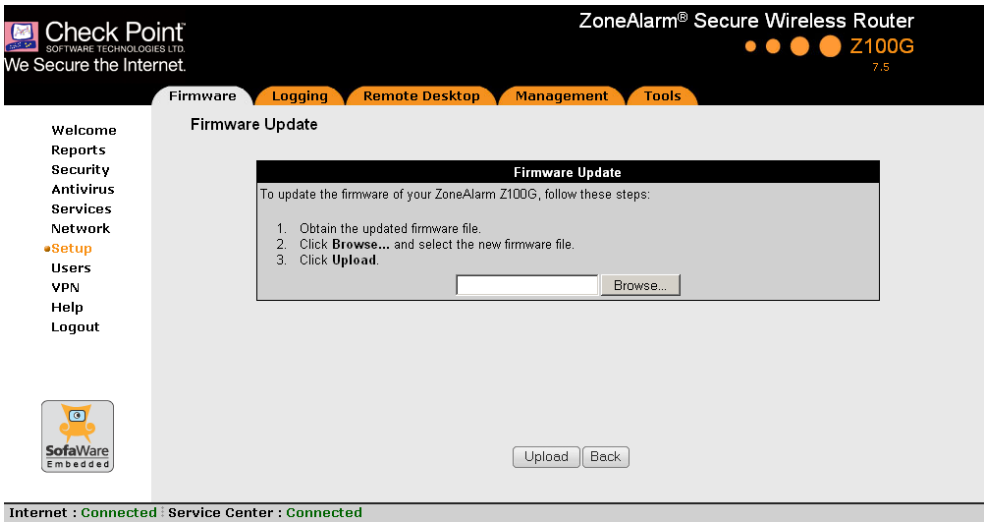
To update your ZoneAlarm firmware manually

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

   The Firmware page appears.

2. Click Firmware Update.

The Firmware Update page appears.



3. Click Browse.

   A browse window appears.

4. Select the image file and click Open.

   The Firmware Update page reappears. The path to the firmware update image file appears in the Browse text box.

5. Click Upload.

   Your ZoneAlarm router firmware is updated.

   Updating may take a few minutes. Do not power off the router.

   At the end of the process the ZoneAlarm router restarts automatically.

Upgrading Your License

If product upgrades are available, you can upgrade the ZoneAlarm product installed on your router, by purchasing a new license. You will receive a new Product Key that enables you to use advanced features on the same ZoneAlarm router you have today. There is no need to replace your hardware. You can also purchase node upgrades, if available.

Note: To determine whether product or node upgrades are available, contact your ZoneAlarm router provider. Alternatively, you can click Upgrades & Services in the Welcome page to view and purchase available upgrades.

To upgrade your product, you must install the new Product Key.

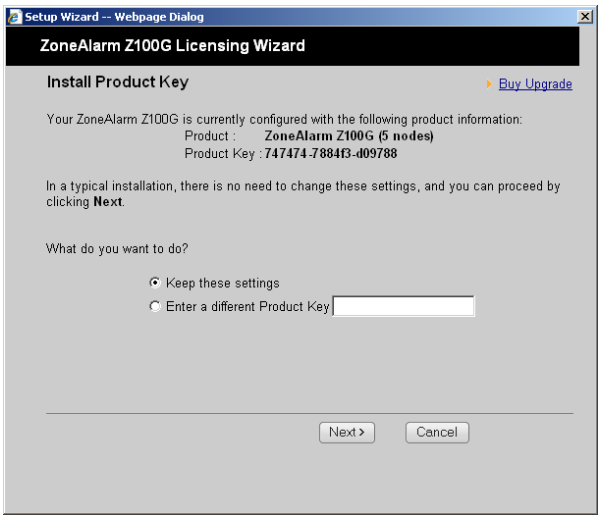
To install a Product Key

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

   The Firmware page appears.

2. Click Upgrade Product.

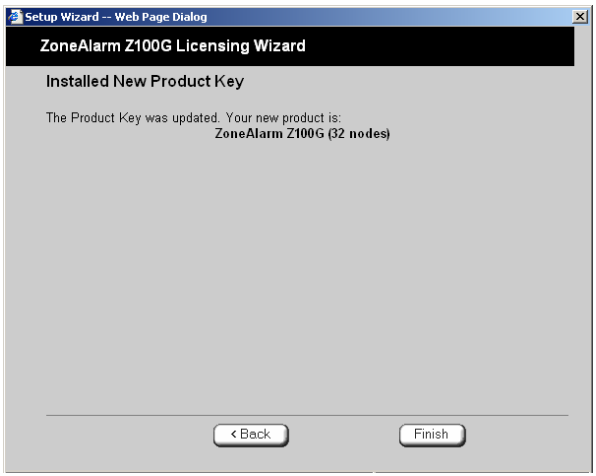
   The ZoneAlarm Licensing Wizard opens, with the Install Product Key dialog box displayed.



3. Click Enter a different Product Key.

4. In the Product Key field, enter the new Product Key.
5. Click Next.

   The Installed New Product Key dialog box appears.



6. Click Finish.

Configuring Syslog Logging

You can configure the ZoneAlarm router to send event logs to a Syslog server residing in your internal network or on the Internet. The logs detail the date and the time each event occurred. If the event is a communication attempt that was rejected by the firewall, the event details include the source and destination IP address, the destination port, and the protocol used for the communication attempt (for example, TCP or UDP).

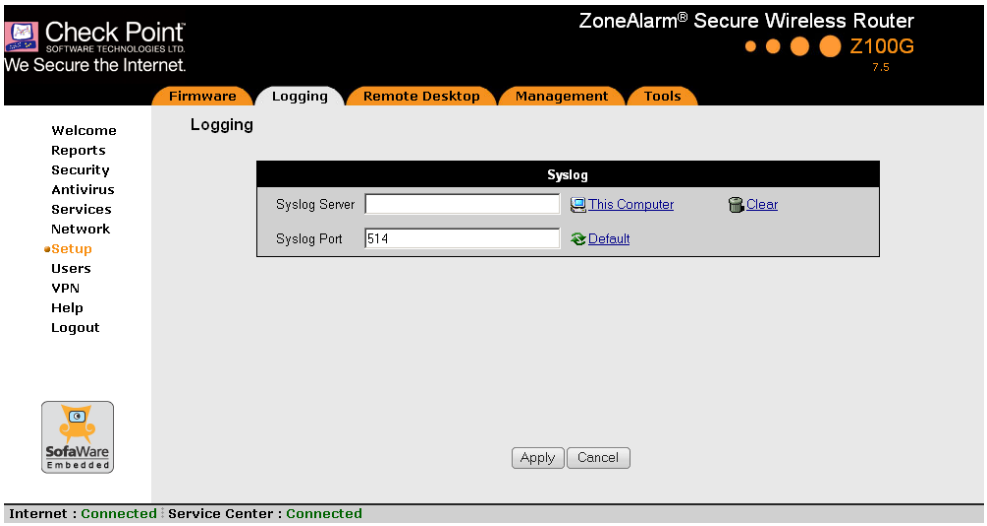
This same information is also available in the Event Log page (see ***Viewing the Event Log*** on page 151). However, while the Event Log can display hundreds of logs, a Syslog server can store an unlimited number of logs. Furthermore, Syslog servers can provide useful tools for managing your logs.

Note: Kiwi Syslog Daemon is freeware and can be downloaded from http://www.kiwisyslog.com. For technical support, contact Kiwi Enterprises.

To configure Syslog logging

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

   The Logging page appears.



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

Table 80: Logging Page Fields

In this field…	Do this…
Syslog Server	Type the IP address of the computer that will run the Syslog service (one of your network computers), or click This Computer to allow your computer to host the service.
Clear	Click to clear the Syslog Server field.
Syslog Port	Type the port number of the Syslog server.
Default	Click to reset the Syslog Port field to the default (port 514 UDP).

Configuring HTTPS

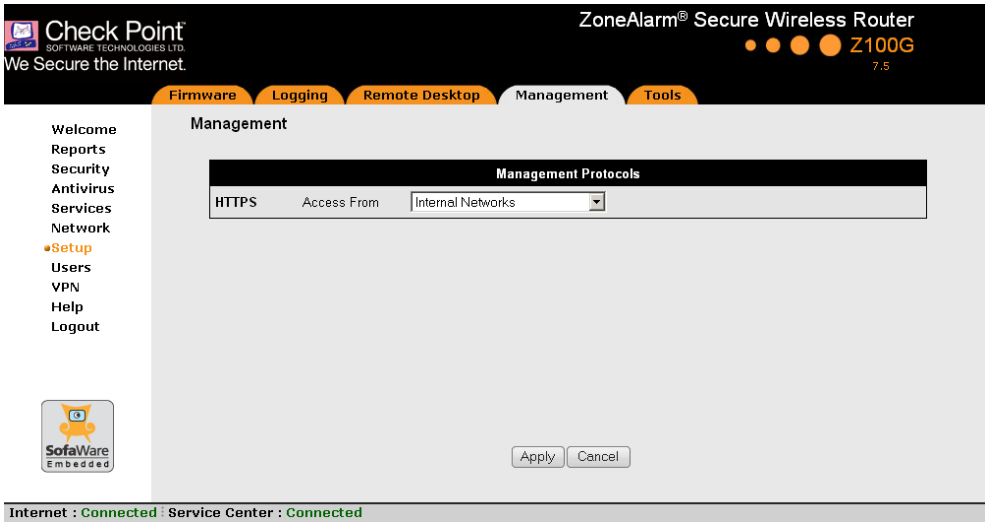
You can enable ZoneAlarm router users to access the ZoneAlarm Portal from the Internet. To do so, you must first configure HTTPS.

Note: Configuring HTTPS is equivalent to creating a simple Allow rule, where the destination is This Gateway. To create more complex rules for HTTPS, such as allowing HTTPS connections from multiple IP address ranges, define Allow rules for TCP port 443, with the destination This Gateway. For information, see ***Using Rules*** on page 172.

To configure HTTPS

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

   The Management page appears.



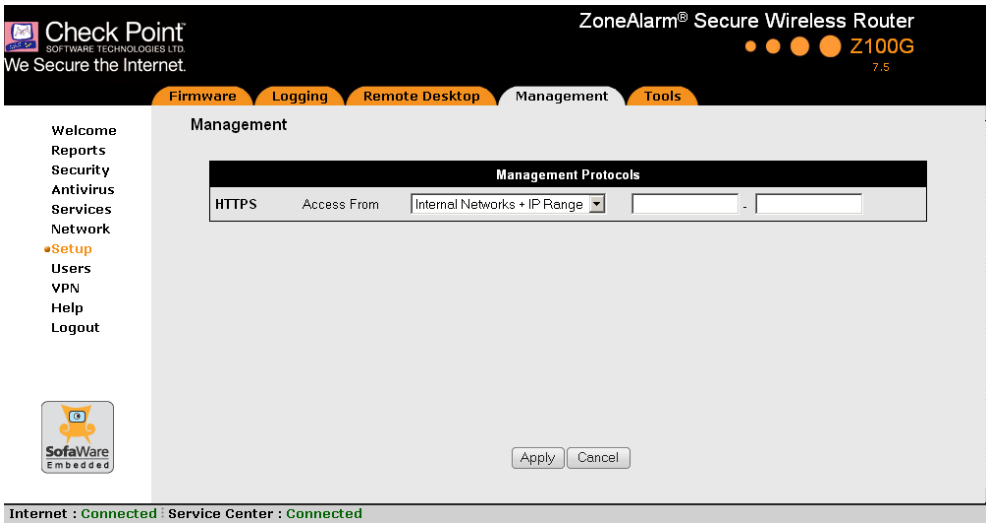
2. Specify from where HTTPS access to the ZoneAlarm Portal should be granted.

