# WatchGuard® Firebox® X Edge User Guide

Firebox X Edge - Firmware Version 7.0

## Certifications and Notices

### FCC Certification

This appliance has been tested and found to comply with limits for a Class A digital appliance, pursuant to Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This appliance may not cause harmful interference.
- This appliance must accept any interference received, including interference that may cause undesired operation.

### CE Notice

The CE symbol on your WatchGuard Technologies equipment indicates that it is in compliance with the Electromagnetic Compatibility (EMC) directive and the Low Voltage Directive (LVD) of the European Union (EU).

CE

### Industry Canada

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numerique de la classe A respecte toutes les exigences du Reglement sur le materiel broulleur du Canada.

### Class A Korean Notice

사용자 안내문(A급 기기)
본 기기는 업무용으로 전자파적합등록을 받은 기기이오니,
만약 잘못 구입하셨을 때에는 구입한 곳에서 비업무용으로
교환 하시기 바랍니다.

## VCCI Notice Class A ITE

この装置は、情報処理装置等電波障害自主規制協議会（VCCI)の基準に基づくクラス A 情報技術装置です。この装置を家庭用環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

## Declaration of Conformity

# DECLARATION OF CONFORMITY

**WatchGuard Technologies, Inc.**
**505 Fifth Ave. S., Suite 500**
**Seattle, WA 98104-3892**
**USA**

**WatchGuard Technologies Inc. hereby declares that the product(s) listed below conform to the European Union directives and standards identified in this declaration.**

**Product (s):**

Internet Firewall with VPN, Models MF16S32E10, MF4S16E5

**EU Directive(s):**

Low Voltage (73/23/EEC)
Electromagnetic Compatibility (89/336/EEC)

**Standard(s):**

EN60950 3rd Ed. (1999) Safety of ITE

| | |
|---|---|
| EN50022 (1998), Class A | Emissions for ITE |
| EN50024 (1998) | Immunity for ITE |

Signature
Full Name Edward Borey
Position Chairman, CEO
Date 14 July 2004

# Notice to Users

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

# WatchGuard Firebox Software End-User License Agreement

IMPORTANT - READ CAREFULLY BEFORE ACCESSING WATCHGUARD SOFTWARE:

This Firebox Software End-User License Agreement ("AGREEMENT") is a legal agreement between you (either an individual or a single entity) and WatchGuard Technologies, Inc. ("WATCHGUARD") for the WATCHGUARD Firebox software product, which includes computer software components (whether installed separately on a computer workstation or on the WATCHGUARD hardware product or included on the WATCHGUARD hardware product) and may include associated media, printed materials, and on-line or electronic documentation, and any updates or modifications thereto, including those received through the WatchGuard LiveSecurity Service (or its equivalent), (the "SOFTWARE PRODUCT"). WATCHGUARD is willing to license the SOFTWARE PRODUCT to you only on the condition that you accept all of the terms contained in this Agreement. Please read this Agreement carefully. By installing or using the SOFTWARE PRODUCT you agree to be bound by the terms of this Agreement. If you do not agree to the terms of this AGREEMENT, WATCHGUARD will not license the SOFTWARE PRODUCT to you, and you will not have any rights in the SOFTWARE PRODUCT. In that case, promptly return the SOFTWARE PRODUCT, along with proof of payment, to the authorized dealer from whom you obtained the SOFTWARE PRODUCT for a full refund of the price you paid. The WATCHGUARD hardware product is subject to a separate agreement and limited hardware warranty included with the WATCHGUARD hardware product packaging and/or in the associated user documentation.

1. Ownership and License. The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. This is a license agreement and NOT an agreement for sale. All title and copyrights in and to the SOFTWARE PRODUCT (including but not limited to any images, photographs, animations, video, audio, music, text, and applets incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT are owned by WATCHGUARD or its licensors. Your rights to use the SOFTWARE PRODUCT are as specified in this AGREEMENT, and WATCHGUARD retains all rights not expressly granted to you in this AGREEMENT. Nothing in this AGREEMENT constitutes a waiver of our rights under U.S. copyright law or any other law or treaty.

2. Permitted Uses. You are granted the following rights to the SOFTWARE PRODUCT:

(A) You may install and use the SOFTWARE PRODUCT on any single WATCHGUARD hardware product at any single location and may install and use the SOFTWARE PRODUCT on multiple workstation computers.

(B) To use the SOFTWARE PRODUCT on more than one WATCHGUARD hardware product at once, you must purchase an additional copy of the SOFTWARE PRODUCT for each additional WATCHGUARD hardware product on which you want to use it. To the extent that you install copies of the SOFTWARE PRODUCT on additional WATCHGUARD hardware products in accordance with the prior sentence without installing the additional copies of the SOFTWARE PRODUCT included with such WATCHGUARD hardware products, you agree that use of any software provided with or included on the additional WATCHGUARD hardware products that does not require installation will be subject to the terms and conditions of this AGREEMENT. You must also maintain a current subscription to the WatchGuard LiveSecurity Service (or its equivalent) for each additional WATCHGUARD hardware product on which you will use a copy of an updated or modified version of the SOFTWARE PRODUCT received through the WatchGuard LiveSecurity Service (or its equivalent).

(C) In addition to the copies described in Section 2(A), you may make a single copy of the SOFTWARE PRODUCT for backup or archival purposes only.

3. Prohibited Uses. You may not, without express written permission from WATCHGUARD:

(A) Use, copy, modify, merge or transfer copies of the SOFTWARE PRODUCT or printed materials except as provided in this AGREEMENT;

(B) Use any backup or archival copy of the SOFTWARE PRODUCT (or allow someone else to use such a copy) for any purpose other than to replace the original copy in the event it is destroyed or becomes defective;

(C) Sublicense, lend, lease or rent the SOFTWARE PRODUCT;

(D) Transfer this license to another party unless

(i) the transfer is permanent,

(ii) the third party recipient agrees to the terms of this AGREEMENT, and

(iii) you do not retain any copies of the SOFTWARE PRODUCT; or

(E) Reverse engineer, disassemble or decompile the SOFTWARE PRODUCT.

4. Limited Warranty. WATCHGUARD makes the following limited warranties for a period of ninety (90) days from the date you obtained the SOFTWARE PRODUCT from WATCHGUARD or an authorized dealer:

(A) Media. The disks and documentation will be free from defects in materials and workmanship under normal use. If the disks or documentation fail to conform to this warranty, you may, as your sole and exclusive remedy, obtain a replacement free of charge if you return the defective disk or documentation to WATCHGUARD with a dated proof of purchase.

(B) SOFTWARE PRODUCT. The SOFTWARE PRODUCT will materially conform to the documentation that accompanies it. If the SOFTWARE PRODUCT fails to operate in accordance with this warranty, you may, as your sole and exclusive remedy, return all of the SOFTWARE PRODUCT and the documentation to the authorized dealer from whom you obtained it, along with a dated proof of purchase, specifying the problems, and they will provide you with a new version of the SOFTWARE PRODUCT or a full refund, at their election.

Disclaimer and Release. THE WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD, AND YOUR REMEDIES, SET FORTH IN PARAGRAPHS 4, 4(A) AND 4(B) ABOVE ARE EXCLUSIVE AND IN SUBSTITUTION FOR, AND YOU HEREBY WAIVE, DISCLAIM AND RELEASE ANY AND ALL OTHER WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD AND ITS LICENSORS AND ALL OTHER RIGHTS, CLAIMS AND REMEDIES YOU MAY HAVE AGAINST WATCHGUARD AND ITS LICENSORS, EXPRESS OR IMPLIED, ARISING BY LAW OR OTHERWISE, WITH RESPECT TO ANY NONCONFORMANCE OR DEFECT IN THE SOFTWARE PRODUCT (INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ANY IMPLIED WARRANTY ARISING FROM COURSE OF PERFORMANCE, COURSE OF DEALING, OR USAGE OF TRADE, ANY WARRANTY OF NONINFRINGEMENT, ANY WARRANTY THAT THE SOFTWARE PRODUCT WILL MEET YOUR REQUIREMENTS, ANY WARRANTY OF UNINTERRUPTED OR ERROR-FREE OPERATION, ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY IN TORT, WHETHER OR NOT ARISING FROM THE NEGLIGENCE (WHETHER ACTIVE, PASSIVE OR IMPUTED) OR FAULT OF WATCHGUARD AND ITS LICENSORS AND ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY FOR LOSS OR DAMAGE TO, OR CAUSED BY OR CONTRIBUTED TO BY, THE SOFTWARE PRODUCT).

Limitation of Liability. WATCHGUARD'S LIABILITY (WHETHER IN CONTRACT, TORT, OR OTHERWISE; AND NOTWITHSTANDING ANY FAULT, NEGLIGENCE, STRICT LIABILITY OR PRODUCT LIABILITY) WITH REGARD TO THE SOFTWARE PRODUCT WILL IN NO EVENT EXCEED THE PURCHASE PRICE PAID BY YOU FOR SUCH PRODUCT. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF AN AGREED REMEDY. IN NO EVENT WILL WATCHGUARD BE LIABLE TO YOU OR ANY THIRD PARTY, WHETHER ARISING IN CONTRACT (INCLUDING WARRANTY), TORT (INCLUDING ACTIVE, PASSIVE OR IMPUTED NEGLIGENCE AND STRICT LIABILITY AND FAULT), FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF OR IN CONNECTION WITH THIS WARRANTY OR THE USE OF OR

INABILITY TO USE THE SOFTWARE PRODUCT, EVEN IF WATCHGUARD HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF AN AGREED REMEDY.

5. United States Government Restricted Rights. The SOFTWARE PRODUCT is provided with Restricted Rights. Use, duplication or disclosure by the U.S. Government or any agency or instrumentality thereof is subject to restrictions as set forth in subdivision (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, or in subdivision (c)(1) and (2) of the Commercial Computer Software -- Restricted Rights Clause at 48 C.F.R. 52.227-19, as applicable. Manufacturer is WatchGuard Technologies, Inc., 505 5th Ave. South, Suite 500, Seattle, WA 98104.

6. Export Controls. You agree not to directly or indirectly transfer the SOFTWARE PRODUCT or documentation to any country to which such transfer would be prohibited by the U.S. Export Administration Act and the regulations issued thereunder.

7. Termination. This license and your right to use the SOFTWARE PRODUCT will automatically terminate if you fail to comply with any provisions of this AGREEMENT, destroy all copies of the SOFTWARE PRODUCT in your possession, or voluntarily return the SOFTWARE PRODUCT to WATCHGUARD. Upon termination you will destroy all copies of the SOFTWARE PRODUCT and documentation remaining in your control or possession.

8. Miscellaneous Provisions. This AGREEMENT will be governed by and construed in accordance with the substantive laws of Washington excluding the 1980 United National Convention on Contracts for the International Sale of Goods, as amended. This is the entire AGREEMENT between us relating to the SOFTWARE PRODUCT, and supersedes any prior purchase order, communications, advertising or representations concerning the SOFTWARE PRODUCT AND BY USING THE SOFTWARE PRODUCT YOU AGREE TO THESE TERMS. IF THE SOFTWARE PRODUCT IS BEING USED BY AN ENTITY, THE INDIVIDUAL INDICATING AGREEMENT TO THESE TERMS REPRESENTS AND WARRANTS THAT (A) SUCH INDIVIDUAL IS DULY AUTHORIZED TO ACCEPT THIS AGREEMENT ON BEHALF OF THE ENTITY AND TO BIND THE ENTITY TO THE TERMS OF THIS AGREEMENT; (B) THE ENTITY HAS THE FULL POWER, CORPORATE OR OTHERWISE, TO ENTER INTO THIS AGREEMENT AND PERFORM ITS OBLIGATIONS UNDER THIS AGREEMENT AND; (C) THIS AGREEMENT AND THE PERFORMANCE OF THE ENTITY'S OBLIGATIONS UNDER THIS AGREEMENT DO NOT VIOLATE ANY THIRD-PARTY AGREEMENT TO WHICH THE ENTITY IS A PARTY. No change or modification of this AGREEMENT will be valid unless it is in writing and is signed by WATCHGUARD.

Version: 040226

## Copyright, Trademark, and Patent Information



WatchGuard, the WatchGuard logo, Firebox, LiveSecurity, and any other mark listed as a trademark in the "Terms of Use" portion of the WatchGuard Web site that is used herein are either registered trademarks or trademarks of WatchGuard Technologies, Inc. and/or its subsidiaries in the United States and/or other countries. All other trademarks are the property of their respective owners.

Printed in the United States of America.



Microsoft®, Internet Explorer®, Windows® 95, Windows® 98, Windows NT®, Windows® 2000 and Windows XP are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corporation in the United States and other countries.

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

The mod_ssl package falls under the Open-Source Software label because it's distributed under a BSD-style license. The detailed license information follows.

Copyright (c) 1998-2003 Ralf S. Engelschall. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/)."

4. The names "mod_ssl" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact rse@engelschall.com.

5. Products derived from this software may not be called "mod_ssl" nor may "mod_ssl" appear in their names without prior written permission of Ralf S. Engelschall.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/)."

THIS SOFTWARE IS PROVIDED BY RALF S. ENGELSCHALL ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL RALF S. ENGELSCHALL OR HIS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY

THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The Apache Software License, Version 1.1

Copyright (c) 2000-2004 The Apache Software Foundation. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment:

"This product includes software developed by the Apache Software Foundation (http://www.apache.org/)." Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

4. The names "Apache" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.

5. Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see <http://www.apache.org/>.

Portions of this software are based upon public domain software originally written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign.

PCRE LICENSE

---

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Written by: Philip Hazel <ph10@cam.ac.uk>

University of Cambridge Computing Service,

Cambridge, England. Phone: +44 1223 334714.

Copyright (c) 1997-2003 University of Cambridge

Permission is granted to anyone to use this software for any purpose on any computer system, and to redistribute it freely, subject to the following restrictions:

1. This software is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

2. The origin of this software must not be misrepresented, either by explicit claim or by omission. In practice, this means that if you use PCRE in software that you distribute to others, commercially or otherwise, you must put a sentence like this:

Regular expression support is provided by the PCRE library package, which is open source software, written by Philip Hazel, and copyright by the University of Cambridge, England.

somewhere reasonably visible in your documentation and in any relevant files or online help data or similar. A reference to the ftp site for the source, that is, to:

ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/

should also be given in the documentation. However, this condition is not intended to apply to whole chains of software. If package A includes
PCRE, it must acknowledge it, but if package B is software that includes
package A, the condition is not imposed on package B (unless it uses
PCRE independently).

3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software.

4. If PCRE is embedded in any software that is released under the GNU General Purpose License (GPL), or Lesser General Purpose License (LGPL), then the terms of that license shall supersede any condition above with which it is incompatible.

The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

**PLEASE NOTE:** Some components of the WatchGuard WFS software incorporate source code covered under the GNU Lesser General Public License (LGPL). To obtain the source code covered under the LGPL, please contact WatchGuard Technical Support at:

877.232.3531 in the United States and Canada
+1.360.482.1083 from all other countries

This source code is free to download. There is a $35 charge to ship the CD.

This product includes software covered by the LGPL.

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it

too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, 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 and use pieces of

it in new free programs; and that you are informed that you can do these things.

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

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, 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 library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete 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 distribute a copy of this License along with the Library.

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 Library or any portion of it, thus forming a work based on the Library, 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) The modified work must itself be a software library.

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

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, 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 Library, 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 Library.

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

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you 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.

If distribution of 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 satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during

execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system rather than copying library functions into the executable, and (2) operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be 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.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library 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.

9. 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 Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library 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 with this License.

11. 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 Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library 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 Library.

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.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library 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.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser 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 Library 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 Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, 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.

PLEASE NOTE: Some components of the WatchGuard WFS software incorporate source code covered under the GNU General Public License (GPL). To obtain the source code covered under the GPL, please contact WatchGuard Technical Support at:

877.232.3531 in the United States and Canada
+1.360.482.1083 from all other countries

This source code is free to download. There is a $35 charge to ship the CD.

This product includes software covered by the GPL.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Preamble

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

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

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

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

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

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

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

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

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.

END OF TERMS AND CONDITIONS

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.

## Limited Hardware Warranty

This Limited Hardware Warranty (the "Warranty") applies to the enclosed Firebox hardware product, not including any associated software which is licensed pursuant to a separate end-user license agreement and warranty (the "Product"). BY USING THE PRODUCT, YOU (either an individual or a single entity) AGREE TO THE TERMS HEREOF. If you do not agree to these terms, please return this package, along with proof of purchase, to the authorized dealer from which you purchased it for a full refund. WatchGuard Technologies, Inc. ("WatchGuard") and you agree as set forth below or on the reverse side of this card, as applicable:

1. LIMITED WARRANTY. WatchGuard warrants that upon delivery and for one (1) year thereafter (the "Warranty Period"): (a) the Product will be free from material defects in materials and workmanship, and (b) the Product, when properly installed and used for its intended purpose and in its intended operating environment, will perform substantially in accordance with WatchGuard applicable specifications.

This warranty does not apply to any Product that has been: (i) altered, repaired or modified by any party other than WatchGuard except for the replacement or inclusion of specified components authorized in and performed in strict accordance with documentation provided by WatchGuard; or (ii) damaged or destroyed by accidents, power spikes or similar events or by any intentional, reckless or negligent acts or omissions of any party. You may have additional warranties with respect to the Product from the manufacturers of Product components. However, you agree not to look to WatchGuard for, and hereby release WatchGuard from any liability for, performance of, enforcement of, or damages or other relief on account of, any such warranties or any breach thereof.

2. REMEDIES. If any Product does not comply with the WatchGuard warranties set forth in Section 1 above, WatchGuard will, following receipt of the product you claim is defective and at its option, either (a) repair the Product, or (b) replace the Product; provided, that you will be responsible for returning the Product and for all costs of shipping and handling. Repair or replacement of the Product shall not extend the Warranty Period. Any Product, component, part or other item replaced by WatchGuard becomes the property of WatchGuard. WatchGuard shall not be responsible for return of or damage to any software, firmware, information or data contained in, stored on, or integrated with any returned Products.

3. DISCLAIMER AND RELEASE. THE WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD, AND YOUR REMEDIES, SET FORTH IN PARAGRAPHS 1 AND 2 ABOVE ARE EXCLUSIVE AND IN SUBSTITUTION FOR,

AND YOU HEREBY WAIVE, DISCLAIM AND RELEASE ANY AND ALL OTHER WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD AND ALL OTHER RIGHTS, CLAIMS AND REMEDIES YOU MAY HAVE AGAINST WATCHGUARD, EXPRESS OR IMPLIED, ARISING BY LAW OR OTHERWISE, WITH RESPECT TO ANY NONCONFORMANCE OR DEFECT IN THE PRODUCT (INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ANY IMPLIED WARRANTY ARISING FROM COURSE OF PERFORMANCE, COURSE OF DEALING, OR USAGE OF TRADE, ANY WARRANTY OF NONINFRINGEMENT, ANY WARRANTY OF UNINTERRUPTED OR ERROR-FREE OPERATION, ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY IN TORT, WHETHER OR NOT ARISING FROM THE NEGLIGENCE (WHETHER ACTIVE, PASSIVE OR IMPUTED) OR FAULT OF WATCHGUARD OR FROM PRODUCT LIABILITY, STRICT LIABILITY OR OTHER THEORY, AND ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY FOR LOSS OR DAMAGE TO, OR CAUSED BY OR CONTRIBUTED TO BY, THE PRODUCT).

4. LIMITATION AND LIABILITY. WATCHGUARD'S LIABILITY (WHETHER ARISING IN CONTRACT (INCLUDING WARRANTY), TORT (INCLUDING ACTIVE, PASSIVE OR IMPUTED NEGLIGENCE AND STRICT LIABILITY AND FAULT) OR OTHER THEORY) WITH REGARD TO ANY PRODUCT WILL IN NO EVENT EXCEED THE PURCHASE PRICE PAID BY YOU FOR SUCH PRODUCT. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF ANY AGREED REMEDY. IN NO EVENT WILL WATCHGUARD BE LIABLE TO YOU OR ANY THIRD PARTY (WHETHER ARISING IN CONTRACT (INCLUDING WARRANTY), TORT (INCLUDING ACTIVE, PASSIVE OR IMPUTED NEGLIGENCE AND STRICT LIABILITY AND FAULT) OR OTHER THEORY) FOR COST OF COVER OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOSS OF PROFITS, BUSINESS, OR DATA) ARISING OUT OF OR IN CONNECTION WITH THIS WARRANTY OR THE USE OF OR INABILITY TO USE THE PRODUCT, EVEN IF WATCHGUARD HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF ANY AGREED REMEDY.

5. MISCELLANEOUS PROVISIONS. This Warranty will be governed by the laws of the state of Washington, U.S.A., without reference to its choice of law rules. The provisions of the 1980 United Nations Convention on Contracts for the International Sales of Goods, as amended, shall not apply. You agree not to directly or indirectly transfer the Product or associated documentation to any country to which such transfer would be prohibited by the U.S. Export laws and regulations. If any provision of this Warranty is found to be invalid or unenforceable, then the remainder shall have full force and effect and the invalid provision shall be modified or partially enforced to the maximum extent permitted by law to effectuate the purpose of this Warranty. This is the entire agreement between WatchGuard and you relating to the Product, and supersedes any prior purchase order, communications, advertising or representations concerning the Product AND BY USING THE PRODUCT YOU AGREE TO THESE TERMS. IF THE PRODUCT IS BEING USED BY AN ENTITY, THE INDIVIDUAL INDICATING AGREEMENT TO THESE TERMS BY USING THE PRODUCT REPRESENTS AND WARRANTS THAT (A) SUCH INDIVIDUAL IS DULY AUTHORIZED TO ACCEPT THE WARRANTY ON BEHALF OF THE ENTITY AND TO BIND THE ENTITY TO THE TERMS OF THIS WARRANTY; (B) THE ENTITY HAS THE FULL POWER, CORPORATE OR OTHERWISE, TO ENTER INTO THE WARRANTY AND PERFORM ITS OBLIGATIONS UNDER THE WARRANTY AND; (C) THE WARRANTY AND THE PERFORMANCE OF THE ENTITY'S OBLIGATIONS UNDER THE WARRANTY DO NOT VIOLATE ANY THIRD-PARTY AGREEMENT TO WHICH THE ENTITY IS A PARTY. No change or modification of the Warranty will be valid unless it is in writing and is signed by WatchGuard.

Firmware Version: 7.0
Part Number: 1776-0000
Guide Version: 7.0-3

## Abbreviations Used in this Guide

| | |
|---|---|
| 3DES | Triple Data Encryption Standard |
| BOVPN | Branch Office Virtual Private Network |
| DES | Data Encryption Standard |
| DNS | Domain Name Service |
| DHCP | Dynamic Host Configurationl Protocol |
| DSL | Digital Subscriber Line |
| IP | Internet Protocol |
| IPSec | Internet Protocol Security |
| ISDN | Integrated Services Digital Network |
| ISP | Internet Service Provider |
| MAC | Media Access Control |
| MUVPN | Mobile User Virtual Private Network |
| NAT | Network Address Translation |
| PPP | Point-to-Point Protocol |
| PPPoE | Point-to-Point Protocol over Ethernet |
| TCP | Transfer Control Protocol |
| UDP | User Datagram Protocol |
| URL | Universal Resource Locator |
| VPN | Virtual Private Network |
| WAN | Wide Area Network |
| WSEP | WatchGuard Security Event Processor |

# Contents

CHAPTER 1

# Introduction to Network Security

Congratulations on your purchase of the WatchGuard Firebox® X Edge. Your new security device provides peace of mind when countering today's network security threats.

To provide context for the many features described throughout this user guide, this chapter explains basic concepts of networking and network security.

## Network Security

Although the Internet puts a tremendous volume of information at your fingertips, it also presents risks by exposing your network to attackers. Network security is the process of preventing and detecting unauthorized use of your computer or network. Prevention measures help you to stop intruders from accessing any part of your computer system.

Although you may not consider anything on your computer "top secret," you should still be very concerned about security. If you aren't careful, intruders can take malicious actions such as use your computer to attack other computer systems, send forged e-mail from your computer, or steal your financial information. They can also damage your computer by reformatting your hard drive or changing your data.

Computer security must always be kept up-to-date. Intruders are always discovering new vulnerabilities to exploit in computer software.

## About Networks

A network is a connected group of computers and other devices. It can consist of anything from two computers connected by a serial cable to thousands of computers connected by high-speed data communication links located throughout the world.

A *Local Area Network* (LAN) is a group of computers linked electronically to form a common work environment. This facilitates the sharing of applications and data, and is especially important when a group of people need to work together on one project.

A *Wide Area Network* (WAN) involves computers separated by significant distances, such as those located in different buildings.

### Clients and servers

The terms *client* and *server* are used to describe individual computers that are part of a network. A server is a computer that makes its resources available to the network and responds to the commands of a client. Examples of a server's shared resources are files (a file server), printers (a print server), and processing power (an application server). A client is a computer that uses the resources made available by the server.

## Connecting to the Internet

You have a number of options for connecting to the Internet. High-speed Internet connections, such as cable modem or Digital Subscriber Line (DSL), are referred to as broadband connections. *Bandwidth* describes the relative speed of an Internet connection, such as 1 Megabit per second (Mbps).

You can use a cable modem to connect to the Internet via the cable TV network. The cable modem usually has an Ethernet LAN connection to the computer, and it is capable of speeds in excess of 5 Mbps.

Typical speeds tend to be lower than the maximum, however, because cable providers turn entire neighborhoods into LANs that

share the same bandwidth. Because of this "shared-medium" topology, cable modem users might experience somewhat slower network access during periods of peak demand, and can be more susceptible to certain types of attacks more than users with other types of connectivity.

Digital Subscriber Line (DSL) Internet connectivity, unlike cable modem-based service, provides the user with dedicated bandwidth. However, the maximum bandwidth available to DSL users is usually lower than the maximum cable modem rate because of differences in their respective network technologies. Also, the "dedicated bandwidth" is dedicated only between your home or office and the DSL provider's central office. The provider offers little or no guarantee of bandwidth across the Internet.

*Internet Service Providers* (ISP) are companies that provide access to the Internet.

## Protocols

You will often hear the term protocol. A *protocol* is a specification that allows computers to communicate across a network. In a way, protocols define the grammar that computers use to communicate with each other.

The standard protocol whenever you connect to the Internet is called Internet Protocol (IP). This protocol can be thought of as the common language of computers on the Internet.

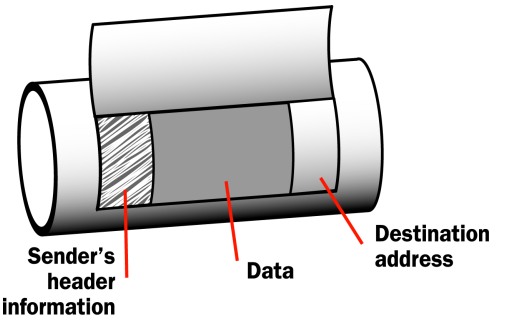
A protocol also defines how data is assembled and transmitted through a network. The most frequently used protocols are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). Other IP protocols are less commonly used.

TCP/IP is the basic protocol used by computers connected to the Internet. TCP/IP involves certain settings that you need to know when setting up your Firebox X Edge. For more information on TCP/IP, see "Learning your TCP/IP properties" on page 13.

## How Information Travels on the Internet

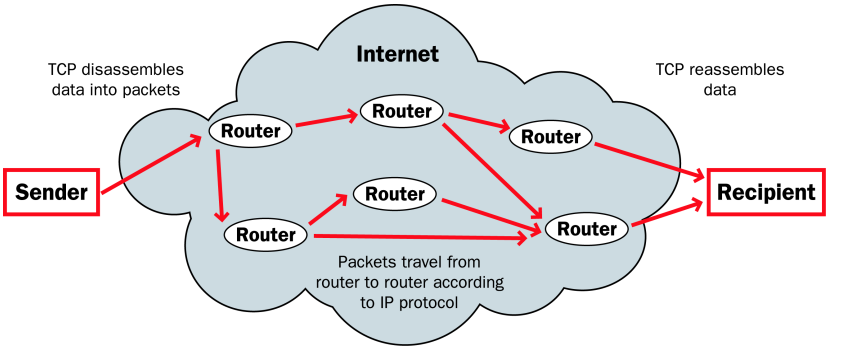
The data that is sent through the Internet is divided into units called packets. When you send a file from one place to another on the

Internet, the file is divided into chunks of data. Each chunk, or packet, 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. To make sure that the packets are received at the destination, information is added to the packets.




Data packet

The TCP and IP protocols are used for sending and receiving these packets. TCP disassembles and reassembles the data; for example, data that may consist of an e-mail message or a program file. IP adds information to the packets that includes the destination and the handling requirements.




Packets traveling on the Internet

# IP Addresses

IP addresses are like street addresses—when you want to send some information to someone, you must first know his or her address. Similarly, when a computer connected to the Internet needs to send data to another computer, it must first know its IP address.

Each computer on the Internet has its own unique IP address. An IP address consists of four sets of numbers separated by decimal points. Examples of IP addresses are:

- 192.168.0.11
- 10.1.20.18
- 208.15.15.15

A firewall device such as the Firebox® X Edge is also a computer and therefore has its own IP address.

## Network addressing

Your ISP assigns IP addresses, which are a requirement to connect to the Internet. The assignment of IP addresses is *dynamic* or *static*.

Static IP addressing occurs when an ISP permanently assigns one or more IP addresses for each user. These addresses do not change over time. However, if a static address is assigned but not in use, it is effectively wasted. Because ISPs have a limited number of addresses allocated to them, they sometimes need to make more efficient use of their addresses.

Dynamic IP addressing allows the ISP to use their address space more efficiently. Using dynamic IP addressing, the IP addresses of individual user computers may change over time. If a dynamic address is not in use (the user is not connected to the network), it can be automatically reassigned to another computer as needed.