   See ***Access Options*** on page 340 for information.

Warning: If remote HTTPS is enabled, your ZoneAlarm router settings can be changed remotely, so it is especially important to make sure all ZoneAlarm router users' passwords are difficult to guess.

Note: You can use HTTPS to access the ZoneAlarm Portal from your internal network, by surfing to https://my.firewall.

If you selected Internal Networks + IP Range, additional fields appear.



3. If you selected Internal Networks + IP Range, enter the desired IP address range in the fields provided.
4. Click Apply.

   The HTTPS configuration is saved. If you configured remote HTTPS, you can now access the ZoneAlarm Portal through the Internet, using the procedure ***Accessing the ZoneAlarm Portal Remotely*** on page 47.

Table 81: Access Options

Select this option…	To allow access from…
Internal Networks	The internal network only. This disables remote access capability. This is the default.
Internal Networks + VPN	The internal network and your VPN.
Internal Networks + IP Range	A particular range of IP addresses. Additional fields appear, in which you can enter the desired IP address range.
ANY	Any IP address.
Disabled	Nowhere. Access via this protocol is disabled. This option is relevant to the SNMP protocol only.

Setting the Time on the Router

You set the time displayed in the ZoneAlarm Portal during initial router setup. If desired, you can change the date and time using the procedure below.

To set the time

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

   The Tools page appears.

2. Click Set Time.

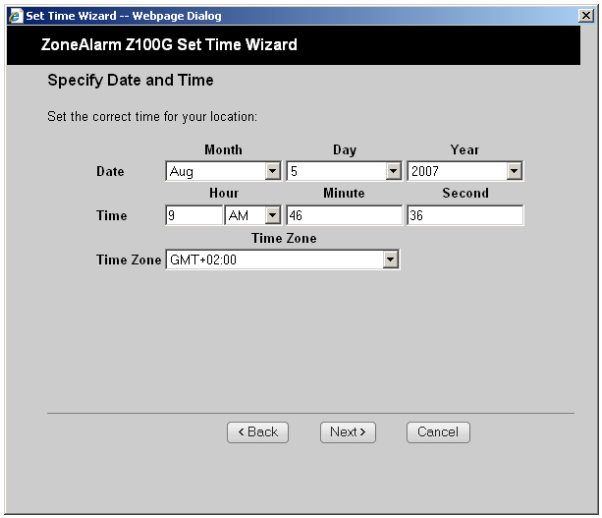
   The ZoneAlarm Set Time Wizard opens displaying the Set the ZoneAlarm Time dialog box.

3. Complete the fields using the information in ***Set Time Wizard Fields*** on page 343.

4. Click Next.

The following things happen in the order below:

- If you selected Specify date and time, the Specify Date and Time dialog box appears.

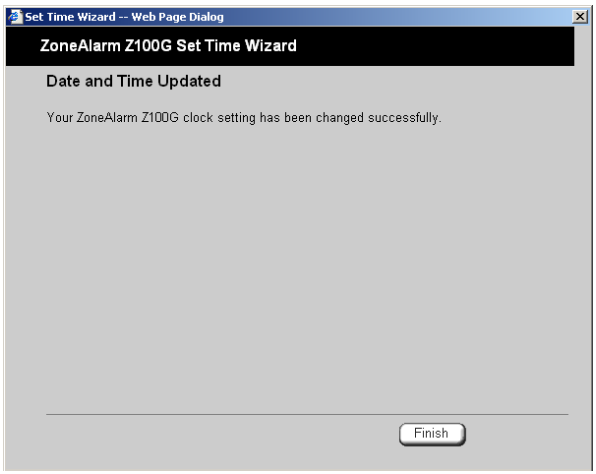


Set the date, time, and time zone in the fields provided, then click Next.

- If you selected Use a Time Server, the Time Servers dialog box appears.

Complete the fields using the information in ***Time Servers Fields*** on page 344, then click Next.

- The Date and Time Updated screen appears.



5. Click Finish.

Table 82: Set Time Wizard Fields

Select this option…	To do the following…
Your computer's clock	Set the router time to your computer's system time. Your computer's system time is displayed to the right of this option.
Keep the current setting	Do not change the router's time. The current router time is displayed to the right of this option.
Use a Time Server	Synchronize the router time with a Network Time Protocol (NTP) server.
Specify date and time	Set the router to a specific date and time.

Table 83: Time Servers Fields

In this field…	Do this…
Primary Server	Type the IP address of the Primary NTP server.
Secondary Server	Type the IP address of the Secondary NTP server. This field is optional.
Clear	Clear the field.
Select your time zone	Select the time zone in which you are located.

Using Diagnostic Tools

The ZoneAlarm router is equipped with a set of diagnostic tools that are useful for troubleshooting Internet connectivity.

Table 84: Diagnostic Tools

Use this tool…	To do this…	For information, see...
Ping	Check that a specific IP address or DNS name can be reached via the Internet.	***Using IP Tools*** on page 345
Traceroute	Display a list of all routers used to connect from the ZoneAlarm router to a specific IP address or DNS name.	***Using IP Tools*** on page 345
WHOIS	Display the name and contact information of the entity to which a specific IP address or DNS name is registered. This information is useful in tracking down hackers.	***Using IP Tools*** on page 345

Use this tool...	To do this...	For information, see...
Packet Sniffer	Capture network traffic. This information is useful troubleshooting network problems.	***Using Packet Sniffer*** on page 347

Using IP Tools

To use an IP tool

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

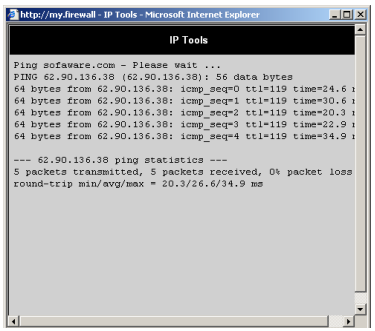
   The Tools page appears.

2. In the Tool drop-down list, select the desired tool.
3. In the Address field, type the IP address or DNS name for which to run the tool.
4. Click Go.

   - If you selected Ping, the following things happen:

     The ZoneAlarm router sends packets to the specified the IP address or DNS name.

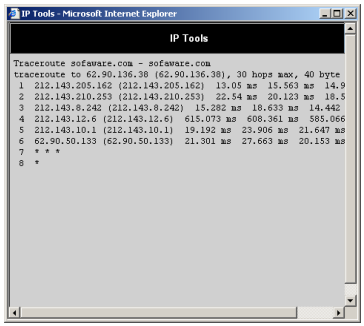
     The IP Tools window opens and displays the percentage of packet loss and the amount of time it took each packet to reach the specified host and return (round-trip) in milliseconds.



- If you selected Traceroute, the following things happen:

  The ZoneAlarm router connects to the specified IP address or DNS name.

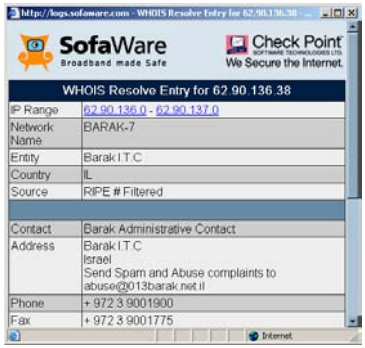
  The IP Tools window opens and displays a list of routers used to make the connection.



- If you selected WHOIS, the following things happen:

  The ZoneAlarm router queries the Internet WHOIS server.

  A window displays the name of the entity to which the IP address or DNS name is registered and their contact information.



Using Packet Sniffer

The ZoneAlarm router includes the Packet Sniffer tool, which enables you to capture packets from any internal network or ZoneAlarm port. This is useful for troubleshooting network problems and for collecting data about network behavior.

The ZoneAlarm router saves the captured packets to a file on your computer. You can use a free protocol analyzer, such as Ethereal or Wireshark, to analyze the file, or you can send it to technical support. Wireshark runs on all popular computing platforms and can be downloaded from http://www.wireshark.com.

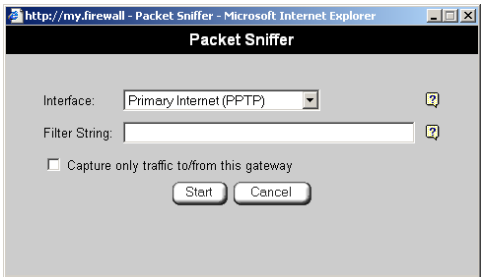
To use Packet Sniffer

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

   The Tools page appears.

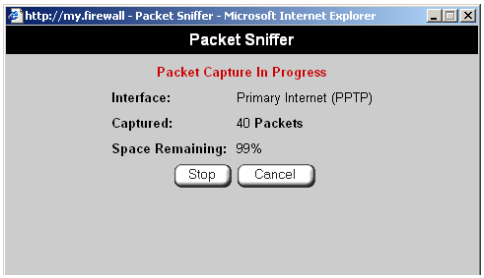
2. Click Sniffer.

   The Packet Sniffer window opens.



3. Complete the fields using the information in the following table.
4. Click Start.

The Packet Sniffer window displays the name of the interface, the number of packets collected, and the percentage of storage space remaining on the router for storing the packets.



5. Click Stop to stop collecting packets.

   A standard File Download dialog box appears.

6. Click Save.

   The Save As dialog box appears.

7. Browse to a destination directory of your choice.

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

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

9. Click Cancel to close the Packet Sniffer window.

Table 85: Packet Sniffer Fields

In this field…	Do this…
Interface	Select the interface from which to collect packets. The list includes the primary Internet connection, the ZoneAlarm router ports, and all defined networks.
Filter String	Type the filter string to use for filtering the captured packets. Only packets that match the filter condition will be saved. For a list of basic filter strings elements, see ***Filter String Syntax*** on page 350. For detailed information on filter syntax, go to http://www.tcpdump.org/tcpdump_man.html. Note: Do not enclose the filter string in quotation marks. If you do not specify a filter string, Packet Sniffer will save all packets on the selected interface.
Capture only traffic to/from this gateway	Select this option to capture incoming and outgoing packets for this gateway only. If this option is not selected, Packet Sniffer will collect packets for all traffic on the interface.

Filter String Syntax

The following represents a list of basic filter string elements:

For detailed information on filter syntax, refer to http://www.tcpdump.org.

and

PURPOSE

The `and` element is used to concatenate filter string elements. The filtered packets must match *all* concatenated filter string elements.

SYNTAX

element `and` element [`and` element...]

element `&&` element [`&&` element...]

PARAMETERS

`element`	String. A filter string element.

EXAMPLE

The following filter string saves packets that both originate from IP address is 192.168.10.1 and are destined for port 80:

```
src 192.168.10.1 and dst port 80
```

dst

PURPOSE

The `dst` element captures all packets with a specific destination.