Your ISP can tell you how their system assigns IP addresses.

## About DHCP

Most ISPs make dynamic IP address assignments through (Dynamic Host Configuration Protocol (DHCP). When a computer connects to the network, a DHCP server at the ISP assigns that computer an IP address. The manual assignment of IP addresses is not necessary when using DHCP.

### About PPPoE

Some ISPs assign the IP addresses through Point-to-Point Protocol over Ethernet (PPPoE). PPPoE emulates a standard dial-up connection to provide some of the features of Ethernet and PPP. This system allows the ISP to use the billing, authentication, and security systems designed for dial-up, DSL modem, and cable modem service.

## Domain Name Service (DNS)

If you don't know a person's street address, you can look it up in the telephone directory. On the Internet, the equivalent to a telephone directory is the Domain Name Service, or DNS. You probably use DNS all the time without knowing it. Whenever you use a ".com" address such as www.mysite.com (which is actually the site's *domain name*) to visit an Internet site, you are using DNS. When you type the .com address into your Internet browser (such as Internet Explorer or Netscape), your computer asks its DNS server for the actual IP address of the site.

A URL (Uniform Resource Locator) identifies each IP address on the Internet. An example of a URL is:

http://www.watchguard.com/

## Services

As the name implies, a service provides some kind of useful function for you on the computer, such as exchanging e-mail or transferring files from one computer to another through the network. These services are based on specific protocols. Commonly used Internet services are:

- World Wide Web access uses Hypertext Transfer Protocol (HTTP)
- E-mail uses Simple Mail Transfer Protocol (SMTP)
- File transfer uses File Transfer Protocol (FTP)
- Resolving a domain name into an Internet address uses Domain Name Service (DNS)
- Remote terminal access uses Telnet or Secure Shell

Although some services are essential, they can also be a security risk. To send and receive data, you must “open a door” in your computer, which makes your network vulnerable. One of the most common ways networks are broken into is by intruders exploiting services.

## Ports

On computers and other telecommunication devices, a port is a specific place for physically connecting another device, usually with a socket and plug. A computer usually has one or more serial ports and one parallel port. The serial port supports sequential, one bit-at-a-time transmission to devices such as scanners, and the parallel port supports multiple-bit-at-a-time transmission to devices such as printers.

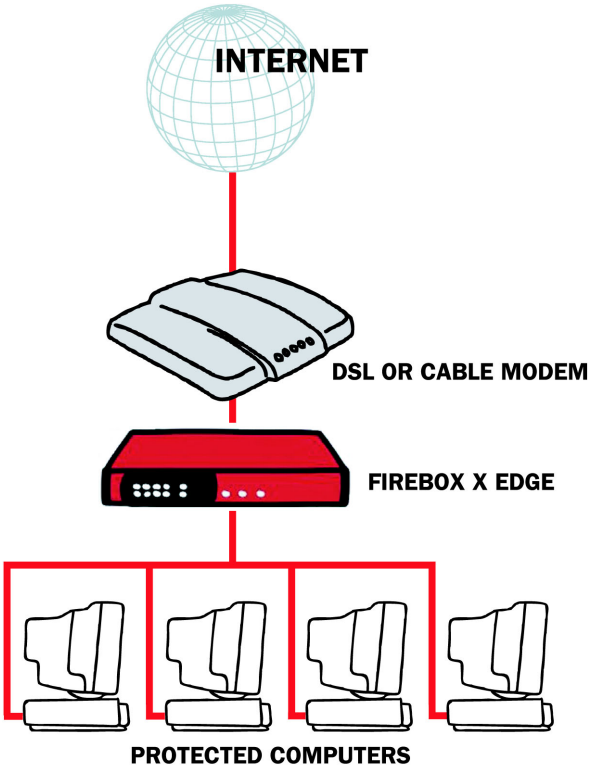
Computers also have ports that are not physical locations. These ports are “logical connection places” for programs or applications on a computer in a network. Some applications, such as HTTP, have ports with preassigned numbers. These are known as “well-known ports.” Other application processes are assigned port numbers dynamically for each connection. When a service is initially started, it is said to “bind” to its designated port number.

Every Internet service using TCP is identified by a unique port number. When a client initiates a connection to a server, it chooses to connect to, say, port 25 on the remote machine. Port 25 is assigned to the SMTP protocol which is the service of delivering electronic mail.

Most services are assigned a port number in the range from 0 to 1024, but the valid port numbers range from 0 to 65535.

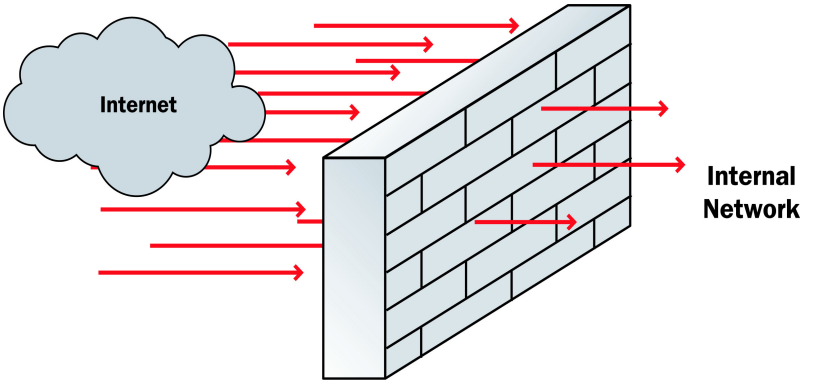
## Firewalls

A *firewall* divides your internal network from the Internet to reduce this danger. The computers on the "trusted" (internal) side of a firewall are protected. The illustration below shows how a firewall physically divides the trusted network (your computers) from the Internet.




Firewalls allow the user to define access policies for the Internet traffic going to the computers they are protecting. Many also provide the ability to control what services or ports the protected computers are able to access on the Internet (outbound access). Most firewalls intended for home use come with pre-configured security policies from which the user chooses, and some—such as the Firebox X Edge—allow the user to customize these policies for their specific

needs.




Firewalls are implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

## Firebox® X Edge and Your Network

The Firebox® X Edge controls all traffic between the external network (the Internet) and the trusted network. The Firebox also supports an optional network to extend the protection of the firewall to include telecommuters on a separate network. All suspicious traffic is stopped. The rules and policies that identify the suspicious traffic are described in Chapter 5, “Configuring Firewall Settings.”

Designed for small and remote offices with modest in-house security expertise, the Firebox X Edge is a high-performance security device that simply plugs in between your cable, DSL, or ISDN router and your network.

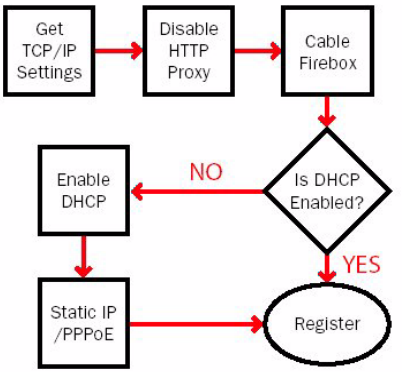
The Web-based user interface of the Firebox X Edge intuitive and straight-forward. You don’t need additional security expertise to install and manage your firewall. Because you can manage your network securely from anywhere, at any time, you have more time and resources to focus on your business.

CHAPTER 2

# Installing the Firebox® X Edge

To install the WatchGuard® Firebox® X Edge in your network, use this procedure:

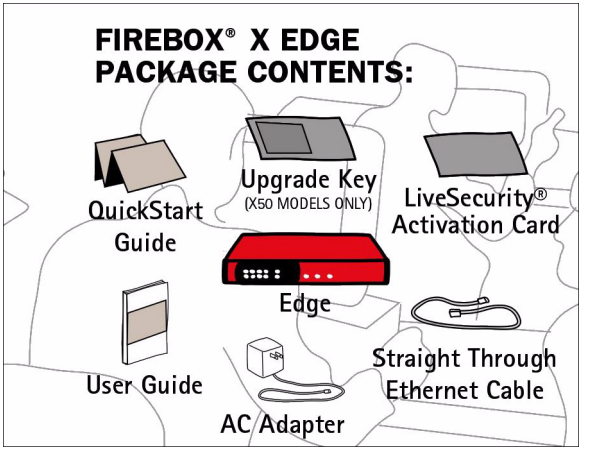
- Identify and record the TCP/IP properties for your Internet connection.
- Disable the HTTP proxy property of your Web browser.
- Connect the Firebox X Edge to your network.
- Enable DHCP on your computer.
- Activate the LiveSecurity® Service.



## Package Contents

Make sure that the Firebox® X Edge package includes:

- The Firebox X Edge *QuickStart Guide* - read the *Firebox X Edge QuickStart Guide* for a summary of the procedures in this chapter.
- A LiveSecurity® Service activation card - use this card to activate LiveSecurity Service.
- A Hardware Warranty Card - use this card to read your hardware warranty.
- An AC adapter (12 V) - use this adapter to connect the Firebox to a power source.
- One Ethernet cable - use this cable to connect your Firebox to your computer.




## Installation Requirements

Other installation requirements are:

- A computer with an Ethernet network interface card.
- A Web browser, for example Netscape or Microsoft Internet Explorer. Netscape 7.0 or later is required. Internet Explorer 6.0 or later is required.

- The Firebox X Edge serial number. Find this number on the bottom of the Firebox.
  You use the serial number to register the Firebox.
- An Internet connection.
  The Internet connection can be a cable or DSL modem, an ISDN router, or a direct LAN connection.

# Identifying Your Network Settings

An Internet Service Provider (ISP) gives computers an Internet Protocol (IP) address. An ISP can give you a static or dynamic IP address. A static address is an address that does not change. A dynamic address is an address that can change each time you connect to the Internet.

Your ISP gives you an IP address in one of three ways:

- Static: Web servers, FTP sites, and other Internet resources with addresses that cannot change get static IP addresses.
- DHCP: ISPs use the Dynamic Host Configuration Protocol (DHCP) to give dynamic IP addresses to computers. Each time you connect to the ISP, a DHCP server can give you a different IP address.
- PPPoE: ISPs use Point-to-Point Protocol over Ethernet (PPPoE) to give dynamic and static IP addresses to computers. A user name and passphrase are necessary for PPPoE.

An ISP can also give computers a network mask (netmask). A netmask is a series of bits that "mask" certain portions of an IP address. This is used to divide an organization's network into smaller units, creating additional destinations for routing purposes.

Read your DSL or cable modem instructions or call your ISP to learn which type of IP address you have.

## Learning your TCP/IP properties

Transmission Control Protocol/Internet Protocol (TCP/IP) is the primary protocol computers use to connect to the Internet. Make sure that your computer is connected to your ISP and you can browse Web pages on the Internet.

**NOTE**

If your ISP gives your computer an IP address of 10.0.0.0/8 or one that starts with 192.168 or 172.16 to 172.31, then your ISP uses

network address translation (NAT). You must get a public IP address and disable NAT on your intranet router for full functionality. Get instructions from your ISP.

### Your TCP/IP Properties Table

| TCP/IP Property | | Value |
|---|---|---|
| IP Address | | . . . |
| Subnet Mask | | . . . |
| Default Gateway | | . . . |
| DHCP Enabled | | Yes No |
| DNS Server(s) | Primary | . . . |
| | Secondary | . . . |

To find your TCP/IP properties, follow the instructions for your computer operating system.

### Microsoft Windows 2000 and Windows XP

1 Click **Start** ⇒ **Programs** ⇒ **Accessories** ⇒ **Command Prompt**.

2 At the MS-DOS prompt, type `ipconfig /all` and then press the **Enter** key.

3 Record the values in the Your TCP/IP Properties Table on page 14.

4 Close the window.

### Microsoft Windows NT

1 Click **Start** ⇒ **Programs** ⇒ **Command Prompt**.

2 At the MS-DOS prompt, type `ipconfig /all`. Press the **Enter** key.

3 Record the values in the Your TCP/IP Properties Table on page 14.

4 Close the window.

### Microsoft Windows 98 or ME

1 Click **Start** ⇒ **Run**.

2 At the MS-DOS prompt, type `winipcfg` and then press the **Enter** key.

3 Click **OK**.

4 Select the **Ethernet Adapter**.

5 Record the values in the Your TCP/IP Properties Table on page 14.

6 Click **Cancel**.

### Macintosh

1 Click the **Apple** menu ⇒ **Control Panels** ⇒ **TCP/IP**.

2 Record the values in the Your TCP/IP Properties Table on page 14.

3 Close the window.

### Other operating systems (Unix, Linux)

1 Read your operating system guide to locate the TCP/IP settings.

2 Record the values in the Your TCP/IP Properties Table on page 14.

3 Exit the TCP/IP configuration screen.

## Disabling the HTTP Proxy Setting

A proxy is a computer process that receives and acts on data on behalf of a server, to which the proxy then relays the data. By acting in place of the server, the proxy protects the server from direct contact with the Internet.

The HTTP Proxy used by many Web browsers handles Internet traffic. If the HTTP proxy setting is enabled, you can use the browser to view Web pages on the Internet. However, your browser won't work for pages in other locations. Because setting up the Firebox® X Edge requires that you use your browser to view special pages stored on the device, you must temporarily disable the HTTP proxy feature.

The following instructions tell you how to disable the HTTP proxy in two common browser types. If you are using different browser, use the Help menus of the browser application to find the necessary

information. Many opensource browsers automatically disable the HTTP proxy feature by default.

### Netscape

1 Open Netscape.

2 Click **Edit ⇒ Preferences.**
The Preferences window appears.

3 There is a list of options at the left side of the window. Click the arrow symbol to the left of the **Advanced** heading to expand the list.

4 Click **Proxies**.

5 Make sure the **Direct Connection to the Internet** option is selected.

6 Click **OK**.

### Internet Explorer

1 Open Internet Explorer.

2 Click **Tools ⇒ Internet Options**.
The Internet Options window appears.

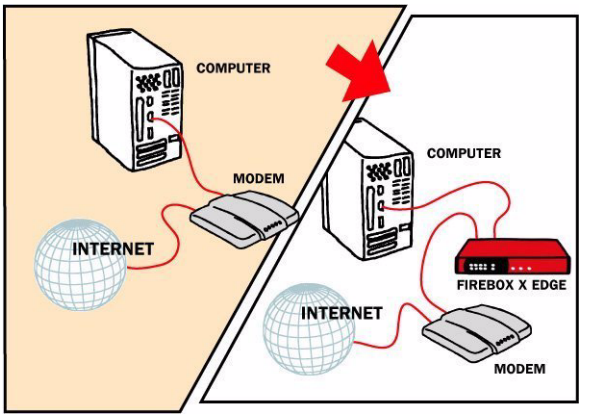
3 Click the **Advanced** tab.

4 Scroll down the page to **HTTP 1.1 Settings**.

5 Clear all of the checkboxes.

6 Click **OK**.

# Connecting the Firebox X Edge

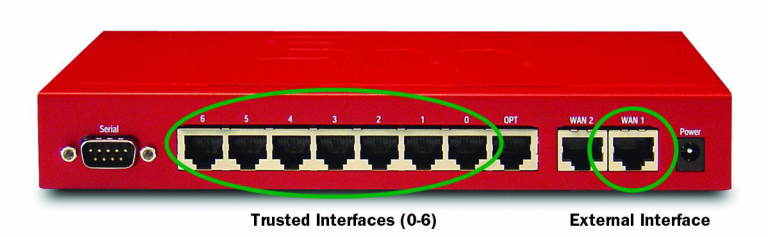



Use this procedure to connect your Firebox® X Edge Ethernet and power cables:

1 Shut down your computer.

2 If you use a DSL or cable modem to connect to the Internet, disconnect its power supply.

3 Find the Ethernet cable between the modem and your computer. Disconnect this cable from your computer and connect it to the Firebox external interface (WAN 1).




4 Find the Ethernet cable supplied with your Firebox. Connect this cable to a trusted interface (0-6) on the Firebox. Connect the other end of this cable to the Ethernet interface of your computer.

5 If you use a DSL or cable modem, connect its power supply.

6 Find the AC adapter supplied with your Firebox. Connect the AC adapter to the Firebox and to a power source.
The Firebox power indicator light comes on and the external interface indicator lights flash and then come on. The Firebox is ready.

**NOTE**

Use only the AC adapter supplied with the Firebox X Edge.

7 When the Firebox is ready, start your computer.

## Cabling the Firebox X Edge for more than seven devices

Although the Firebox X Edge has only seven numbered Ethernet ports (labeled 0-6), you can connect more than seven devices. Use one or more network hubs to make more connections.

The maximum number of devices that can connect to the Internet at the same time is set by model. For example, the Firebox X5 has a 5-session license. There can be more than five devices on the trusted network, but the Firebox allows only five Internet connections at the same time.

A Firebox uses a session when it makes a connection between a computer on the trusted interface and a computer on the external interface. The Firebox releases the session when:

- the session reaches the idle timeout limit;
- the session reaches the maximum time limit;
- the Firebox administrator uses the Firebox Users page to end the session;
- the user ends the session by closing all browser windows; or
- the Firebox restarts.

For more information, see the FAQ:

https://www.watchguard.com/support/AdvancedFaqs/sogen_seatlimit.asp

License upgrades are available from your reseller or from the WatchGuard Web site:

http://www.watchguard.com/sales/buyonline.asp

To connect more than seven devices to the Firebox, you need:

- An Ethernet 10/100Base TX hub or switch
- A straight-through Ethernet cable, with RJ-45 connectors, for each computer

- A straight-through Ethernet cable to connect each hub to the Firebox X Edge.

To connect more than seven devices to the Firebox X Edge:

1 Shut down your computer. If you connect to the Internet through a DSL modem or cable modem, disconnect the power supply from this device.

2 Disconnect the Ethernet cable that runs from your DSL modem, cable modem, or other Internet connection to your computer. Connect the Ethernet cable to the WAN port on the Firebox X Edge.
The Firebox X Edge is connected directly to the modem or other Internet connection.

3 Connect one end of the straight-through Ethernet cable supplied with your Firebox X Edge to one of the seven numbered Ethernet ports (labeled 0-6) on the Firebox X Edge. Connect the other end to the uplink port of the Ethernet hub or switch.
The Firebox X Edge is connected to the Internet and your Ethernet hub or switch.

4 Connect an Ethernet cable between each of the computers and an uplink port on the Ethernet hub, and make sure the link lights are lit on both devices when powered back on.

5 If you connect to the Internet through a DSL modem or cable modem, reconnect the power supply to this device. The indicator lights flash and then stop. The modem is ready for use.

6 Attach the AC adapter to the Firebox X Edge. Connect the AC adapter to a power supply.

7 Restart your computer.

## Connecting to the System Configuration Pages

Use a Web browser to connect to the Firebox® X Edge system configuration pages. The first time you connect to the Firebox configuration pages, the End User License Agreement appears. To continue, you must accept the agreement. You must also set the administrator password.

A factory default Firebox allows HTTP traffic on port 80. After you set the administrator password, the Firebox uses only secure HTTP (HTTPS) on port 443 for system configuration.

For your computer to connect to the Firebox, you must choose one of these options:

- Get a dynamic IP address from the Firebox using DCHP
- Set a static IP address within the default trusted interface address range
  The default trusted interface IP address is 192.168.111.1/24.

For more information on network addressing, see "IP Addresses" on page 5.

## Setting your computer to use DHCP

This procedure sets a computer with the Windows XP operating system to use DHCP. If your computer does not use Windows XP, read the documentation for instructions to set your computer to use DHCP.

1. Click **Start** ⇒ **Control Panel**.
   The Control Panel window appears.
2. Double-click the **Network Connections** icon.
3. Double-click the **Local Area Connection i**con.
4. Double-click the **Internet Protocol (TCP/IP)** item.
   The Internet Protocol (TCP/IP) Properties dialog box appears.
5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** options.
6. Click **OK** to close the **Internet Protocol (TCP/IP) Properties** dialog box.
7. Click **OK** to close the **Local Area Network Connection Properties** dialog box. Close the **Network Connections** and **Control Panel** windows.
   Your computer is now connected to the Firebox X Edge.

## Setting your computer with a static IP address

This procedure sets a computer with the Windows XP operating system to a static IP address. If your computer does not use Windows XP, read the documentation for instructions to set your computer to

use DHCP. You must use an IP address on the same network as the Firebox X Edge trusted interface.

1 Click **Start ⇒ Control Panel**.
The Control Panel window appears.

2 Double-click the **Network Connections** icon.

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

4 Double-click the **Internet Protocol (TCP/IP)** item.
The Internet Protocol (TCP/IP) Properties dialog box appears.

5 Select the **Use the following IP address** option.

6 In the IP address field, type an IP address on the same network as the Firebox trusted interface. We recommend 192.168.111.2.
The default trusted interface network is 192.168.111.0/24. The last number can be between 2 and 254.

7 In the **Subnet Mask** field, type `255.255.255.0`.

8 In the **Default Gateway** field, type the IP address of the Firebox trusted interface.
The default Firebox trusted interface address is 192.168.111.1.

9 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** dialog box.

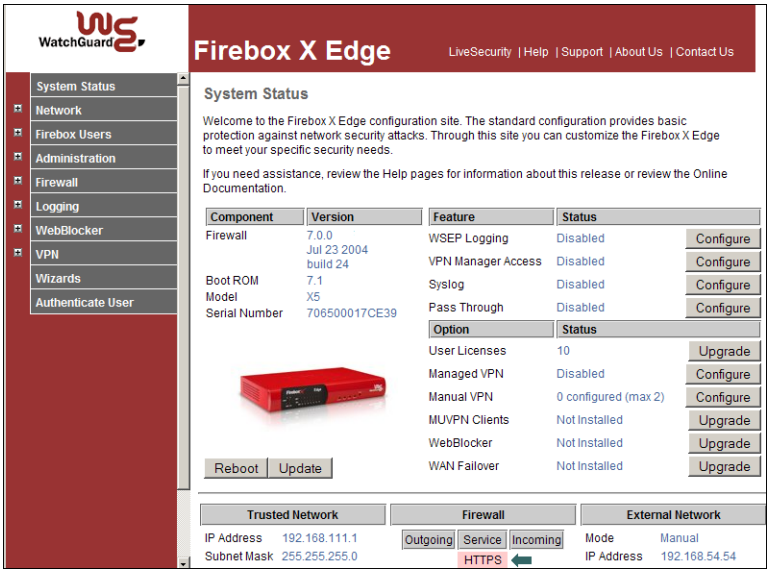
10 Click **OK** to close the **Local Area Network Connection Properties** dialog box. Close the **Network Connections** and **Control Panel** windows.
Your computer is now connected to the Firebox X Edge.

## Browsing to the System Status page

Use a Web browser to connect to the Firebox and change network settings.

1 Open your Web browser.
If this is the first connection to the Firebox, the End User License Agreements appears. You must accept the agreement and set your administrator password to continue. See

2 In the Address bar, type the Firebox trusted interface IP address which is **https://192.168.111.1** for a new Firebox. Press the **Enter** key.




# Configuring the External Interface

Your Internet Service Provider (ISP) uses DHCP, PPPoE, or static IP addressing to identify your computer on their network. After you connect the Firebox, you must configure the external interface with the information from your ISP.

## Setting the Firebox to use DHCP

A new Firebox uses DHCP to get an IP address for the external interface. If your ISP uses DHCP addressing to identify your computer on their network, you do not need to make a configuration change unless the ISP gives you a DHCP ID or name. If necessary, use this procedure to set the DHCP ID or name:

1 Open your Web browser. Browse to the System Status page at https://192.168.111.1.
Type the URL in the Address bar of your browser and press the [Enter] key.

2 From the navigation bar on the left side, click the **+** symbol to the left of **Network**. Click **External**.

3 Use the **Configuration mode** drop-down list to select **DHCP.**

4 In the DHCP ID field, type the DHCP name or ID you got from your ISP.

5 Click **Submit**.

## Setting a Static IP Address

If your ISP uses static IP addressing, you must set the Firebox external interface address. Use the information in the Your TCP/IP Properties Table on page 14 to do this procedure.

1 Open your Web browser. Browse to the System Status page at https://192.168.111.1.
Type the URL in the Address bar of your browser and press the [Enter] key.

2 From the navigation bar on the left side, click the **+** symbol to the left of **Network**. Click **External**.

3 Use the **Configuration mode** drop-down list to select **Manual Configuration**.

4 Type the IP address, subnet mask, and default gateway.

5 Type the IP addresses of the primary and secondary DNS servers.

6 Type the DNS domain suffix.

7 Click **Submit**.

## Entering PPPoE settings

Point to Point Protocol over Ethernet (PPPoE) is another method commonly used by service providers as it integrates well with traditional dial-up infrastructure. If your service provider assigns IP addresses through PPPoE, you need to gather additional information to set up your Firebox.

*PPPoE Address Settings*

| PPPoE Setting | Value |
|---|---|
| Login Name | |
| Domain | |
| Password | |

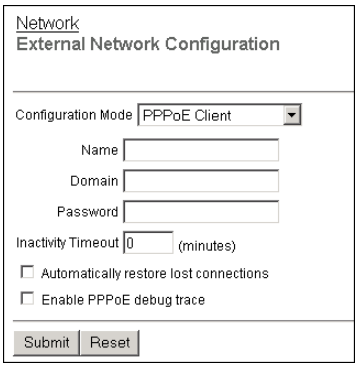
For more information in PPPoE, see “About PPPoE” on page 6. To configure the Firebox for PPPoE:

1 Open your Web browser and click **Stop**.
Because the Internet connection is not configured, the browser cannot load your home page from the Internet. The browser can only open the configuration pages stored on the Firebox.

2 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
The default IP address is: https://192.168.111.1

3 From the navigation bar at left, select **Network** ⇒ **External**.
The External Network Configuration page opens.

4 From the **Configuration Mode** drop-down list, select **PPPoE Client**.



5 Type the PPPoE login name and domain as well as the PPPoE password supplied by your service provide in the applicable fields.

6 Type the time delay before inactive TCP connections are disconnected.

7 If appropriate, select the **Automatically restore lost connections** checkbox.

This option keeps a constant flow of traffic between the Firebox and the PPPoE server. This allows the Firebox to keep the PPPoE connection open during a period of frequent packet loss. If the flow of traffic stops, the Firebox reboots. A reboot frequently restores the connection. The ISP sees this constant flow of traffic as a continuous connection. The regulations and billing policy of the ISP determine whether you can use this option.

8 Select the **Enable PPPoE debug trace** checkbox to activate PPPoE debug trace.

This can assist WatchGuard Technical Support in troubleshooting PPPoE problems.

9 Click **Submit**.

## Registering Your Firebox and Activating LiveSecurity Service

Assuming you have installed the Firebox® X Edge, you can now register the Firebox and activate your LiveSecurity® Service subscription. LiveSecurity Service provides threat alert notifications, security advice, free virus protection, software updates, technical support by Web or telephone, and access to online help resources and the WatchGuard user forum.

A subscription to the LiveSecurity Service is required to get the license keys for the upgrades that you purchase. To apply upgrades, you must log into LiveSecurity Service and enter your upgrade key. You are then given a *feature key* to activate features on your Firebox X Edge.

You must have the serial number of your Firebox X Edge to register. The Firebox serial number is located on the bottom of the appliance. Record the serial number in the table below:

1 Register your Firebox X Edge with the LiveSecurity Service at the WatchGuard Web site:

http://www.watchguard.com/activate

**NOTE**

To activate the LiveSecurity Service, your browser must have JavaScript enabled.

2 If you have a user profile on the WatchGuard Web site, enter your user name and password. If you have not registered before, you must create a user profile. To do this, follow the instructions on the Web site.

3 Record your LiveSecurity Service user profile information in the table below. Keep this information confidential.

*WatchGuard User Profile*

| | |
|---|---|
| User name: | |
| Password: | |
| Serial Number: | |

4 If a model upgrade key is included with your model, activate it by going to:
http://www.watchguard.com/upgrade

5 Select your product and follow the instructions for product activation.

CHAPTER 3

# Configuration and Management Basics

*Configuration* is the process of customizing the WatchGuard® Firebox® X Edge to meet the specific security needs of your organization. This is your main task after installing your Firebox. The configuration of the Firebox X Edge is made using Web pages stored on the Firebox. You can connect to these configuration pages with your Web browser.

In conjunction with configuring the Firebox, you can also use the Firebox's Web pages to manage your network and view its current configuration.

This chapter introduces the Firebox X Edge Web pages and describes, in general, how to use them. Detailed instructions on configuring and managing the Firebox X Edge are provided throughout this guide and are cross-referenced in this chapter.

## Navigating the Configuration Pages

To configure your Firebox® X Edge, you must use a Web browser such as Internet Explorer, Mozilla Firefox, or NetScape Navigator. The HTTP Proxy feature must be disabled. For more information, see "Disabling the HTTP Proxy Setting" on page 15.

In this User Guide, every procedure starts with a step to:

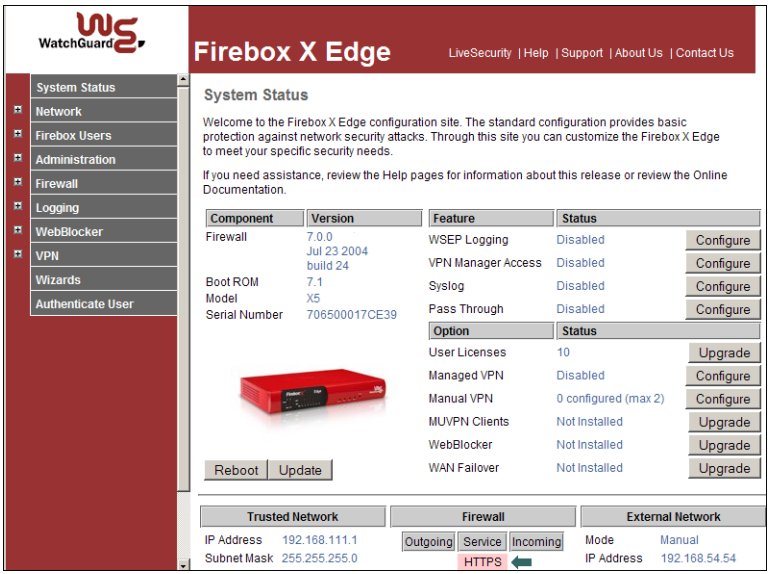
"Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge. The default IP address is https://192.168.111.1."