SYNTAX

dst *destination*

PARAMETERS

`destination`	IP Address or String. The computer to which the packet is sent. This can be the following: • An IP address • A host name

EXAMPLE

The following filter string saves packets that are destined for the IP address 192.168.10.1:

```
dst 192.168.10.1
```

dst port

PURPOSE

The `dst port` element captures all packets destined for a specific port.

SYNTAX

dst port *port*

Note: This element can be prepended by tcp or udp. For information, see ***tcp*** on page 356 and ***udp*** on page 357.

PARAMETERS

`port`	Integer. The port to which the packet is sent.

EXAMPLE

The following filter string saves packets that are destined for port 80:

```
dst port 80
```

ether proto

PURPOSE

The `ether proto` element is used to capture packets of a specific ether protocol type.

SYNTAX

ether proto *protocol*

PARAMETERS

`protocol`	String. The protocol type of the packet. This can be the following: `ip`, `ip6`, `arp`, `rarp`, `atalk`, `aarp`, `dec net`, `sca`, `lat`, `mopdl`, `moprc`, `iso`, `stp`, `ipx`, or `netbeui`.

EXAMPLE

The following filter string saves ARP packets:

```
ether proto arp
```

host

PURPOSE

The `host` element captures all incoming and outgoing packets for a specific computer.

SYNTAX

host *host*

PARAMETERS

`host`	IP Address or String. The computer to/from which the packet is sent. This can be the following: • An IP address • A host name

EXAMPLE

The following filter string saves all packets that either originated from IP address 192.168.10.1, or are destined for that same IP address:

host 192.168.10.1

not

PURPOSE

The `not` element is used to negate filter string elements.

SYNTAX

not element

! element

PARAMETERS

`element`	String. A filter string element.

EXAMPLE

The following filter string saves packets that are *not* destined for port 80:

```
not dst port 80
```

or

PURPOSE

The `or` element is used to alternate between string elements. The filtered packets must match at least one of the filter string elements.

SYNTAX

element or element [or element...]

element || element [|| element...]

PARAMETERS

`element`	String. A filter string element.

EXAMPLE

The following filter string saves packets that either originate from IP address 192.168.10.1 or IP address 192.168.10.10:

```
src 192.168.10.1 or src 192.168.10.10
```

port

PURPOSE

The `port` element captures all packets originating from or destined for a specific port.

SYNTAX

port *port*

Note: This element can be prepended by tcp or udp. For information, see ***tcp*** on page 356 and ***udp*** on page 357.

PARAMETERS

`port`	Integer. The port from/to which the packet is sent.

EXAMPLE

The following filter string saves all packets that either originated from port 80, or are destined for port 80:

```
port 80
```

src

PURPOSE

The `src` element captures all packets with a specific source.

SYNTAX

src *source*

PARAMETERS

`source`	IP Address or String. The computer from which the packet is sent. This can be the following: • An IP address • A host name

EXAMPLE

The following filter string saves packets that originated from IP address 192.168.10.1:

```
src 192.168.10.1
```

src port

PURPOSE

The `src port` element captures all packets originating from a specific port.

SYNTAX

src port *port*

Note: This element can be prepended by tcp or udp. For information, see ***tcp*** on page 356 and ***udp*** on page 357.

PARAMETERS

`port`	Integer. The port from which the packet is sent.

EXAMPLE

The following filter string saves packets that originated from port 80:

```
src port 80
```

tcp

PURPOSE

The `tcp` element captures all TCP packets. This element can be prepended to port-related elements.

Note: When not prepended to other elements, the `tcp` element is the equivalent of `ip proto tcp`.

SYNTAX

tcp

tcp *element*

PARAMETERS

`element`	String. A port-related filter string element that should be restricted to saving only TCP packets. This can be the following: • `dst port` - Capture all TCP packets destined for a specific port. • `port` - Capture all TCP packets originating from or destined for a specific port. • `src port` - Capture all TCP packets originating from a specific port.

EXAMPLE 1

The following filter string captures all TCP packets:

```
tcp
```

EXAMPLE 2

The following filter string captures all TCP packets destined for port 80:

```
tcp dst port 80
```

udp

PURPOSE

The `udp` element captures all UDP packets. This element can be prepended to port-related elements.

Note: When not prepended to other elements, the `udp` element is the equivalent of `ip proto udp`.

SYNTAX

udp

udp *element*

PARAMETERS

`element`	String. A port-related filter string element that should be restricted to saving only UDP packets. This can be the following: • `dst port` - Capture all UDP packets destined for a specific port. • `port` - Captures all UDP packets originating from or destined for a specific port. • `src port` - Capture all UDP packets originating from a specific port.

EXAMPLE 1

The following filter string captures all UDP packets:

```
udp
```

EXAMPLE 2

The following filter string captures all UDP packets destined for port 80:

```
udp dst port 80
```

Backing Up the ZoneAlarm Router Configuration

You can export the ZoneAlarm router configuration to a *.cfg file, and use this file to backup and restore ZoneAlarm router settings, as needed. The file includes all your settings.

Exporting the ZoneAlarm Router Configuration

Exporting the ZoneAlarm router configuration creates a configuration file.

To export the ZoneAlarm router configuration

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

   The Tools 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.

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

Importing the ZoneAlarm Router Configuration

In order to restore your ZoneAlarm router's configuration from a configuration file, you must import the file.

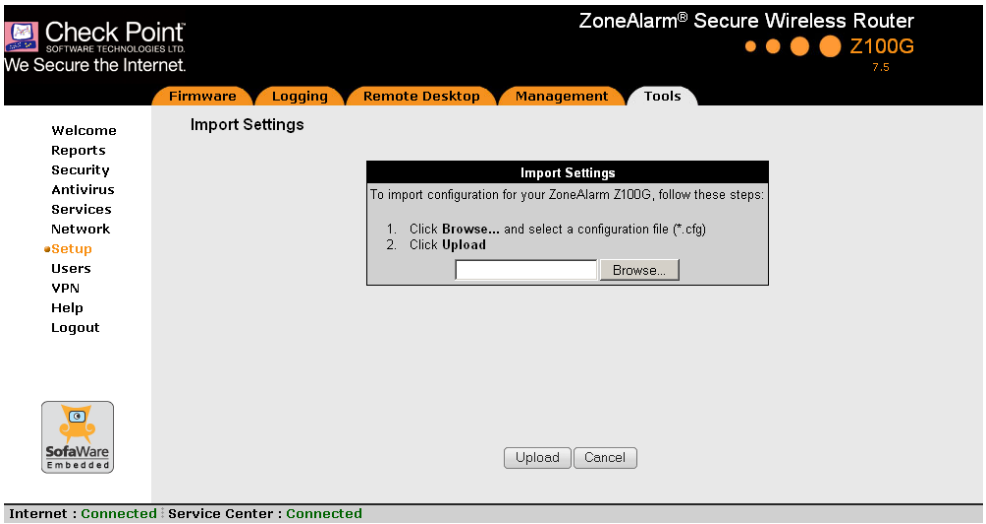
To import the ZoneAlarm router configuration

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

   The Tools page appears.

2. Click Import.

   The Import Settings page appears.



3. Do one of the following:

   - In the Import Settings field, type the full path to the configuration file.

   Or

   - Click Browse, and browse to the configuration file.

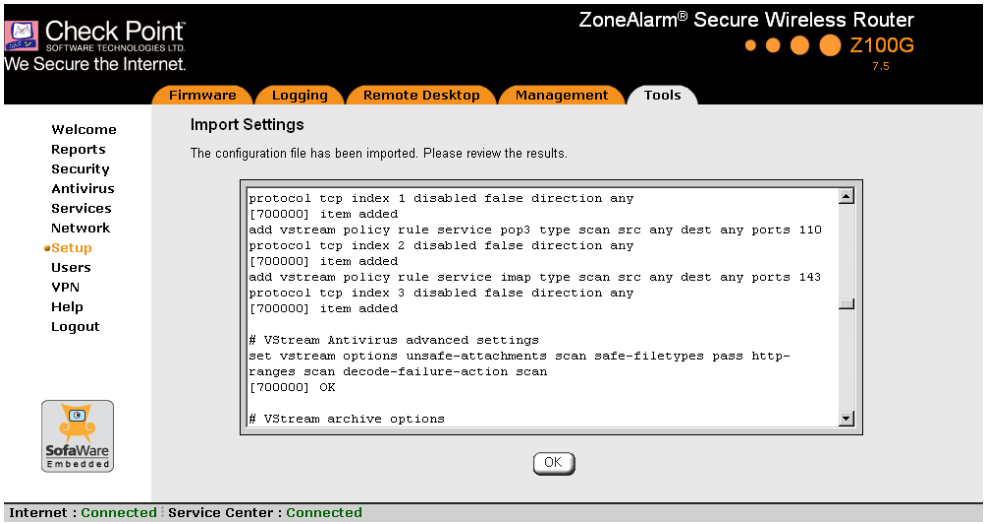
4. Click Upload.

   A confirmation message appears.

5. Click OK.

The ZoneAlarm router settings are imported.

The Import Settings page displays the configuration file's content and the result of implementing each configuration command.



Note: If the router's IP address changed as a result of the configuration import, your computer may be disconnected from the network; therefore you may not be able to see the results.

Resetting the ZoneAlarm Router to Defaults

You can reset the ZoneAlarm router to its default settings. When you reset your ZoneAlarm router, it reverts to the state it was originally in when you purchased it.

Warning: This operation erases all your settings and password information. You will have to set a new password and reconfigure your ZoneAlarm router for Internet connection. For information on performing these tasks, see ***Setting Up the ZoneAlarm Router*** on page 39.

This operation also resets your router to its default Product Key. Therefore, if you upgraded your license, you should save your Product Key before resetting to defaults. You can view the installed Product Key by in the ZoneAlarm Licensing Wizard. For information on accessing this wizard, see ***Upgrading Your License*** on page 335.

You can reset the ZoneAlarm router to defaults via the Web management interface (software) or by manually pressing the Reset button (hardware) located at the back of the ZoneAlarm router.

When resetting the router via the ZoneAlarm Portal, you can choose to keep the current firmware or to revert to the firmware version that shipped with the ZoneAlarm router. In contrast, using the Reset button automatically reverts the firmware version.

To reset the ZoneAlarm router to factory defaults via the Web interface

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

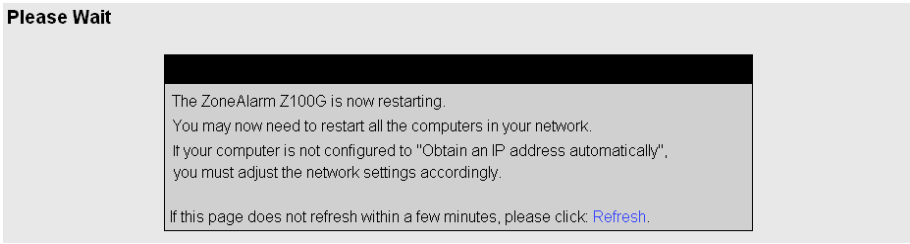
   The Tools page appears.