The purpose of the step is to open your Firebox system configuration pages. Your computer must be connected to the Firebox with an Ethernet cable. You can change the IP address of the trusted network from https://192.168.111.1 to an IP address of your choice. For more information, see "Configuring the Trusted Network" on page 48.

For example, if you are using Internet Explorer to configure your Firebox:

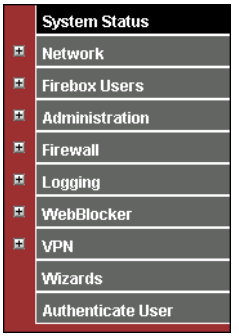
1 Start Internet Explorer.

2 Click **File** ⇒ **Open**, type **https://192.168.111.1** in the text box next to the word **Open**, and then click **OK**.
You can also type the URL directly into the Address bar and press the Enter key.



## Using the navigation bar

On the left side of the System Status page is a navigation bar that provides access to other Firebox X Edge configuration and status pages.




To view the main page for each area, click the appropriate menu item on the navigation bar. For example, to view how logging is currently configured for your Firebox and to see the current event log, click **Logging**.

Each area contains submenus that you use to configure various settings within that area. To access these submenus, click the plus sign (+) to the left of the area. For example, if you click the plus sign next to WebBlocker, the following submenu items appear: Settings, Profiles, Allowed Sites, Denied Sites, and Trusted Hosts.

In this guide, clicking and expanding menus is represented with a series of arrow (⇒) symbols. The menu names are in **bold**. In this example, to open the Denied Sites page, the command would appear in the text as **WebBlocker ⇒ Denied Sites.**

## Logging in for the first time

The first time you log into your Firebox X Edge, no administrative password is set. To connect to the Firebox before it has a password:

1 Start your Internet browser.

2 Click **File ⇒ Open**, type **https://192.168.111.1** in the text box next to the word **Open**, and then click **OK**.

3 The End User License Agreement (EULA) appears. Read through it, and if you agree, indicate that you accept the EULA.

4 Type and confirm your administrative password.

# Configuration Overview

The Firebox X Edge system configuration pages are grouped by functional task. The following provides a brief introduction to each category and directs you to chapters in this User Guide providing detailed information about each feature.

## Firebox System Status Page

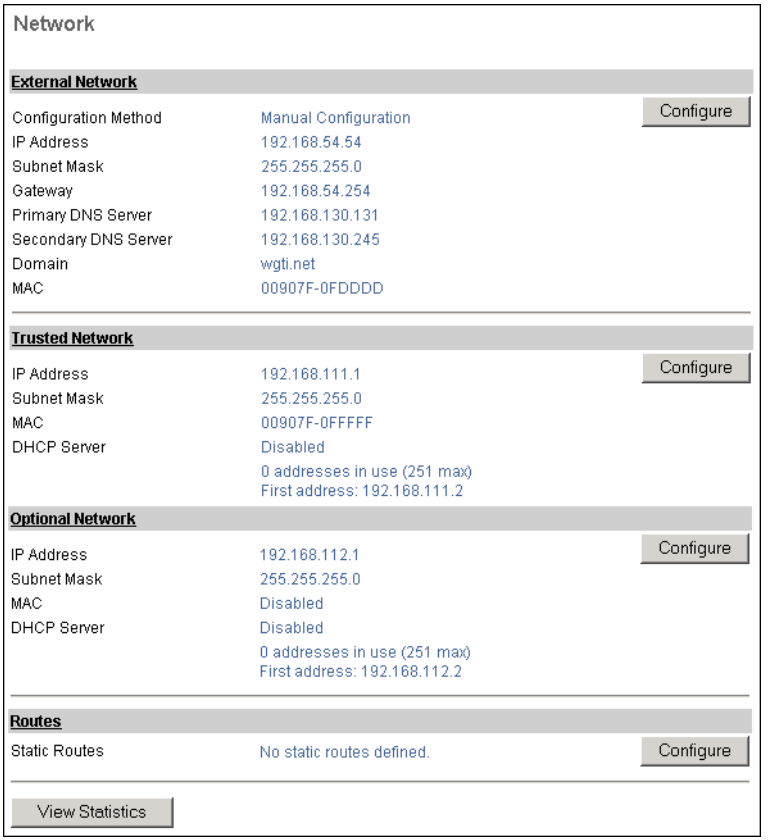
The System Status page is the main configuration page of the Firebox X Edge. The center panel of the page shows information about the current settings. It also contains buttons so you can change these settings. Each setting and display is explained in detail later in this guide.

To summarize, the information on this page includes the following:

- Firebox components and their current versions
- The serial number of the device
- The status of key Firebox X Edge features
- The status of upgrade options
- Network configuration information
- Firewall configuration information
- A button to reboot the Firebox

## Network Page

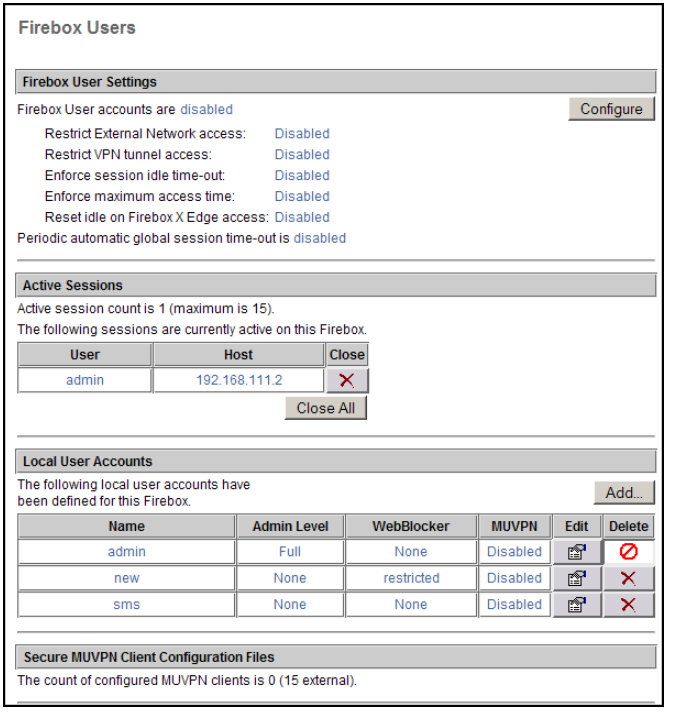
The Network page shows the configuration of each network interface. It also shows any configured routes and provides buttons to change configurations and to view network statistics. For more information, see Chapter 4, “Changing Your Network Settings.”



## Firebox Users Page

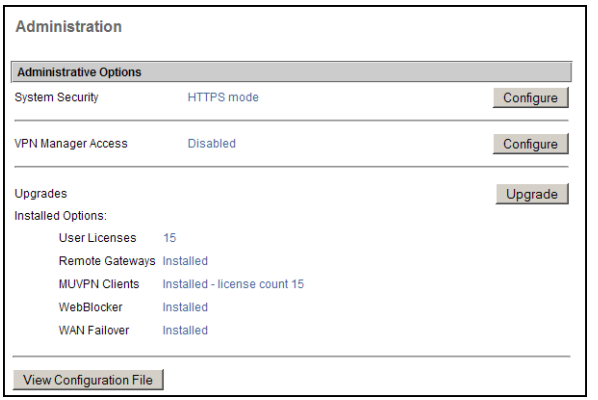
The Firebox Users page shows statistics on the active sessions and defined local user accounts. It provides buttons to close current sessions and to add, edit, and delete user accounts.

This page also shows the MUVPN client configuration files that are available for download. If your Firebox does not yet support MUVPN clients, the page provides a button for you to upgrade your Firebox to enable MUVPN client support. For more information, see Chapter 10, “Managing the Firebox X Edge.”



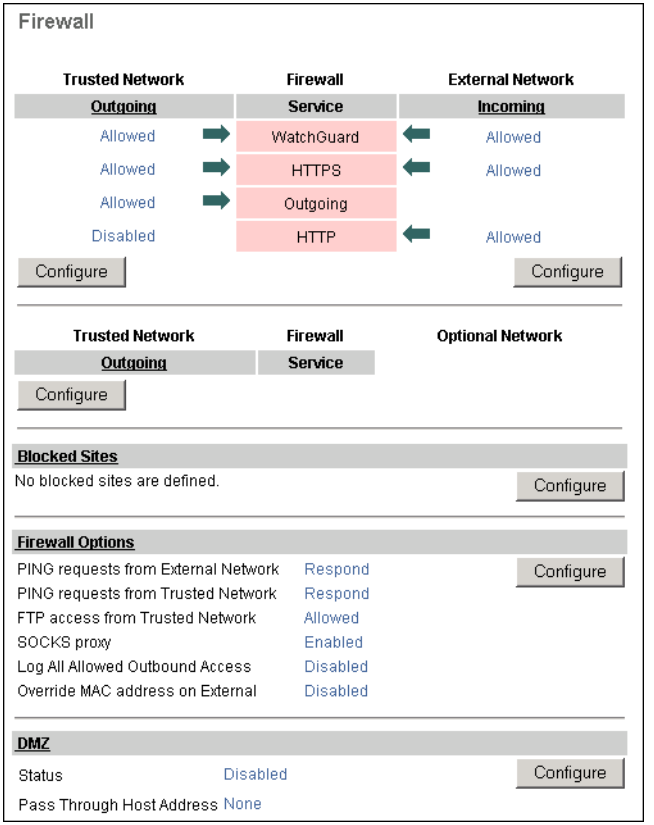
## Administration Page

The Administration page shows whether the Firebox uses HTTP or HTTPS for its configuration pages, whether VPN Manager access is enabled, and which upgrades are enabled. It provides buttons to change configurations, add upgrades, and view the configuration file. For more information, see Chapter 10, “Managing the Firebox X Edge.”



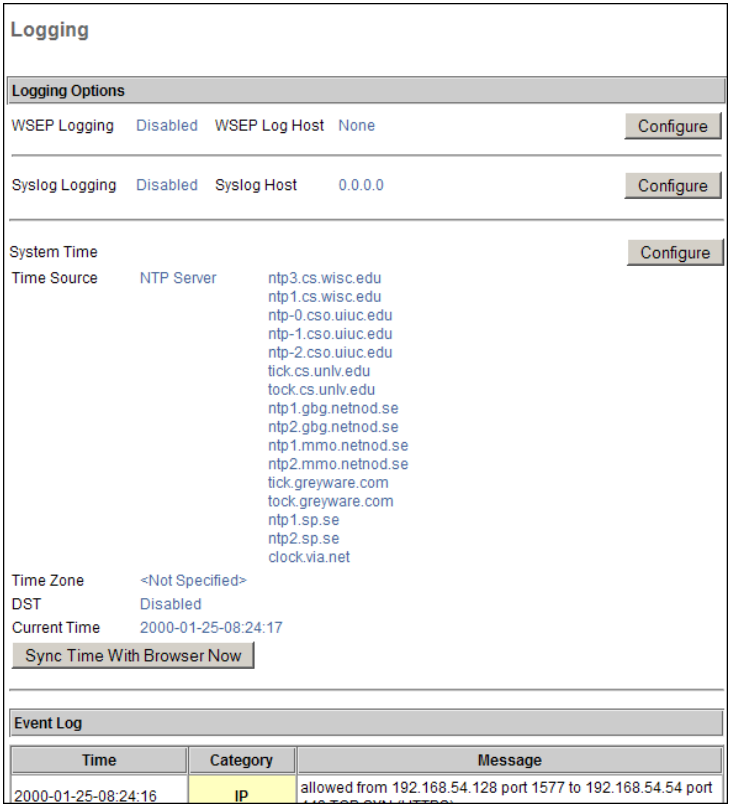
## Firewall Page

The Firewall page shows the incoming and outgoing services, blocked sites, as well as other firewell settings including an unrestricted address on the optional network. It also provides buttons to change these settings. For more information, see Chapter 5, “Configuring Firewall Settings.”



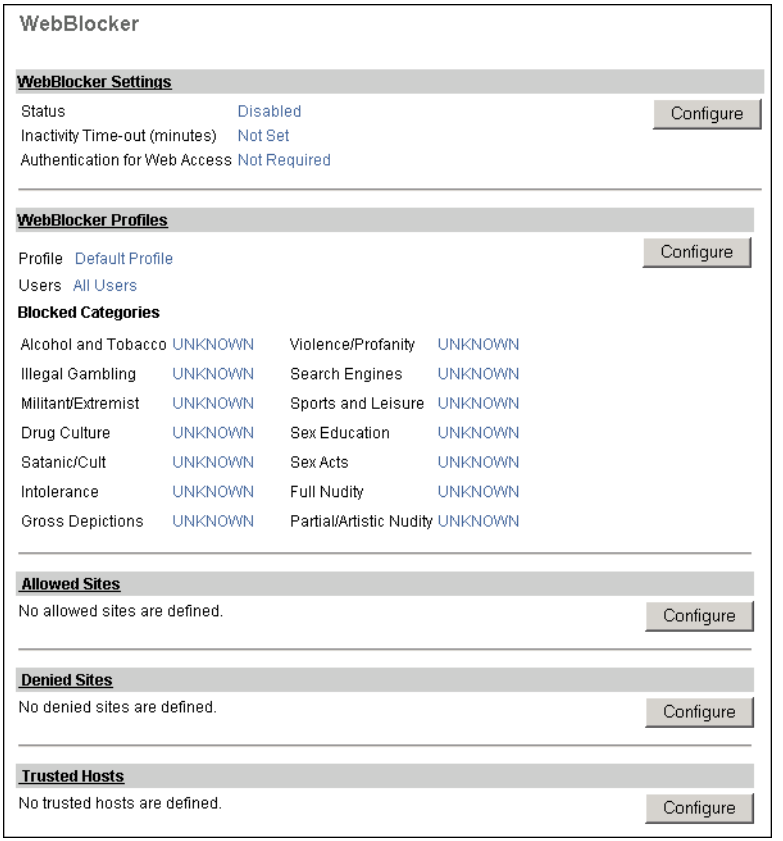
## Logging Page

The Logging page shows the current event log, status of WSEP and Syslog logging, and the system time. It also provides buttons to change these settings and to synchronize system time with your local computer. For more information, see Chapter 6, “Configuring Logging.”