2. Click Factory Settings.

A confirmation message appears.

3. To revert to the firmware version that shipped with the router, select the check box.
4. Click OK.

   - The Please Wait screen appears.



   - The ZoneAlarm router returns to its factory defaults.
   - The ZoneAlarm router is restarted.

     This may take a few minutes.
   - The Login page appears.

To reset the ZoneAlarm router to factory defaults using the Reset button

1. Make sure the ZoneAlarm router is powered on.
2. Using a pointed object, press the RESET button on the back of the ZoneAlarm router steadily for seven seconds and then release it.
3. Allow the ZoneAlarm router to boot-up until the system is ready.

   For information on the router's front and rear panels, see the *Getting to Know Your Router* section in ***Introduction*** on page 1.

Warning: If you choose to reset the ZoneAlarm router by disconnecting the power cable and then reconnecting it, be sure to leave the ZoneAlarm router disconnected for at least three seconds. Disconnecting and reconnecting the power without waiting might cause permanent damage.

Running Diagnostics

You can view technical information about your ZoneAlarm router's hardware, firmware, license, network status, and Service Center.

This information is useful for troubleshooting. You can export it to an *.html file and send it to technical support.

To view diagnostic information

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

   The Tools page appears.

2. Click Diagnostics.

   Technical information about your ZoneAlarm router appears in a new window.

3. To save the displayed information to an *.html 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 *.html file is created and saved to the specified directory.

4. To refresh the contents of the window, click Refresh.

   The contents are refreshed.

5. To close the window, click Close.

Rebooting the ZoneAlarm Router

If your ZoneAlarm router is not functioning properly, rebooting it may solve the problem.

To reboot the ZoneAlarm router

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

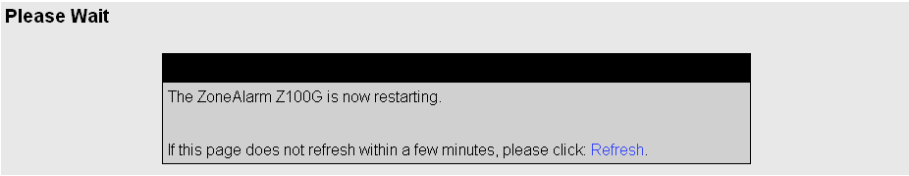
   The Firmware page appears.

2. Click Restart.

   A confirmation message appears.

3. Click OK.

   - The Please Wait screen appears.



   - The ZoneAlarm router is restarted.

     This may take a few minutes.

   - The Login page appears.

Chapter 18

Using Network Printers

This chapter describes how to set up and use network printers.

This chapter includes the following topics:

Overview

The ZoneAlarm Z100G router includes a built-in print server, enabling you to connect USB-based printers to the router and share them across the network.

Note: When using computers with a Windows 2000/XP operating system, the ZoneAlarm router supports connecting up to four USB-based printers to the router. When using computers with a MAC OS-X operating system, the ZoneAlarm router supports connecting one printer.

The router automatically detects printers as they are plugged in, and they immediately become available for printing. Usually, no special configuration is required on the ZoneAlarm router.

Note: The ZoneAlarm print server supports printing via "all-in-one" printers. Copying and scanning functions are not supported.

Setting Up Network Printers

To set up a network printer

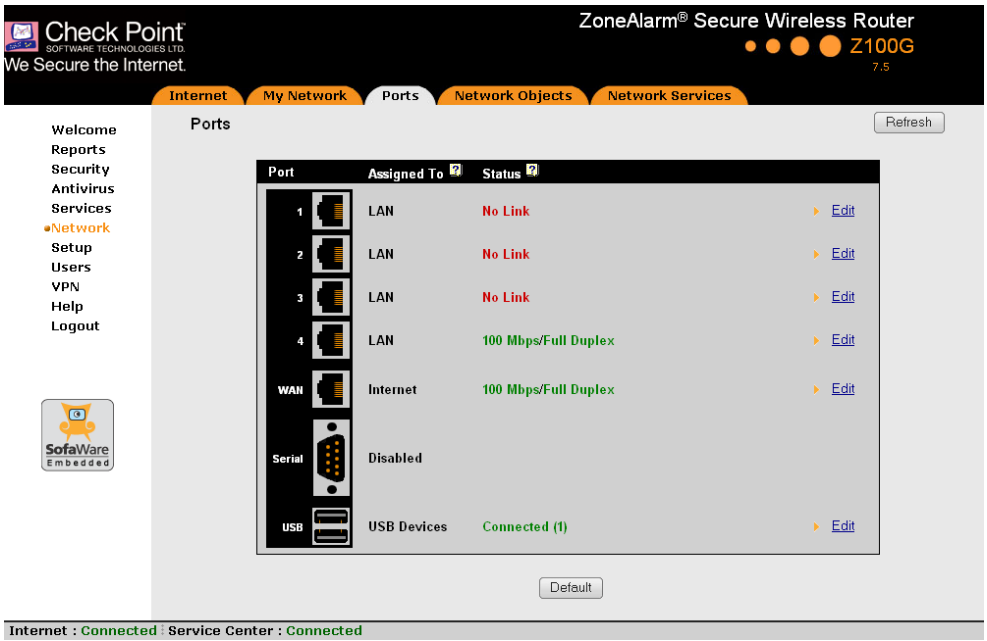
1. Connect the network printer to the ZoneAlarm router.

   See Connecting the Router to Network Printers.

2. Turn the printer on.

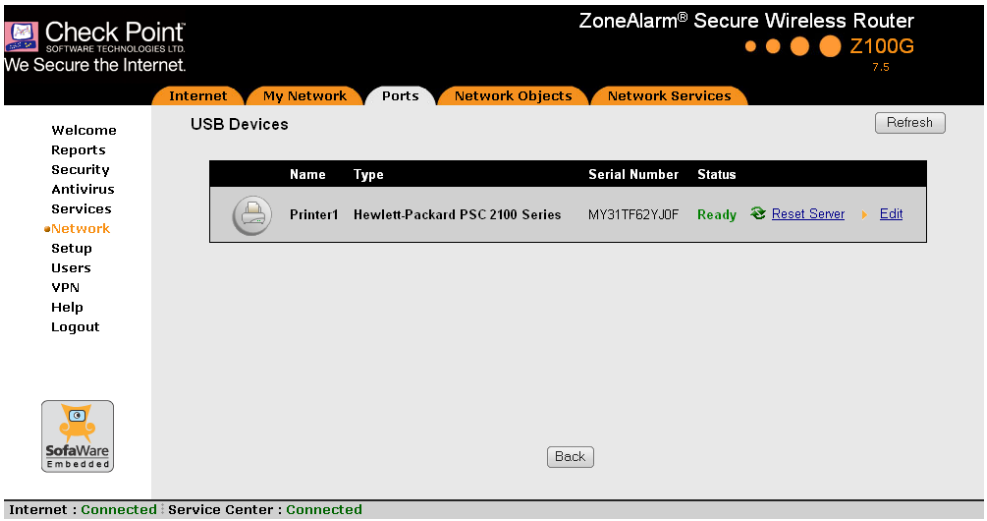
3. In the ZoneAlarm Portal, click Network in the main menu, and click the Ports tab.

   The Ports page appears.



4. Next to USB, click Edit.

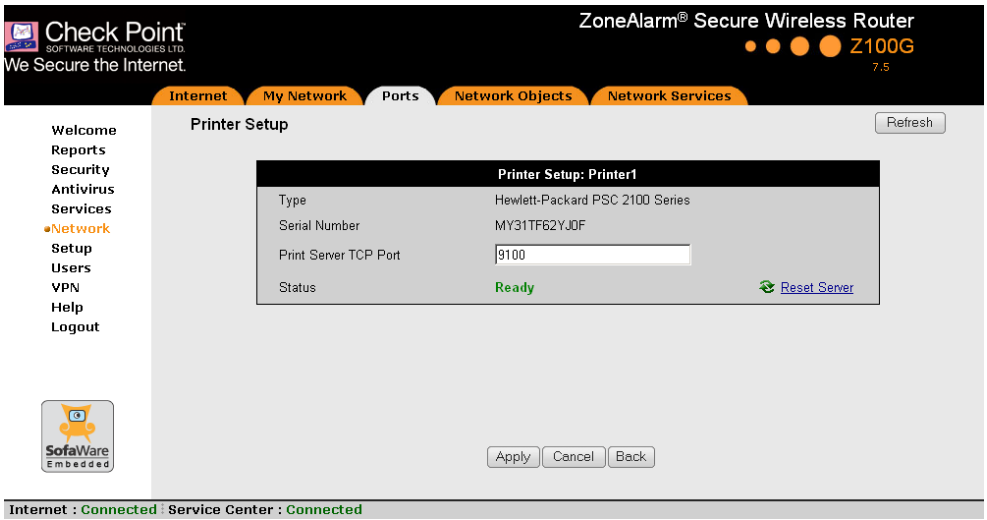
The USB Devices page appears. If the ZoneAlarm router detected the printer, the printer is listed on the page.



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

5. Next to the printer, click Edit.

   The Printer Setup page appears.



6. Write down the port number allocated to the printer.

   The port number appears in the Printer Server TCP Port field. You will need this number later, when configuring computers to use the network printer.

7. To change the port number, do the following:

   a. Type the desired port number in the Printer Server TCP Port field.

Note: Printer port numbers may not overlap, and must be high ports.

   b. Click Apply.

   You may want to change the port number if, for example, the printer you are setting up is intended to replace another printer. In this case, you should change the replacement printer's port number to the old printer's port number, and you can skip the next step.

8. Configure each computer from which you want to enable printing to the network printer.

   See ***Configuring Computers to Use Network Printers*** on page 371.

Configuring Computers to Use Network Printers

Perform the relevant procedure on each computer from which you want to enable printing via the ZoneAlarm print server to a network printer.

Windows Vista

This procedure is relevant for computers with a Windows Vista operating system.

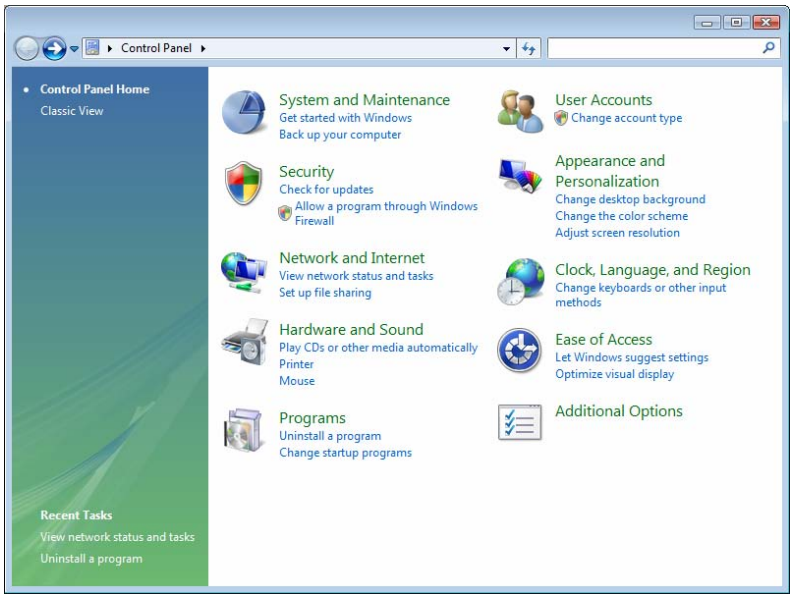
To configure a computer to use a network printer

1. If the computer for which you want to enable printing is located on the WAN, create an Allow rule for connections from the computer to This Gateway.

   See ***Adding and Editing Rules*** on page 176.

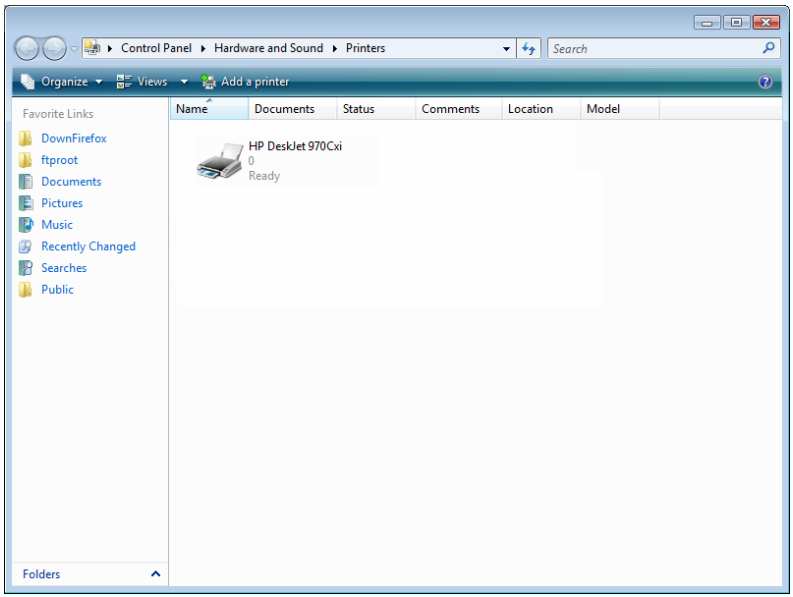
2. Click Start > Control Panel.

   The Control Panel window opens.



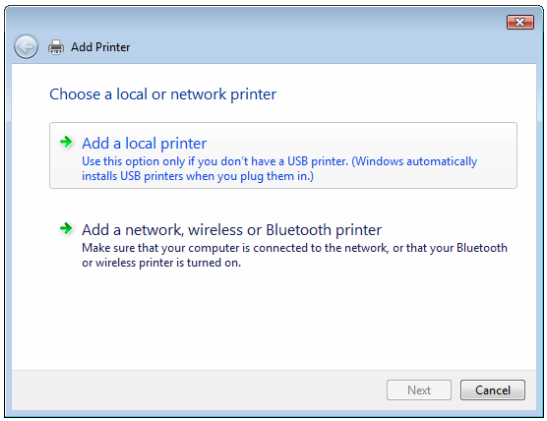
3. Under Hardware and Sound, click Printer.

The Printers screen appears.



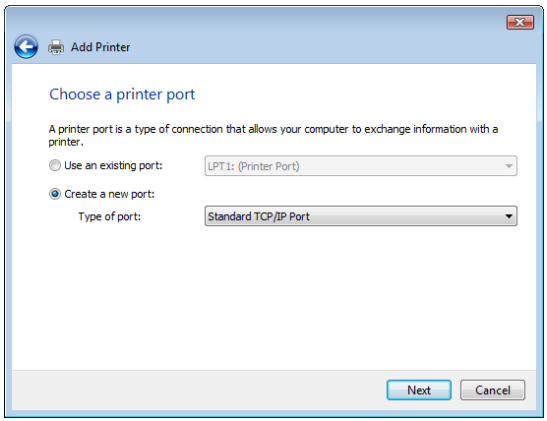
4. Click Add a printer.

   The Add Printer wizard opens displaying the Choose a local or network printer screen.



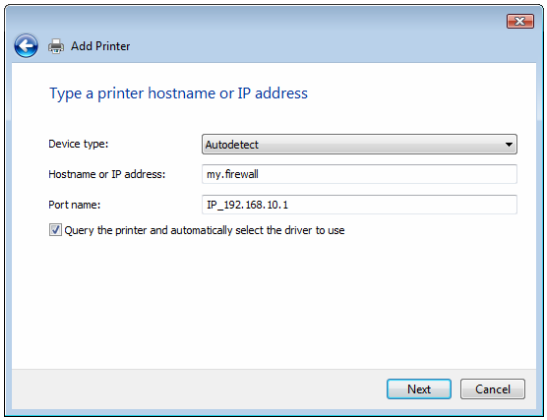
5. Click Add a local printer.
6. Click Next.

The Choose a printer port dialog box appears.



7. Click Create a new port.
8. In the Type of port drop-down list, select Standard TCP/IP Port.
9. Click Next.

   The Type a printer hostname or IP address dialog box appears.



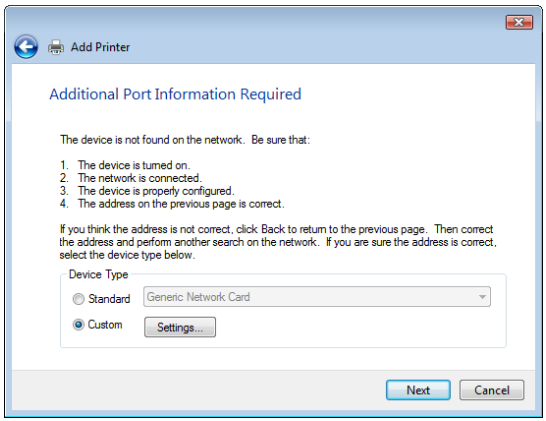
10. In the Device type drop-down list, select Autodetect.
11. In the Hostname or IP address field, type the ZoneAlarm router's LAN IP address, or "my.firewall".

    You can find the LAN IP address in the ZoneAlarm Portal, under Network > My Network.

12. In the Port name field, type the port name.
13. Select the Query the printer and automatically select the driver to use check box.
14. Click Next.

    The following things happen:

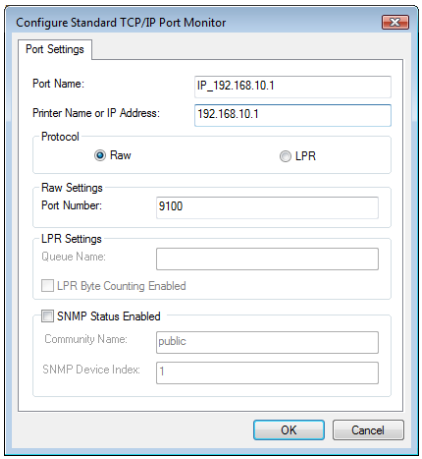
    - If Windows cannot identify your printer, the Additional Port Information Required dialog box appears.



    Do the following:

    1) Click Custom.
    2) Click Settings.

The Configure Standard TCP/IP Port Monitor dialog box opens.



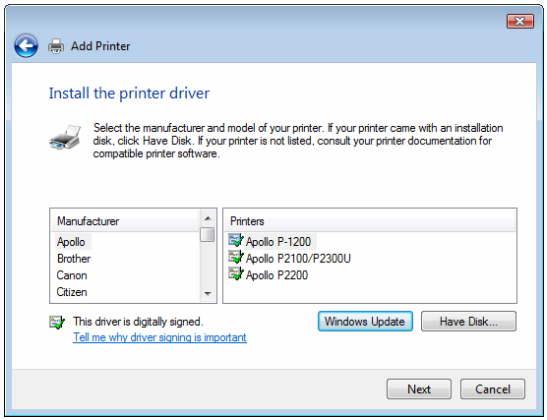
3) In the Protocol area, make sure that Raw is selected.

4) In the Port Number field, type the printer's port number, as shown in the Printers page.

5) Click OK.

6) Click Next.

- The Install the printer driver dialog box displayed.

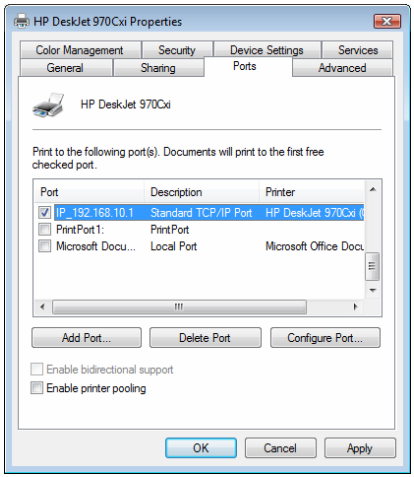


15. Do one of the following:
    - Use the lists to select the printer's manufacturer and model.
    - If your printer does not appear in the lists, insert the CD that came with your printer in the computer's CD-ROM drive, and click Have Disk.
16. Click Next.
17. Complete the remaining dialog boxes in the wizard as desired, and click Finish.

    The printer appears in the Printers and Faxes window.
18. Right-click the printer and click Properties in the popup menu.

    The printer's Properties dialog box opens.
19. In the Ports tab, in the list box, select the port you added.

    The port's name is IP_<LAN IP address>.



20. Click OK.

Windows 2000/XP

This procedure is relevant for computers with a Windows 2000/XP operating system.

To configure a computer to use a network printer

1. If the computer for which you want to enable printing is located on the WAN, create an Allow rule for connections from the computer to This Gateway.

   See ***Adding and Editing Rules*** on page 176.

2. Click Start > Settings > Control Panel.

   The Control Panel window opens.

3. Click Printers and Faxes.

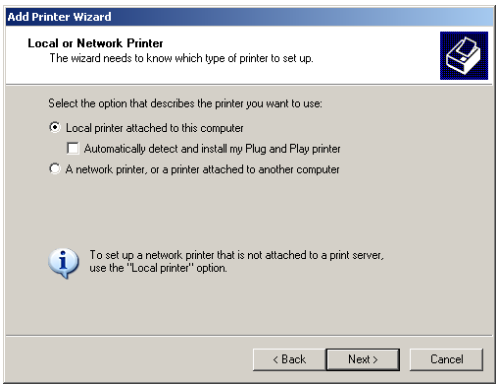
   The Printers and Faxes window opens.

4. Right-click in the window, and click Add Printer in the popup menu.

   The Add Printer Wizard opens with the Welcome dialog box displayed.

5. Click Next.

The Local or Network Printer dialog box appears.

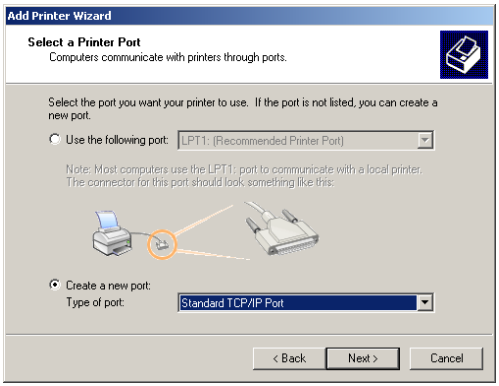


6. Click Local printer attached to this computer.

Note: Do not select the Automatically detect and install my Plug and Play printer check box.

7. Click Next.

   The Select a Printer Port dialog box appears.