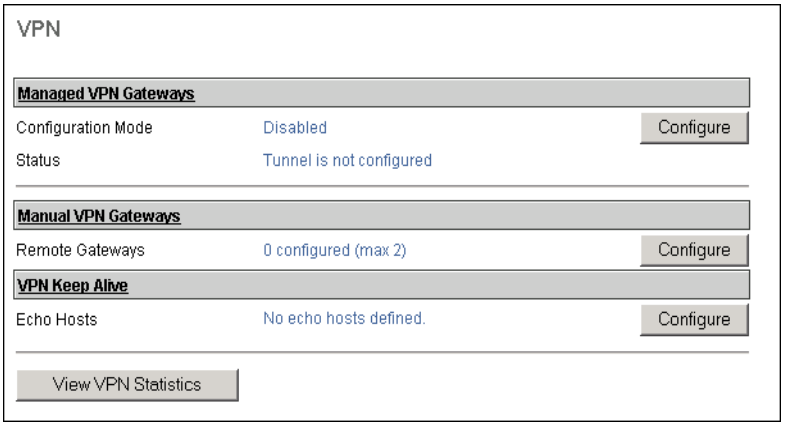
## WebBlocker Page

The WebBlocker page shows the WebBlocker settings, profiles, allowed sites, and denied sites. It also provides buttons to change the current settings. For more information, see Chapter 7, "Configuring WebBlocker."



## VPN Page

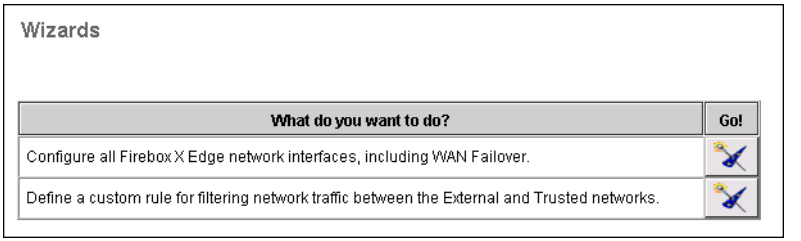
The VPN page shows information on managed VPNs, manual VPN gateways, and echo hosts along with buttons to change the configuration of VPN tunnels. It also provides a button for you to view statistics on active tunnels. For more information, see Chapter 8, “Configuring VPNs.




## Wizards Page

The Wizards page shows the wizards available to help you quickly and easily set up key Firebox X Edge features:

- Network Interface Wizard
  Configure all interfaces, including WAN failover. For more information, see “Using the Network Interface Wizard” on page 43.
- Service Configuration Wizard
  Define a rule for filtering network traffic between interfaces. For more information, see “Creating a custom service using the wizard” on page 67.



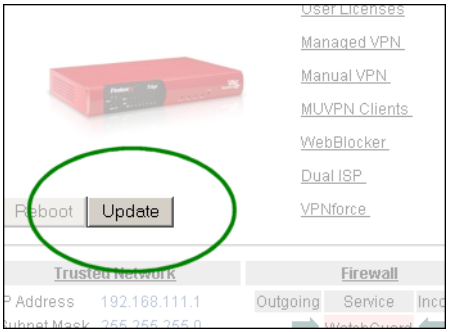
# Updating Firebox X Edge Software

One benefit of your LiveSecurity® Service is ongoing software updates. As new threats appear and WatchGuard adds product enhancements, you receive alerts to let you know about new versions of your Firebox® X Edge software.

When you receive the alert, you will be provided with instructions on how to download the software to your personal computer. Once this download is complete, use the following instructions to update your Firebox software:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
The default IP address is https://192.168.111.1.

2 At the bottom of the System Status page, click **Update**.
The Administration Page appears with the End User License Agreement (EULA). You can also reach this page by selecting Administration ⇒ Update from the navigation bar at left.




3 Read the text of the EULA. If you agree, select the **I accept the above license agreement** checkbox.

4 Type the name of the file containing the new Firebox X Edge software in the **Select file** box or click **Browse** to locate the file on your local computer.

5 Click **Update**.
The Firebox checks the software package to verify it is a legimate software upgrade. It then copies the new software to the system and reboots. This can take 15 to 45 seconds. When the update is complete, the System Status page appears and shows the new version number.

# Factory Default Settings

The term *factory default settings* refers to how the Firebox® X Edge is configured when you first receive it—before you have made any changes of your own to the configuration. The default network and configuration settings for the Firebox X Edge are as follows:

**Trusted network**

- The default IP address for the trusted network is 192.168.111.1. The subnet mask for the trusted network is 255.255.255.0.
- The Firebox X Edge is configured to assign IP addresses for computers on the trusted network through DHCP. You can also statically address computers in the trusted network with IP addresses in the 192.168.111.2–192.168.111.254 range.

**External network**

- The external network settings use DHCP.

**Optional network**

- The optional network is disabled.

**Firewall settings**

- All incoming services are blocked.
- An outgoing service allows all outbound traffic.
- All of the options on the Firewall Options page are disabled.
- The DMZ pass-through is disabled.

**System Security**

- The System Security is disabled. The system administrator name and system administrator passphrase are not set. All computers on the trusted network can access the configuration pages.
- Remote Management is disabled.
- VPN Manager Access is disabled.
- The remote logging is not configured.

**WebBlocker**

- The WebBlocker feature is disabled and the settings are not configured.

**Upgrade Options**

- The upgrade options are disabled until you enter the license keys into the configuration page.

### Resetting the Firebox to the factory default settings

You may have occasion to reset the Firebox to the factory default settings. For example, you might be having problems correcting a configuration problem and just want to "start over." Sometimes, a reset is your only choice: such as if the system security passphrase is unknown or the firmware of the Firebox X Edge is damaged by a power interruption.

You should have a copy of the most recent Firebox X Edge software on your local computer before attempting to return to factory default settings.

Follow these steps to reset the Firebox to the factory default settings:

1 Disconnect the power supply.

2 Press and hold down the **Reset** button, located on the front of the Firebox.

3 Connect the power supply while still holding down the Reset button.

4 Continue holding down the button until the red light on the front of the Firebox blinks in a steady pattern (about 15 seconds).

5 Disconnect the power supply.

6 Reconnect the power supply.
The Power indicator is on and the reset is complete.

## Rebooting the Firebox

You can reboot the Firebox® X Edge from a computer on the trusted network. You can also reboot the Firebox from a computer using the Internet to connect to the Firebox external interface.

The Firebox reboot cycle is up to 30 seconds. During the reboot cycle, the mode light on the front of the Firebox goes off and then comes on again.

### Local reboot

You can locally reboot the Firebox X Edge either using the Web browser or by disconnecting the power supply.

### Using the Web browser

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
The default IP address is: https://192.168.111.1

2 Click **Reboot**.


### Disconnecting the power supply

Disconnect the Firebox power supply. After a minimum of 10 seconds, connect the power supply.

## Remote reboot

The remote Firebox X Edge must be configured to forward incoming HTTP (Web) or FTP traffic to the Firebox's trusted interface IP address if you want to use the following method to reboot it. For more information on how to configure the Firebox to receive incoming traffic, see "Configuring Incoming and Outgoing Services" on page 65. Also, see the following FAQ for more information on configuring a Firebox X Edge to receive incoming traffic:
https://www.watchguard.com/support/tutorials/stepsoho_remotemanage.asp

1 Type the external network IP address of the remote Firebox X Edge in your browser window to connect to its System Status page.

2 Click **Reboot**.

CHAPTER 4

# Changing Your Network Settings

A primary task in setting up your WatchGuard® Firebox® X Edge is configuring the network interfaces. At the least, you must configure the external and trusted network interfaces to enable traffic to flow through the Firebox from the Internet to the internal network. You can also set up a third, optional interface, which connects to a second secured network, typically any network of servers provided for public access.

You can set up your network either with the Network Interface Wizard or by manually using the Network page of the Firebox X Edge configuration pages.

## Using the Network Interface Wizard

The easiest way to set up your Firebox® X Edge network is with using the Network Interface Wizard.

1 From the navigation bar at left, select **Wizards**.

2 Next to **Configure all Firebox X Edge network interfaces, including WAN failover**, click **Go**.

3 Work through the wizard, following the instructions on the screens. Steps associated with optional functionality you decide not to enable are automatically skipped by the wizard.

The Network Interface Wizard consists of the following steps:

**Step 1: Welcome**
The first screen describes the purpose of the wizard and the information you need before running it.

**Step 2: External Interface Configuration**
The next screen asks you how the Firebox X Edge determines its external IP address settings. For more information, see the introductory material in "Configuring the External Network" on page 45.

**Step 3: External Interface Failover Configuration (Optional)**
Using the next screen, select the interface to be used for failover and specify which remote hosts the Firebox X Edge should periodically contact when an interface has become unavailable. For more information, see the introductory material in "Enabling the WAN Failover Option" on page 61.

**Step 4: Failover Interface Configuration (Optional)**
On the Failover Interface Configuration screen, specify how the Firebox X Edge determines its failover external IP address settings.

**Step 5: Trusted Interface Configuration**
The Trusted Interface Configuration screen asks you how the Firebox X Edge determines its trusted IP address settings. For more information, see the introductory material in "Configuring the Trusted Network" on page 48.

**Step 6: Trusted Interface DHCP Server Configuration (Optional)**
On the next screen, define the range of IP addresses to be leased by the Firebox DHCP server to its clients on the trusted network.

**Step 7: Optional Interface Configuration (Optional)**
The Optional Interface Configuration screen asks you how the Firebox X Edge determines its trusted IP address settings. For more information, see the introductory material in "Configuring the Optional Network" on page 53.

**Step 8: Optional Interface DHCP Server Configuration (Optional)**
On the next screen, define the range of IP addresses to be leased by the Firebox X Edge server to its clients on the optional network.

**Step 9: Summary**
The wizard's last screen displays a summary of the settings you have made using the wizard.

## Configuring the External Network

When you configure the external network, you select the method of communication between the Firebox® X Edge and your Internet service provider (ISP). Make this selection based on the method of network address distribution in use by your ISP. The three available methods are:

- **DHCP** - Dynamic Host Configuration Protocol is a communications protocol used by network administrators to automate the assignment of addresses in a network. With DHCP, your Firebox might receive a new external address every time it contacts your service provider.
- **Static IP address** - Static IP addresses are manually assigned by the service provider to each customer. Because they require more administrative overhead, service providers often charge a fee for a static IP address. Static IP addressing is also known as Manual Addressing.
- **PPPoE** - Point to Point Protocol over Ethernet is another method commonly used by service providers as it integrates well with traditional dial-up infrastructure.

In all situations, you need your service provider to give you a public IP address. Some network address ranges are *reserved*, private addresses and are only used by networks behind a device using network address translation (NAT). The default trusted IP address for the Firebox X Edge is an example of a private IP address: 192.168.111.0.

If you don't know how your modem or router is assigned a public IP address, contact your service provider or corporate network support staff.

**NOTE**

You can configure the network interfaces in any order. Although this chapter describes configuring the external interface first, you do not need to configure the external interface before the trusted interface.

## If your service provider uses DHCP

The default configuration sets the Firebox X Edge to get the external address information through DHCP. If your ISP supports this method, the Firebox gets IP address information from the ISP when the Firebox reboots and connects to the Internet.

For more information about DHCP, see “About DHCP” on page 5.

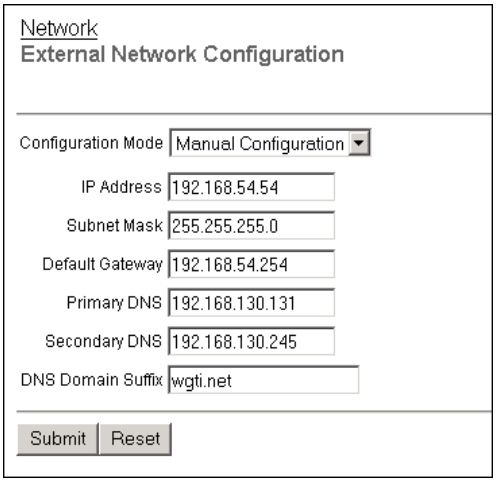
## If your ISP uses static addressing

If your ISP assigns a static IP address, you must assign that to your Firebox so the ISP communicates with the Firebox and not your computer.

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
The default IP address is: https://192.168.111.1

2 From the navigation bar at left, select **Network ⇒ External**.
The External Network Configuration page appears.

3 From the **Configuration Mode** drop-down list, select **Manual Configuration**.




4 Type the TCP/IP settings you recorded from your computer during the installation process. Refer to the table on page 14.

5 Click **Submit**.

## If your ISP uses PPPoE

If your ISP assigns IP addresses through PPPoE, your PPPoE login name and password are required to configure the Firebox X Edge. For more information in PPPoE, see “About PPPoE” on page 6.

To configure the Firebox for PPPoE:

1 Open your Web browser and click **Stop**.

Because the Internet connection is not configured, the browser cannot load your home page from the Internet. The browser can open the configuration pages in the Firebox.

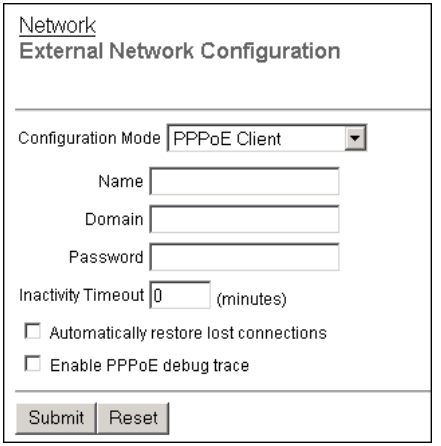
2 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.

The default IP address is: https://192.168.111.1

3 From the navigation bar at left, select **Network** ⇒ **External**.

The External Network Configuration page opens.

4 From the **Configuration Mode** drop-down list, select **PPPoE Client**.




5 Type the PPPoE login name supplied by your ISP.

6 If your ISP provides a domain name, type it in the **Domain** field.

Your ISP most likely provides your domain name as part of your login name; for example, myname@mydomain. If your ISP tells you to use username@domain as your login, type username in the Name field and domain in the Domain field. The “at” sign (@) is dropped. If your ISP provides only a username and password, then leave the Domain field blank.

7 Type the PPPoE password supplied by your ISP.

8 Type the time delay before inactive TCP connections are disconnected.

9 If appropriate, select the **Automatically restore lost connections** checkbox.

This option keeps a constant flow of traffic between the Firebox and the PPPoE server. This allows the Firebox to keep the PPPoE connection open during a period of frequent packet loss. If the flow of traffic stops, the Firebox reboots. A reboot frequently restores the connection. The ISP sees this constant flow of traffic as a continuous connection. The regulations and billing policy of the ISP determine whether you can use this option.

10 Select the **Enable PPPoE debug trace** checkbox to activate PPPoE debug trace.

This can assist WatchGuard Technical Support in troubleshooting PPPoE problems.

11 Click **Submit**.

## Configuring the Trusted Network

You can set the trusted network to use either the Firebox® X Edge's internal DHCP server or you can use static addressing. You can also change the IP address of the trusted network.

By default, the Firebox DHCP server is enabled. The Firebox trusted network starts with IP address 192.168.111.1 and is a class C network using subnet mask 255.255.255.0. In other words, the Firebox can distribute up to 251 additional, unique network addresses from 192.168.111.2 to 192.168.111.252. In addition, the Firebox by default uses the same DNS and domain information as it receives from your service provider.