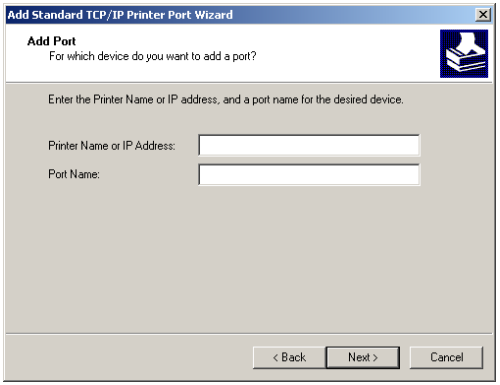


8. Click Create a new port.
9. In the Type of port drop-down list, select Standard TCP/IP Port.
10. Click Next.

The Add Standard TCP/IP Port Wizard opens with the Welcome dialog box displayed.

11. Click Next.

    The Add Port dialog box appears.



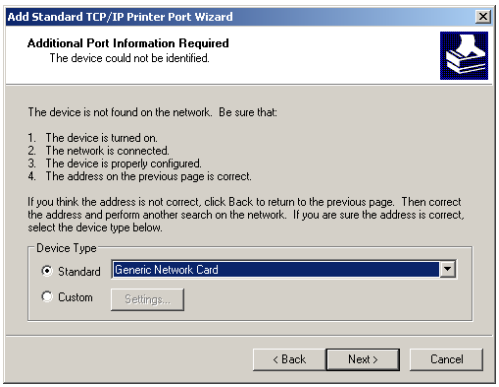
12. In the Printer Name or IP Address field, type the ZoneAlarm router's LAN IP address, or "my.firewall".

    You can find the LAN IP address in the ZoneAlarm Portal, under Network > My Network.

    The Port Name field is filled in automatically.

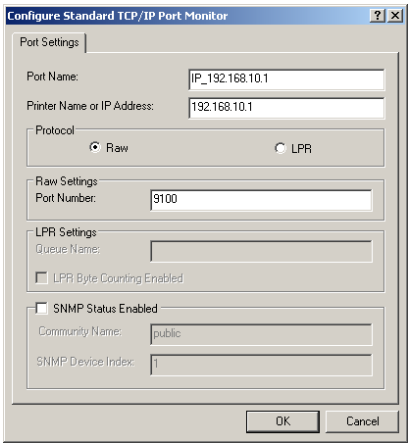
13. Click Next.

The Add Standard TCP/IP Printer Port Wizard opens, with the Additional Port Information Required dialog box displayed.



14. Click Custom.
15. Click Settings.

    The Configure Standard TCP/IP Port Monitor dialog box opens.

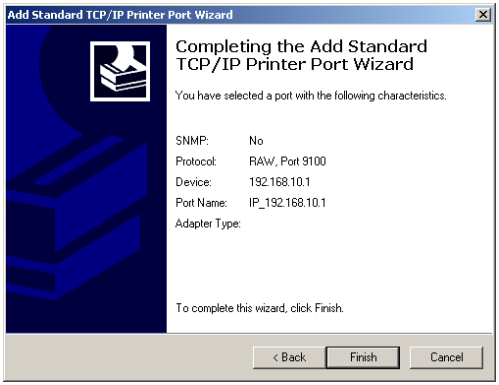


16. In the Port Number field, type the printer's port number, as shown in the Printers page.
17. In the Protocol area, make sure that Raw is selected.
18. Click OK.

    The Add Standard TCP/IP Printer Port Wizard reappears.

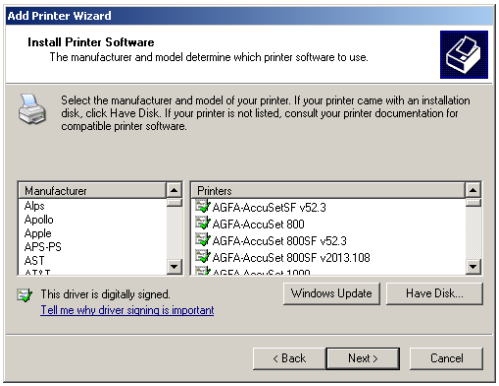
19. Click **Next**.

    The **Completing the Add Standard TCP/IP Printer Port Wizard** dialog box appears.



20. Click **Finish**.

    The **Add Printer Wizard** reappears, with the **Install Printer Software** dialog box displayed.



21. Do one of the following:

    - Use the lists to select the printer's manufacturer and model.
    - If your printer does not appear in the lists, insert the CD that came with your printer in the computer's CD-ROM drive, and click **Have Disk**.

22. Click **Next**.

23. Complete the remaining dialog boxes in the wizard as desired, and click Finish.

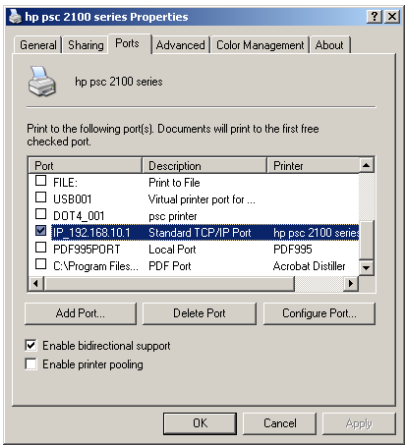
    The printer appears in the Printers and Faxes window.

24. Right-click the printer and click Properties in the popup menu.

    The printer's Properties dialog box opens.

25. In the Ports tab, in the list box, select the port you added.

    The port's name is IP_<LAN IP address>.



26. Click OK.

MAC OS-X

This procedure is relevant for computers with the latest version of the MAC OS-X operating system.

Note: This procedure may not apply to earlier MAC OS-X versions.

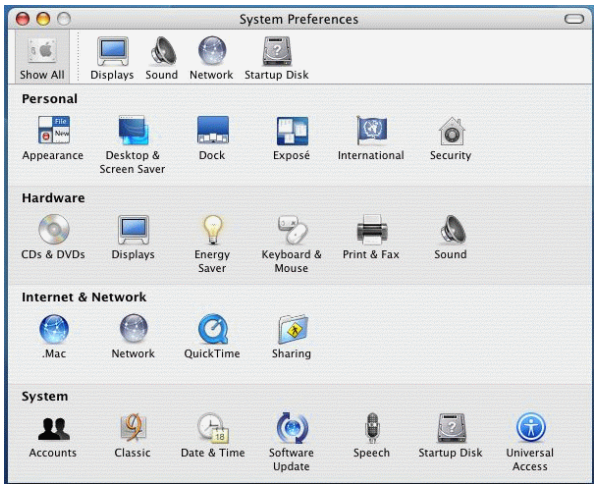
To configure a computer to use a network printer

1. If the computer for which you want to enable printing is located on the WAN, create an Allow rule for connections from the computer to This Gateway.

   See ***Adding and Editing Rules*** on page 176.

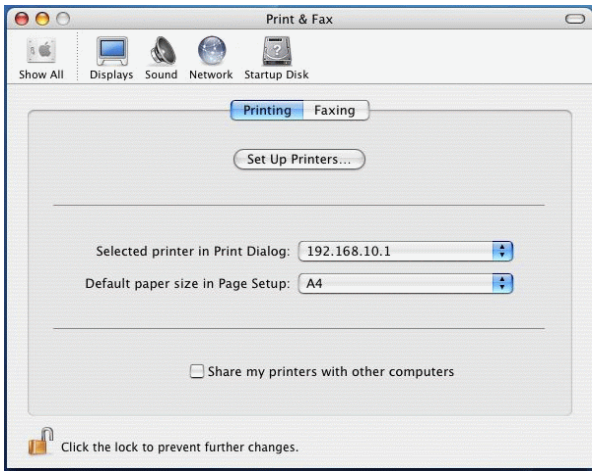
2. Choose Apple -> System Preferences.

   The System Preferences window appears.



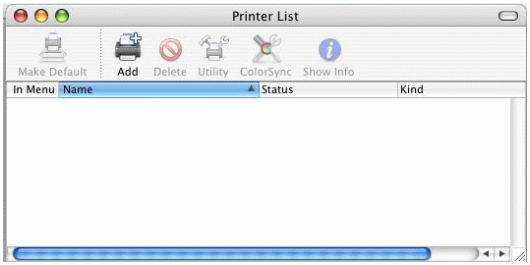
3. Click Show All to display all categories.
4. In the Hardware area, click Print & Fax.

The Print & Fax window appears.



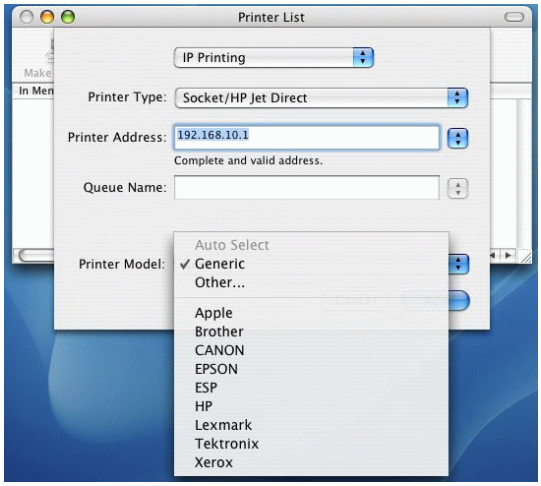
5. In the Printing tab, click Set Up Printers.

   The Printer List window appears.



6. Click Add.

New fields appear.

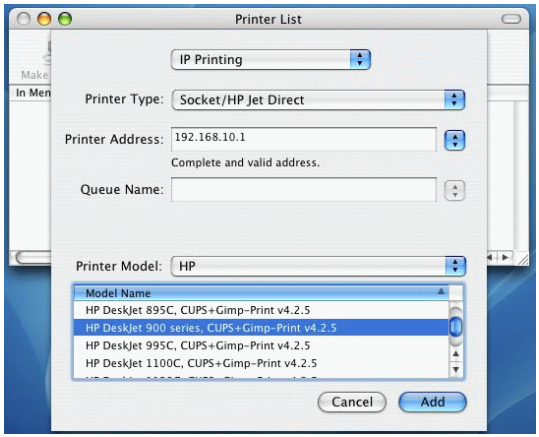


7. In the first drop-down list, select IP Printing.
8. In the Printer Type drop-down list, select Socket/HP Jet Direct.
9. In the Printer Address field, type the ZoneAlarm router's LAN IP address, or "my.firewall".

   You can find the LAN IP address in the ZoneAlarm Portal, under Network > My Network.
10. In the Queue Name field, type the name of the required printer queue.

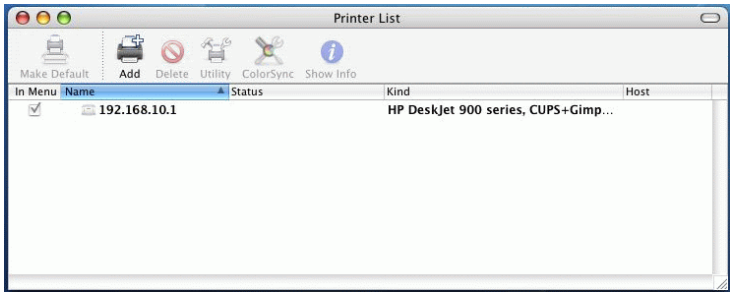
    For example, the printer queue name for HP printers is RAW.
11. In the Printer Model list, select the desired printer type.

A list of models appears.



12. In the Model Name list, select the desired model.
13. Click Add.

    The new printer appears in the Printer List window.



14. In the Printer List window, select the newly added printer, and click Make Default.

Viewing Network Printers

To view network printers

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

   The Ports page appears.

2. Next to USB, click Edit.

   The USB Devices page appears, displaying a list of connected printers.

   For each printer, the model, serial number, and status is displayed.

   A printer can have the following statuses:

   - Initialize. The printer is initializing.
   - Ready. The printer is ready.
   - Not Ready. The printer is not ready. For example, it may be out of paper.
   - Printing. The printer is processing a print job.
   - Restarting. The printer server is restarting.
   - Fail. An error occurred. See the Event Log for details (***Viewing the Event Log*** on page 151).

3. To refresh the display, click Refresh.

Changing Network Printer Ports

When you set up a new network printer, the ZoneAlarm router automatically assigns a port number to the printer. If you want to use a different port number, you can easily change it, as described in ***Setting Up Network Printers*** on page 368.

However, you may sometimes need to change the port number after completing printer setup. For example, you may want to replace a malfunctioning network printer, with another existing network printer, without reconfiguring the client computers. To do this, you must change the replacement printer's port number to the malfunctioning printer's port number, as described below.

Note: Each printer port number must be different, and must be a high port.

To change a printer's port

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

   The Ports page appears.
2. Next to USB, click Edit.

   The USB Devices page appears, displaying a list of connected printers.
3. Next to the desired printer, click Edit.

   The Printer Setup page appears.
4. In the printer's Printer Server TCP Port field, type the desired port number.
5. Click Apply.

Resetting Network Printers

You can cause a network printer to restart the current print job, by resetting the network printer. You may want to do this if the print job has stalled.

To reset a network printer

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

   The Ports page appears.
2. Next to USB, click Edit.

   The USB Devices page appears, displaying a list of connected printers.
3. Next to the desired printer, click Reset Server.

   The network printer's current print job is restarted.

Chapter 19

Troubleshooting

This chapter provides solutions to common problems you may encounter while using the ZoneAlarm router.

Note: For information on troubleshooting wireless connectivity, see ***Troubleshooting Wireless Connectivity*** on page 135.

This chapter includes the following topics:

Connectivity

I cannot access the Internet. What should I do?

- Verify that the ZoneAlarm router is operating. If not, check the power connection to the ZoneAlarm router.
- Check if the LED for the WAN port is green. If not, check the network cable to the modem and make sure the modem is turned on.
- Check if the LED for the LAN port used by your computer is green. If not, check if the network cable linking your computer to the ZoneAlarm router is connected properly. Try replacing the cable or connecting it to a different LAN port.
- Using your Web browser, go to http://my.firewall and see whether "Connected" appears on the Status Bar. Make sure that your ZoneAlarm router network settings are configured as per your ISP directions.
- Check your TCP/IP configuration according to ***Installing and Setting up the ZoneAlarm Router*** on page 19.
- If Web Filtering or Email Filtering are on, try turning them off.

- Check if you have defined firewall rules which block your Internet connectivity.
- Check with your ISP for possible service outage.
- Check whether you are exceeding the maximum number of computers allowed by your license, by viewing the My Computers page.

I cannot access my DSL broadband connection. What should I do?

DSL equipment comes in two flavors: bridges (commonly known as DSL modems) and routers. Some DSL equipment can be configured to work both ways.

- If you connect to your ISP using a PPPoE or PPTP dialer defined in your operating system, your equipment is most likely configured as a DSL bridge. Configure a PPPoE or PPTP type DSL connection.
- If you were not instructed to configure a dialer in your operating system, your equipment is most likely configured as a DSL router. Configure a LAN connection, even if you are using a DSL connection.

For instructions, see ***Configuring the Internet Connection*** on page 55.

I cannot access my Cable broadband connection. What should I do?

- Some cable ISPs require you to register the MAC address of the device behind the cable modem. You may need to clone your Ethernet adapter MAC address onto the ZoneAlarm router. For instructions, see ***Configuring the Internet Connection*** on page 55.
- Some cable ISPs require using a hostname for the connection. Try reconfiguring your Internet connection and specifying a hostname. For further information, see ***Configuring the Internet Connection*** on page 55.

I cannot access http://my.firewall. What should I do?

- Verify that the ZoneAlarm router is operating.
- Check if the LED for the LAN port used by your computer is green. If not, check if the network cable linking your computer to the ZoneAlarm router is connected properly.
- By default, unencrypted HTTP access is not allowed from the wireless LAN to http://my.firewall. Therefore, if you are connecting from the wireless LAN, try connecting to https://my.firewall instead.
- Try surfing to 192.168.10.1 instead of to my.firewall.

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

- Check your TCP/IP configuration according to ***Installing and Setting up the ZoneAlarm Router*** on page 19.
- Restart your ZoneAlarm router and your broadband modem by disconnecting the power and reconnecting after 5 seconds.
- If your Web browser is configured to use an HTTP proxy to access the Internet, add my.firewall to your proxy exceptions list.

My network seems extremely slow. What should I do?

- The Ethernet cables may be faulty. For proper operation, the ZoneAlarm router requires STP CAT5 (Shielded Twisted Pair Category 5) Ethernet cables. Make sure that this specification is printed on your cables.
- Your Ethernet card may be faulty or incorrectly configured. Try replacing your Ethernet card.
- There may be an IP address conflict in your network. Check that the TCP/IP settings of all your computers are configured to obtain an IP address automatically.

I changed the network settings to incorrect values and am unable to correct my error. What should I do?

Reset the network to its default settings using the button on the back of the ZoneAlarm router unit. See ***Resetting the ZoneAlarm Router to Defaults*** on page 361.

I am using the ZoneAlarm router behind another NAT device, and I am having problems with some applications. What should I do?

By default, the ZoneAlarm router performs Network Address Translation (NAT). It is possible to use the ZoneAlarm router behind another device that performs NAT, such as a DSL router or Wireless router, but the device will block all incoming connections from reaching your ZoneAlarm router.

To fix this problem, do ONE of the following. (The solutions are listed in order of preference.)

- Consider whether you really need the router. The ZoneAlarm router can be used as a replacement for your router, unless you need it for some additional functionality that it provides.

- If possible, disable NAT in the router. Refer to the router's documentation for instructions on how to do this.
- If the router has a "DMZ Computer" or "Exposed Host" option, set it to the ZoneAlarm router's external IP address.
- Open the following ports in the NAT device:
  - UDP 9281/9282
  - UDP 500
  - UDP 2746
  - TCP 256
  - TCP 264
  - ESP IP protocol 50
  - TCP 981

I cannot receive audio or video calls through the ZoneAlarm router. What should I do?

To enable audio/video, you must configure an IP Telephony (H.323) virtual server. For instructions, see ***Configuring Servers*** on page 185.

I run a public Web server at home but it cannot be accessed from the Internet. What should I do?

Configure a virtual Web Server. For instructions, see ***Configuring Servers*** on page 185.

I cannot connect to the LAN network from the WLAN network. What should I do?

By default, connections from the WLAN network to the LAN network are blocked. To allow traffic from the WLAN to the LAN, configure appropriate firewall rules. For instructions, see ***Using Rules*** on page 172.

Service Center and Upgrades

I have exceeded my node limit. What does this mean? What should I do?

Your Product Key specifies a maximum number of nodes that you may connect to the ZoneAlarm router.

The ZoneAlarm router tracks the cumulative number of nodes on the internal network that have communicated through the firewall. When the ZoneAlarm router encounters an IP address that exceeds the licensed node limit, the My Computers page displays a warning message and marks nodes over the node limit in red. These nodes will not be able to access the Internet through the ZoneAlarm router, but will be protected. The Event Log page also warns you that you have exceeded the node limit.

To upgrade your ZoneAlarm router to support more nodes, purchase a new Product Key. Contact your reseller for upgrade information.

While trying to connect to a Service Center, I received the message "The Service Center did not respond". What should I do?

- If you are using a Service Center other than the Check Point Service Center, check that the Service Center IP address is typed correctly.
- The ZoneAlarm router connects to the Service Center using UDP ports 9281/9282. If the ZoneAlarm router is installed behind another firewall, make sure that these ports are open.

Other Problems

I have forgotten my password. What should I do?

Reset your ZoneAlarm router to factory defaults using the Reset button as detailed in ***Resetting the ZoneAlarm Router to Defaults*** on page 361.

Why are the date and time displayed incorrectly?

You can adjust the time on the Setup page's Tools tab. For information, see ***Setting the Time on the Router*** on page 341.

I cannot use a certain network application. What should I do?

Look at the Event Log page. If it lists blocked attacks, do the following:

- Set the ZoneAlarm router's firewall level to Low and try again.
- If the application still does not work, set the computer on which you want to use the application to be the exposed host.

  For instructions, see Defining an Exposed Host.

When you have finished using the application, make sure to clear the exposed host setting, otherwise your security might be compromised.

In the ZoneAlarm Portal, I do not see the pop-up windows that the guide describes. What should I do?

Disable any pop-up blockers for http://my.firewall.

Chapter 20

Specifications

This chapter includes the following topics:

Technical Specifications

Check Point is committed to protecting the environment. The ZoneAlarm unified threat management router is compliant with the RoHS Directive, meeting the European Union's strict restrictions on hazardous substances.

RoHS & WEEE Declaration and Certification

The ZoneAlarm router has been verified to comply with the following directives, throughout the design, development, and supply chain stages:

- Directive of the European Parliament and of the Council, of 27 January 2003, on the Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment (RoHS – 2002/95/EC)
- Directive of the European Parliament and of the Council, of 27 January 2003, on Waste Electrical and Electronic Equipment (WEEE – 2002/96/CE)

For a copy of the original signed declaration (in full conformance with EN45014), contact SofaWare technical support at www.sofaware.com/support.