For more information on IP addressing, see "IP Addresses" on page 5.

If you want to use a DHCP server other than the one packaged with the Firebox X Edge, disable the Firebox X Edge DHCP server. If you want to forward DHCP requests to a remote DHCP server through a relay agent, enable the DHCP Relay option as described in "Configuring the Firebox as a DHCP relay agent" on page 51.

## Changing the IP address of the trusted network

Sometimes it is necessary to change the trusted network address range. For example, if you are connect two or more Firebox devices in a virtual private network, each Firebox must use a different network address range. For more information, see “What You Need to Create a VPN” on page 93.

To change the IP address of the trusted network:

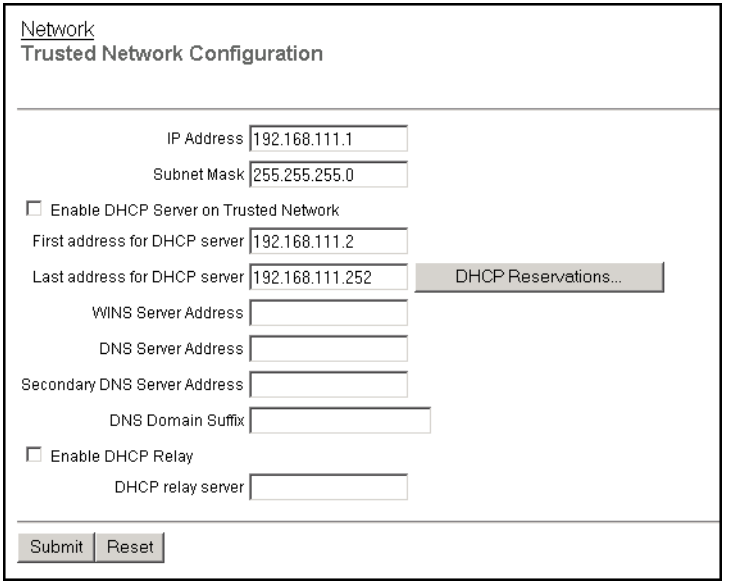
1. Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
   The default IP address is: https://192.168.111.1
2. From the navigation bar at left, select **Network ⇒Trusted**.
   The Trusted Network Configuration page appears.
3. Enter the first address in the new network address range in the IP address text field.
   The default subnet mask works for most networks..

## Configuring the Firebox as a DHCP server

The DHCP Server option sets the Firebox X Edge to assign IP addresses to the computers on the trusted network. The Firebox uses DHCP to make the assignments. When the Firebox receives a request from a new computer on the trusted network, the Firebox assigns the computer an IP address. By default, the Firebox DHCP server is enabled.

To configure the Firebox as a DHCP server:

1 If you have not already done so, use your browser to open the Firebox X Edge configuration pages. Select **Network ⇒Trusted.**
The Trusted Network Configuration page appears.




2 Select the **Enable DHCP Server on the Trusted Network** checkbox.

3 Type the first IP address and last IP address that is available for the computers that connect to the trusted network in the applicable fields.
The address range must be on the same network as the trusted IP address. For example, if your trusted IP address is 192.168.200.1, the range should be from 192.168.200.2 to 192.168.200.252.

4 Type the WINS Server address, DNS Server primary address, DNS Server secondary address, and DNS Domain server suffix in the applicable fields.
If no value is entered, the Firebox by default uses the address settings provided to it from your service provider.

5 Click **Submit.**

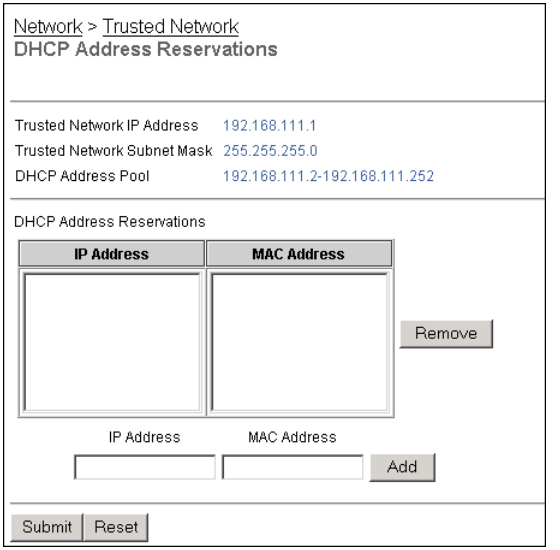
6 Reboot the Firebox X Edge.

## Setting DHCP Address Reservations

You can bind a static IP address to a specific hardware device by way of its MAC address.

1 If you have not already done so, use your browser to open the Firebox X Edge configuration pages. Select **Network ⇒ Trusted**.
The Trusted Network Configuration page appears.

2 Click the **DHCP Reservations** button.
The DHCP Address Reservations page appears.




3 Choose a static IP address from the DHCP address pool listed on the page and type it in the **IP Address** field.

4 Find the MAC address of the hardware device you would like to assign the IP address to and type it in the MAC address field. Click **Add**. Click **Submit**.

## Configuring the Firebox as a DHCP relay agent

Another way to distribute network addresses to the computers protected by the Firebox X Edge is to use a DHCP server on another network. The Firebox can relay DHCP requests to that server and then send the results back to the computers on the trusted network. This option is commonly used by network administrators managing multiple remote offices and allows even remote computers to use the same network address range.

To configure the Firebox as a DHCP relay agent:

1 If you have not already done so, use your browser to open the Firebox X Edge configuration pages. Select **Network ⇒Trusted**.
The Trusted Network Configuration page appears.

2 Select the **Enable DHCP Relay** checkbox.

3 Type the IP address of the DHCP relay server in the applicable field.

4 Click **Submit.**

5 Reboot the Firebox X Edge.
With DHCP relay enabled, the Firebox will send all DHCP requests to the specified, remote DHCP server and relay the resulting IP addresses to the computers connected to the trusted network. If the Firebox is unable to contact the specified, remote DHCP server in 30 seconds, it will revert to using its own DHCP server to respond to computers on the trusted network.

## Assigning static IP addresses

Whether or not you choose to use the Firebox X Edge DHCP server, you can assign static IP addresses to computers on your trusted network. If you disable the DHCP server, you will have to manually configure the IP address and subnet mask of all computers on the trusted network. You can also choose to selectively configure individual computers with a static IP address. This is necessary, for example, when a client-server application requires a static IP address for the server.

To disable the Firebox X Edge DHCP server completely, clear the **Enable DHCP Server on the Trusted Network** checkbox on the Trusted Network Configuration page.

**NOTE**

All changes to the Trusted Network Configuration page require that you click Submit and then reboot the Firebox before they take effect. But you can make all the changes you want to make and then reboot just once when you are done.

## Configuring additional computers on the trusted network

The Firebox X Edge accepts connections from up to seven computers. You can join a larger number of computers into a network using one or more 10/100 BaseTx Ethernet hubs or switches with RJ-45 connectors. The Firebox X Edge system coexists with other systems

over the same LAN. If you mix computers with different operating systems on your network, they pass traffic through the Firebox X Edge to access the Internet.

To add more computers to the trusted network:

1 Verify each additional computer has an Ethernet card installed.

2 Connect each computer to the network the same way you did in “Cabling the Firebox X Edge for more than seven devices” on page 18. Restart each computer.

3 Set the computers to obtain their addresses using DHCP.

4 Turn off and start each computer.

# Configuring the Optional Network

The optional network extends the protection of the firewall to include telecommuters on a separate network. Users on both the optional network and the trusted network have protected access to the Internet, but only the optional network has access to the corporate network. Communication between the optional network and the trusted network are denied by default, although you can enable traffic between the two networks, as described in “Filtering Outgoing Traffic to the Optional Network” on page 69. Note, however, that enabling this traffic removes the security between the two networks.

As with the trusted network, you can use either the Firebox® X Edge’s internal DHCP server or you can use static addressing on the optional network. You can also change the IP address range of the optional network.

Normally, if you have servers on your optional network, you should disable DHCP and use static IP addressing. If your servers need to be secure from Internet traffic, you may want to put your users on the optional network with DHCP enabled and your servers on the trusted, more secure network.

## Enabling the optional network

1 Type the IP address of the optional network in your browser window to connect to the System Status page of the Firebox X Edge.
The default IP address is: https://192.168.111.1

2 From the navigation bar at left, select **Network ⇒ Optional**.
The Optional Network Configuration page appears.
3 Select the **Enable Optional Network** checkbox.

## Changing the IP address of the optional network

Sometimes it is necessary to change the optional network address range. One example might be if your optional network is wireless and you want to separate the wireless and wired networks.

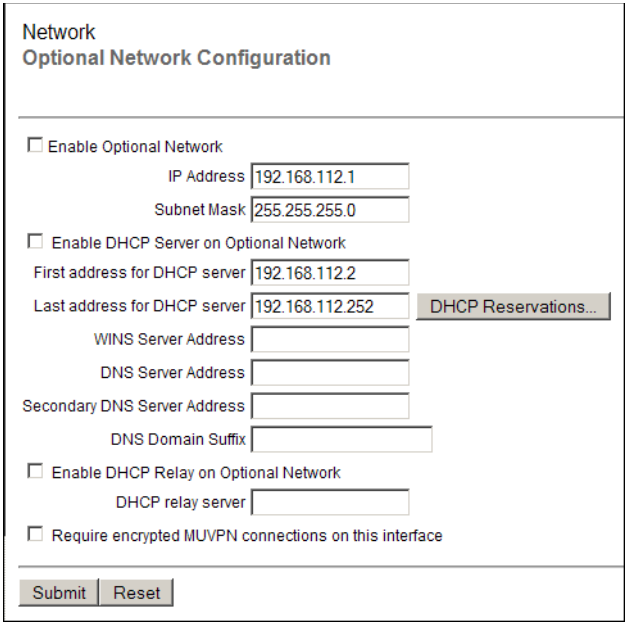
To change the IP address of the optional network:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
The default IP address is: https://192.168.111.1
2 From the navigation bar at left, select **Network ⇒ Optional**.
The Optional Network Configuration page appears.
3 Enter the first address in the new network address range in the IP address text field.
You can leave the subnet mask unchanged.

## Configuring DHCP on the optional network

Just as with the trusted network, you can use the Firebox as either a DHCP server or DHCP relay. To configure the Firebox as a DHCP server:

1 If you have not already done so, use your browser to open the Firebox X Edge configuration pages. Select **Network** ⇒ **Optional**.
The Optional Network Configuration page appears.




2 Select the **Enable DHCP Server on the Optional Network** checkbox.

3 Type the first IP address and last IP address that is available for the computers that connect to the trusted network in the applicable fields.
The address range must be on the same network as the optional IP address. For example, if your trusted IP address is 192.168.200.1, the range should be from 192.168.200.2 to 192.168.200.252.

4 Type the WINS Server address, DNS Server primary address, DNS Server secondary address, and DNS Domain server suffix in the applicable fields.
If no value is entered, the Firebox by default uses the address settings provided to it from your service provider.

5 Click **Submit.**

6 Reboot the Firebox X Edge.

To configure the Firebox as a DHCP relay agent:

1 If you have not already done so, use your browser to open the Firebox X Edge configuration pages. Select **Network** ⇒ **Optional**.
The Trusted Network Configuration page appears.

2 Select the **Enable DHCP Relay** checkbox.

3 Type the IP address of the DHCP relay server in the applicable field.

4 Click **Submit.**

5 Reboot the Firebox X Edge.
The Firebox will send all DHCP requests to the specified, remote DHCP server and relay the resulting IP addresses to the computers connected to the trusted network. If the Firebox is unable to contact the specified, remote DHCP server in 30 seconds, it will revert to using its own DHCP server to respond to computers on the trusted network.

## Assigning static IP addresses on the optional network

Whether or not you choose to use the Firebox X Edge DHCP server, you can assign static IP addresses to computers on your optional network. If you disable the DHCP server, you will have to manually configure the IP address and subnet mask of all computers on the optional network. You can also choose to selectively configure individual computers with a static IP address. This is necessary, for example, when a client-server application requires a static IP address for the server.

To disable the Firebox X Edge DHCP server completely, clear the **Enable DHCP Server on the Optional Network** checkbox on the Optional Network Configuration page.

**NOTE**

All changes to the Optional Network Configuration page require that you click Submit and then reboot the Firebox before they take effect. But you can make all the changes you want to make and then reboot just once when you are done.

You can either enable or disable the DHCP server on the optional network.

### Requiring encrypted connections

You can require encrypted MUVPN connections on this interface if you want to secure a wireless network. If you choose this option, all traffic from wireless clients is encrypted. This reduces the possibility of drive-by "snooping" into a wireless network connected to the optional port.

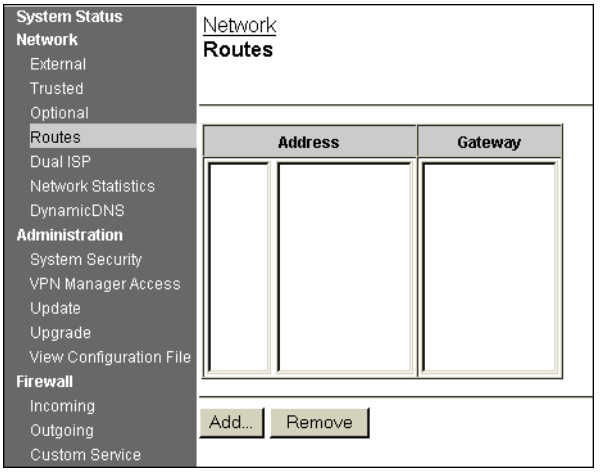
## Configuring Static Routes

To send specific traffic to different segments of the Firebox® X Edge trusted network connected through a router or switch, configure static routes.

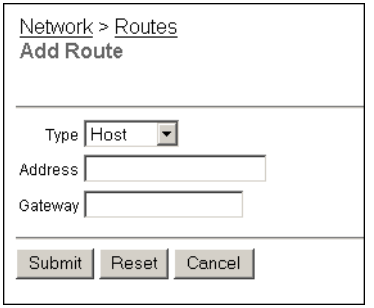
Follow these instructions to configure static routes:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
The default IP address is: https://192.168.111.1

2 From the navigation bar at left, select **Network** ⇒ **Routes**.
The Routes page appears.




3 Click **Add**.
The Add Route page appears.




4 From the **Type** drop-down list, select either **Host** or **Network**.
A host is a single computer. A network is a range of IP addresses on which many computers can connect.