Table 86: ZoneAlarm Attributes

Attribute	ZoneAlarm Z100G SBXWZA-166LHGE-5
Physical Attributes	
Dimensions (width x height x depth)	200 x 33 x 130 mm (7.87 x 1.3 x 5.12 inches) (incl. antenna connectors)
Weight	635 g (1.40 lbs)
Retail Box Dimensions (width x height x depth)	290 x 250 x 80 mm (11.42 x 9.84 x 3.15 inches)
5V Power Supply Unit	
Power Supply Nominal Input	In: 100~240VAC @ 0.5A
Power Supply Nominal Output	12VDC @ 1.5 A
Max. Power Consumption	6.5W, plus up to 5W for host-powered USB devices
Environmental Conditions	
Temperature: Storage/Transport	-5ºC ~ 80ºC
Temperature: Operation	0ºC ~ 40ºC
Humidity: Storage/Operation	10~95% / 10~90% (non-condensed)

Applicable Standards	
Safety	cULus, CB, LVD
Quality	IISO9001, ISO 14001, TL9000
EMC	CE . FCC 15B.VCCI
Reliability	EN 300 019 - 1, 2, 3
Environment	RoHS & WEEE
RF	R&TTE .FCC15C,TELCO
Wireless Attributes	
Operation Frequency	2.412-2.484 MHz
Transmission Power	79.4 mW
Modulation	OFDM, DSSS, 64QAM, 16QAM, QPSK, BPSK, CCK, DQPSK, DBPSK
WPA Authentication Modes	EAP-TLS, EAP-TTLS, PEAP (EAP-GTC), PEAP (EAP-MSCHAP V2)

CE Declaration of Conformity

SofaWare Technologies Ltd., 3 Hilazon St., Ramat-Gan Israel, hereby declares that this equipment is in conformity with the essential requirements specified in Article 3.1 (a) and 3.1 (b) of:

- Directive 89/336/EEC (EMC Directive)
- Directive 73/23/EEC (Low Voltage Directive – LVD)
- Directive 99/05/EEC (Radio Equipment and Telecommunications Terminal Equipment Directive)

In accordance with the following standards:

Table 87: ZoneAlarm Router Standards

Attribute	ZoneAlarm Z100G SBXWZA-166LHGE-5
EMC	EN 55022
	EN 61000-3-2
	EN 61000-3-3
	EN 61000-4-2
	EN 61000-4-3
	EN 61000-4-4
	EN 61000-4-5
	EN 61000-4-6

Attribute	ZoneAlarm Z100G SBXWZA-166LHGE-5
	EN 61000-4-8
	EN 61000-4-11
	ENV50204
	EN 61000-4-5
	EN 61000-4-6
	EN 61000-4-7
	EN 61000-4-8
	EN 61000-4-9
	EN 61000-4-10
	EN 61000-4-11
	EN 61000-4-12
Safety	EN 60950
	IEC 60950

The "CE" mark is affixed to this product to demonstrate conformance to the R&TTE Directive 99/05/EEC (Radio Equipment and Telecommunications Terminal Equipment Directive) and FCC Part 15 Class B.

The product has been tested in a typical configuration. For a copy of the Original Signed Declaration (in full conformance with EN45014), please contact SofaWare at the above address.

Federal Communications Commission Radio Frequency Interference Statement

This equipment complies with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

Shielded cables must be used with this equipment to maintain compliance with FCC regulations.

Any changes or modifications to this product not explicitly approved by the manufacturer could void the user's authority to operate the equipment and any assurances of Safety or Performance, and could result in violation of Part 15 of the FCC Rules.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This Class B digital apparatus complies with Canadian ICES-003.

FCC Radiation Exposure Statement for Wireless Models

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. The antenna(s) used for this equipment must be installed to provide a separation distance of at least eight inches (20 cm) from all persons. This equipment must not be operated in conjunction with any other antenna.

Glossary of Terms

A

ADSL Modem

A device connecting a computer to the Internet via an existing phone line. ADSL (Asymmetric Digital Subscriber Line) modems offer a high-speed 'always-on' connection.

C

CA

The Certificate Authority (CA) issues certificates to entities such as gateways, users, or computers. The entity later uses the certificate to identify itself and provide verifiable information. For instance, the certificate includes the Distinguished Name (DN) (identifying information) of the entity, as well as the public key (information about itself), and possibly the IP address.

After two entities exchange and validate each other's certificates, they can begin encrypting information between themselves using the public keys in the certificates.

Cable Modem

A device connecting a computer to the Internet via the cable television network. Cable modems offer a high-speed 'always-on' connection.

Certificate Authority

The Certificate Authority (CA) issues certificates to entities such as gateways, users, or computers. The entity later uses the certificate to identify itself and provide verifiable information. For instance, the certificate includes the Distinguished Name (DN) (identifying information) of the entity, as well as the public key (information about itself), and possibly the IP address.

After two entities exchange and validate each other's certificates, they can begin encrypting information between themselves using the public keys in the certificates.

Cracking

An activity in which someone breaks into someone else's computer system, bypasses passwords or licenses in computer programs; or in other ways intentionally breaches computer security. The end result is that whatever resides on the computer can be viewed and sensitive data can be stolen without anyone knowing about it. Sometimes, tiny programs are 'planted' on the computer that are designed to watch out for, seize and then transmit to another computer, specific types of data.

D

DHCP

Any machine requires a unique IP address to connect to the Internet using Internet Protocol. Dynamic Host Configuration Protocol (DHCP) is a communications protocol that assigns Internet Protocol (IP) addresses to computers on the network.

DHCP uses the concept of a "lease" or amount of time that a given IP address will be valid for a computer.

DMZ

A DMZ (demilitarized zone) is an internal network defined in addition to the LAN network and protected by the ZoneAlarm appliance.

DNS

The Domain Name System (DNS) refers to the Internet domain names, or easy-to-remember "handles", that are translated into IP addresses.

An example of a Domain Name is 'www.sofaware.com'.

Domain Name System

Domain Name System. The Domain Name System (DNS) refers to the Internet domain names, or easy-to-remember "handles", that are translated into IP addresses.

An example of a Domain Name is 'www.sofaware.com'.

E

Exposed Host

An exposed host allows one computer to be exposed to the Internet. An example of using an exposed host would be exposing a public server, while preventing outside users from getting direct access form this server back to the private network.

F

Firmware

Software embedded in a device.

G

Gateway

A network point that acts as an entrance to another network.

H

Hacking

An activity in which someone breaks into someone else's computer system, bypasses passwords or licenses in computer programs; or in other ways intentionally breaches computer security. The end result is that whatever resides on the computer can be viewed and sensitive data can be stolen without anyone knowing about it. Sometimes, tiny programs are 'planted' on the computer that are designed to watch out for, seize and then transmit to another computer, specific types of data.

HTTPS

Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL.

A protocol for accessing a secure Web server. It uses SSL as a sublayer under the regular HTTP application. This directs messages to a secure port number rather than the default Web port number, and uses a public key to encrypt data

HTTPS is used to transfer confidential user information.

Hub

A device with multiple ports, connecting several PCs or network devices on a network.

I

IP Address

An IP address is a 32-bit number that identifies each computer sending or receiving data packets across the Internet. When you request an HTML page or send e-mail, the Internet Protocol part of TCP/IP includes your IP address in the message and sends it to the IP address that is obtained by looking up the domain name in the Uniform Resource Locator you requested or in the e-mail address you're sending a note to. At the other end, the recipient can see the IP address of the Web page requestor or the e-mail sender and can respond by sending another message using the IP address it received.

IP Spoofing

A technique where an attacker attempts to gain unauthorized access through a false source address to make it appear as though communications have originated in a part of the network with higher access privileges. For example, a packet originating on the Internet may be masquerading as a local packet with the source IP address of an internal host. The firewall can protect against IP spoofing attacks by limiting network access based on the gateway interface from which data is being received.

IPSEC

IPSEC is the leading Virtual Private Networking (VPN) standard. IPSEC enables individuals or offices to establish secure communication channels ('tunnels') over the Internet.

ISP

An ISP (Internet service provider) is a company that provides access to the Internet and other related services.

L

LAN

A local area network (LAN) is a group of computers and associated devices that share a common communications line and typically share the resources of a single server within a small geographic area.

M

MAC Address
The MAC (Media Access Control) address is a computer's unique hardware number. When connected to the Internet from your computer, a mapping relates your IP address to your computer's physical (MAC) address on the LAN.

Mbps
Megabits per second. Measurement unit for the rate of data transmission.

MTU
The Maximum Transmission Unit (MTU) is a parameter that determines the largest datagram than can be transmitted by an IP interface (without it needing to be broken down into smaller units). The MTU should be larger than the largest datagram you wish to transmit un-fragmented. Note: This only prevents fragmentation locally. Some other link in the path may have a smaller MTU - the datagram will be fragmented at that point. Typical values are 1500 bytes for an Ethernet interface or 1452 for a PPP interface.

N

NAT
Network Address Translation (NAT) is the translation or mapping of an IP address to a different IP address. NAT can be used to map several internal IP addresses to a single IP address, thereby sharing a single IP address assigned by the ISP among several PCs.

Check Point FireWall-1's Stateful Inspection Network Address Translation (NAT) implementation supports hundreds of pre-defined applications, services, and protocols, more than any other firewall vendor.

NetBIOS
NetBIOS is the networking protocol used by DOS and Windows machines.

P

Packet
A packet is the basic unit of data that flows from one source on the Internet to another destination on the Internet. When any file (e-mail message, HTML file, GIF file etc.) is sent from one place to another on the Internet, the file is divided into "chunks" of an efficient size for routing. Each of these packets is separately numbered and includes the Internet address of the destination. The individual packets for a given file may travel different routes through the Internet. When they have all arrived, they are reassembled into the original file at the receiving end.

PPPoE
PPPoE (Point-to-Point Protocol over Ethernet) enables connecting multiple computer users on an Ethernet local area network to a remote site or ISP, through common customer premises equipment (e.g. modem).

PPTP

The Point-to-Point Tunneling Protocol (PPTP) allows extending a local network by establishing private "tunnels" over the Internet. This protocol it is also used by some DSL providers as an alternative for PPPoE.

R

RJ-45

The RJ-45 is a connector for digital transmission over ordinary phone wire.

Router

A router is a device that determines the next network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks.

S

Server

A server is a program (or host) that awaits and requests from client programs across the network. For example, a Web server is the computer program, running on a specific host, that serves requested HTML pages or files. Your browser is the client program, in this case.

Stateful Inspection

Stateful Inspection was invented by Check Point to provide the highest level of security by examining every layer within a packet, unlike other systems of inspection. Stateful Inspection extracts information required for security decisions from all application layers and retains this information in dynamic state tables for evaluating subsequent connection attempts. In other words, it learns!

Subnet Mask

A 32-bit identifier indicating how the network is split into subnets. The subnet mask indicates which part of the IP address is the host ID and which indicates the subnet.

T

TCP

TCP (Transmission Control Protocol) is a set of rules (protocol) used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet.

For example, when an HTML file is sent to you from a Web server, the Transmission Control Protocol (TCP) program layer in that server divides the file into one or more packets, numbers the packets, and then forwards them individually to the IP program layer. Although each packet has the same destination IP address, it may get routed differently through the network.

At the other end (the client program in your computer), TCP reassembles the individual packets and waits until they have arrived to forward them to you as a single file.

TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) is the underlying communication protocol of the Internet.

U

UDP

UDP (User Datagram Protocol) is a communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is sometimes referred to as UDP/IP. Like the Transmission Control Protocol, UDP uses the Internet Protocol to actually get a data unit (called a datagram) from one computer to another. Unlike TCP, however, UDP does not provide the service of dividing a message into packets (datagrams) and reassembling it at the other end.

UDP is often used for applications such as streaming data.

URL

A URL (Uniform Resource Locator) is the address of a file (resource) accessible on the Internet. The type of resource depends on the Internet application protocol. On the Web (which uses the Hypertext Transfer Protocol), an example of a URL is 'http://www.sofaware.com'.

V

VPN

A virtual private network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.

VPN tunnel

A secure connection between a Remote Access VPN Client and a Remote Access VPN Server.

W

WLAN

A WLAN is a wireless local area network protected by the ZoneAlarm router.

Index

P

R

S

T

U

V

W

Z