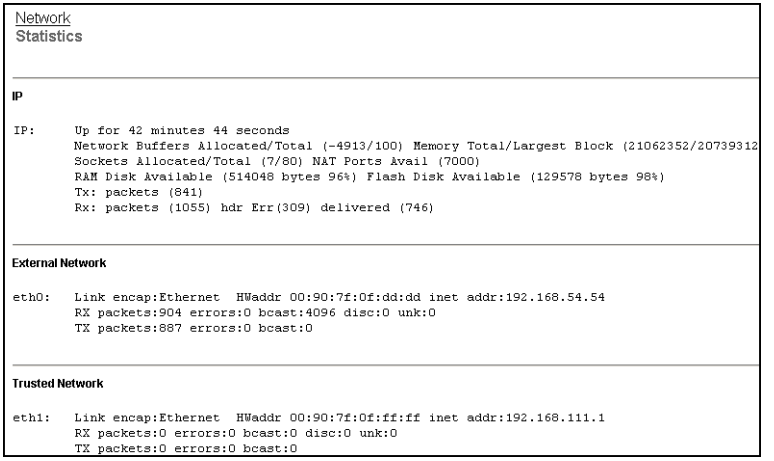
5 Type the IP address of the route's destination and the IP address for the route's gateway in the applicable fields.
The gateway of the route is the local interface of the router.

6 Click **Submit**.

To remove a route, select the route and click **Remove**.

# Viewing Network Statistics

The Firebox® X Edge Network Statistics page gives information about network performance. This page is useful during trouble-shooting.


Network
Statistics

IP

```
IP:     Up for 42 minutes 44 seconds
        Network Buffers Allocated/Total (-4913/100) Memory Total/Largest Block (21062352/20739312
        Sockets Allocated/Total (7/80) NAT Ports Avail (7000)
        RAM Disk Available (514048 bytes 96%) Flash Disk Available (129578 bytes 98%)
        Tx: packets (841)
        Rx: packets (1055) hdr Err(309) delivered (746)
```

External Network

```
eth0:   Link encap:Ethernet  HWaddr 00:90:7f:0f:dd:dd inet addr:192.168.54.54
        RX packets:904 errors:0 bcast:4096 disc:0 unk:0
        TX packets:887 errors:0 bcast:0
```

Trusted Network

```
eth1:   Link encap:Ethernet  HWaddr 00:90:7f:0f:ff:ff inet addr:192.168.111.1
        RX packets:0 errors:0 bcast:0 disc:0 unk:0
        TX packets:0 errors:0 bcast:0
```

Follow these instructions to access the Network Statistics page:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
The default IP address is: https://192.168.111.1

2 From the navigation bar at left, select **Network ⇒ Network Statistics.**
The Network Statistics page appears.

# Registering with the Dynamic DNS Service

You can register the external IP address of the Firebox® X Edge with the dynamic domain name server (DNS) service DynDNS.org. A dynamic DNS service makes sure that the IP address attached to your domain name is changed when your ISP assigns you a new IP address. For more information, browse to the DynDNS.org Web site at:

http://www.dyndns.org/

Or, see the following FAQs on the WatchGuard Technical Support site at:

https://www.watchguard.com/support/advancedfaqs/sogen_main.asp

What is Dynamic DNS?

How do I set up Dynamic DNS?

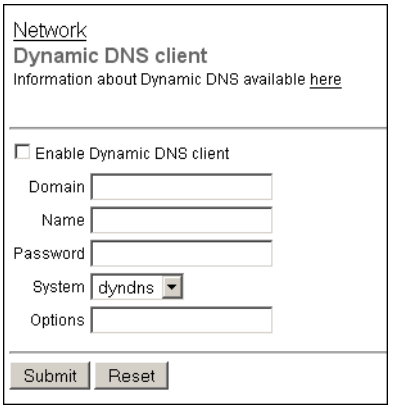
**NOTE**

WatchGuard is not affiliated with DynDNS.org.

1 Create a dynamic DNS account.
For more information, see the Technical Support FAQ "How do I set up Dynamic DNS?

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
The default IP address is: https://192.168.111.1

2 From the navigation bar at left, select **Network ⇒ Dynamic DNS.**
The Dynamic DNS client page appears.




3 Select the **Enable Dynamic DNS client** checkbox.

4 Type the domain, name, and password in the applicable fields.

**NOTE**

The Firebox X Edge receives the IP address of members.dyndns.org when it connects to the time server.

5 Click **Submit**.

# Enabling the WAN Failover Option

The WAN Failover option adds redundant support for the external interface. With this upgrade installed, the Firebox® X Edge starts a connection through the WAN2 port when the primary external port (WAN1) connection fails. It is frequently used by businesses who can not afford even a small amount of lost connection time and will pay for a second Internet account.

No new policy definitions are required. The failover interface uses the same policy definitions as the external interface.

The Firebox X Edge uses two methods to determine whether the external interface connection is down:

- The status of the link to the nearest router
- A ping to a specified location

The Firebox X Edge pings the default gateway or the location selected by the administrator. If there is no response, the Firebox switches to the secondary external network connection.

When this feature is enabled, these actions automatically occur:

- If the WAN1 connection fails, the WAN2 port connection is opened and used.
- If the WAN2 port connection fails, the WAN1 port connection is opened and used.
- If both the WAN1 port and WAN2 port connections fail, the Firebox tries both ports until a connection is made.

When the WAN2 port is in use, the Firebox does not switch back to the WAN1 port unless PPPoE is used to assign IP addresses. After the Firebox switches to the WAN2 port, the administrator must change the configuration back to the WAN1 port when the connection is restored.

If you use PPPoE, you can set an inactivity timeout that disables inactive TCP connections during periods of inactivity. See “If your ISP uses PPPoE” on page 47 for PPPoE configuration information. If your external connection fails, the WAN2 port connection is started and used. The WAN2 port is used until the TCP connection becomes inactive (timeout). When the traffic continues, the Firebox connects through the WAN1 port first. If a connection is made, the WAN1port

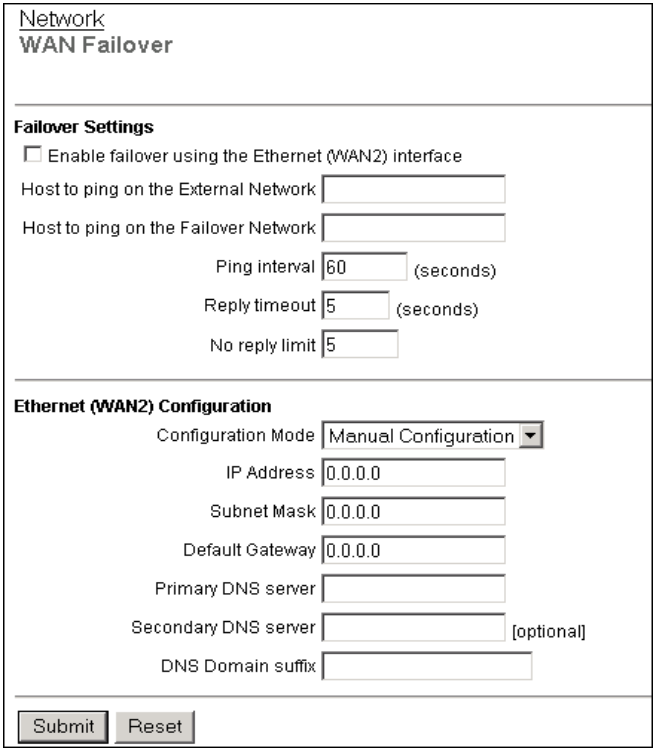
is used. If the WAN1 port is not available, the Firebox connects through the WAN2 port.

To configure the failover network:

1 Connect one end of a straight-through Ethernet cable to the WAN2 port, and connect the other end to the source of the secondary external network connection. This connection can be a cable modem or a hub.

2 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
The default IP address is: https://192.168.111.1

3 From the navigation bar at left, select **Network ⇒ WAN Failover.**
The WAN Failover page appears.



4 Select the **Enable failover using the Ethernet (WAN2) interface** checkbox.

5 From the drop-down list, select the interface for the feature: Ethernet or modem.

6 Type the IP addresses of the hosts to ping for WAN1 and WAN2 interfaces in the applicable fields.

7 Type the number of seconds between pings and the number of seconds to wait for a reply in the applicable fields.

8 Type the limit number of pings before timeout in the applicable field.

9 Click **Submit**.

CHAPTER 5

# Configuring Firewall Settings

The firewall configuration settings of the WatchGuard® Firebox® X Edge control the flow of traffic between the trusted network and the external network. The configuration you select depends on the degree of risk you determine to be acceptable for the trusted network.

## Configuring Incoming and Outgoing Services

For basic information about services, see “Services” on page 6.

Network traffic is classified as either incoming or outgoing. All traffic originating from the external interface is incoming traffic, regardless of the destination network behind your Firebox. Conversely, all traffic destined for the external interface is outgoing traffic, regardless of the location in your organization it originated from.

The default configuration of the Firebox® X Edge prevents the transmission of all packets from the external network to the trusted network. Change the configuration to select the types of traffic that you want to permit. For example, to operate a Web server behind the Firebox X Edge, configure the HTTP service to allow incoming connections and specify the IP address of the Web server (the internal computer that wil receive the requests for Web pages).

Select carefully the number and the types of services that you add. Added services decrease the security of your network. Be sure to com-

pare the value of access to each service against the security risk caused by that service.

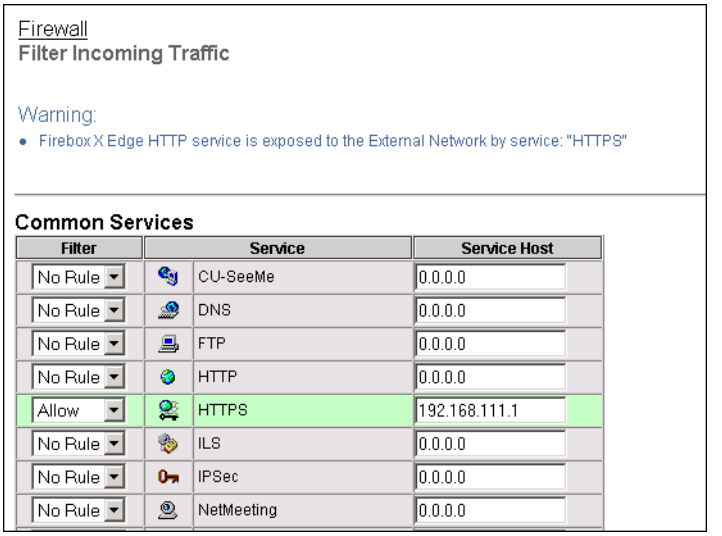
When configuring a service, you set the allowable traffic sources and destinations, as well as determine the filter rules and policies for the service.

## Preconfigured (common) services

A number of pre-configured services are available. Follow these steps to change the configuration of the incoming filters for common services:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
The default IP address is: https://192.168.111.1.

2 From the navigation bar at left, select **Firewall** ⇒ **Incoming** or **Outgoing**.
The Filter Traffic page appears.




3 Locate a pre-configured service, such as FTP, Web, or Telnet. Then select either **Allow**, **Deny**, or **No Rule** from the drop-down list. Continue for all the services you want to configure.

4 Click **Submit**.

## Creating a custom service using the wizard

If you need to allow a service that is not listed in the common services, configure a custom service based on a TCP port, a UDP port, or a protocol. The easiest way to do this is to use the Traffic Filter Wizard.

1 From the navigation bar at left, select **Wizards**.

2 Next to **Define a rule for filtering network traffic between interfaces**, click **Go**.

3 Work through the wizard, following the instructions on the screens.

The Traffic Filter Wizard consists of the following steps (steps associated with optional functionality you decide not to enable are automatically skipped by the wizard):

**Step 1: Welcome**
The first screen describes what the wizard does and the information you need before running it.

**Step 2: Basic Filter Definition**
On the next screen, you specify basic information such as the filter name and whether it is appied to incoming or outgoing traffic.

**Step 3: Protocols and Ports**
Next, you specify the ports you want to assign to this traffic filter.

**Step 4: Source Hosts**
On the next screen, you identify the IP addresses of the source hosts to which this traffic filter will apply.

**Step 5: Destination Hosts**
In this step, you identify the IP addresses of the destination hosts to which this traffic filter will apply.

**Optional: Destination "service" host**
This step appears if you have configured an incoming service to allow traffic from the enternal network to pass through to the trusted network. A local host on the trusted network must be specified as the destination for all traffic matching this filter. This host is referred to as a "service host" because it is generally used

to expose a service such as HTTP (a Web server) to the external network.

**Step 6: Summary**

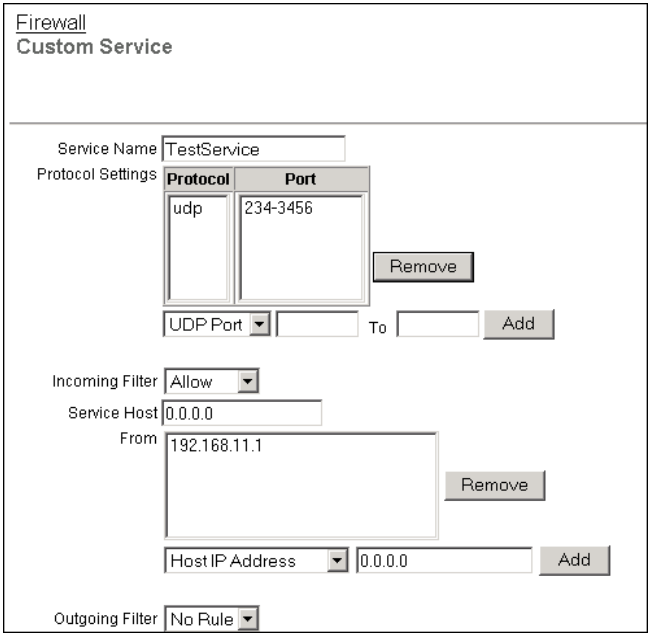
The wizard's last screen displays a summary of the settings you have made using the wizard.

## Creating a custom service manually

Follow these steps to configure a custom service manually:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
The default IP address is: https//192.168.111.1

2 From the Filter Traffic page, click **Add Service**, located at the lower-right portion of the page.
The Custom Service page appears.




3 Type a name for the service in the **Service Name** field.

4 Select **TCP Port**, **UDP Port**, or **Protocol** from the drop-down list below the **Protocol Settings**.

5 In the fields separated by the word **To**, either type a port number and leave the second box blank (for one port), type a range of port numbers (for range of ports), or type the protocol number.

**NOTE**

For a TCP port or a UDP port, specify a port number or a range of ports. For a protocol, specify an IP protocol number. You cannot specify a port number for an IP protocol that is not TCP or UDP. Examples of IP protocols other than TCP and UDP and the associated numbers are IP protocol 47 for GRE; IP protocol 50 for ESP. Creating a custom service using an IP protocol is rarely necessary.

6 Click **Add**.

The following steps determine how the service is filtered.

7 Select **Allow** or **Deny** from the **Incoming Filter** and **Outgoing Filter** drop-down lists.

8 Select **Host IP Address**, **Network IP Address**, or **Host Range** from the drop-down list at the bottom of the page.

9 Type a single host IP address, a network IP address, or the start and end of a range of host IP addresses in the applicable address field.

10 Click **Add**.
Repeat the previous three steps until all of the address information for this custom service is set.

11 Click **Submit**.

## Filtering Outgoing Traffic to the Optional Network

You can also define services to filter traffic from the trusted to the optional interface:

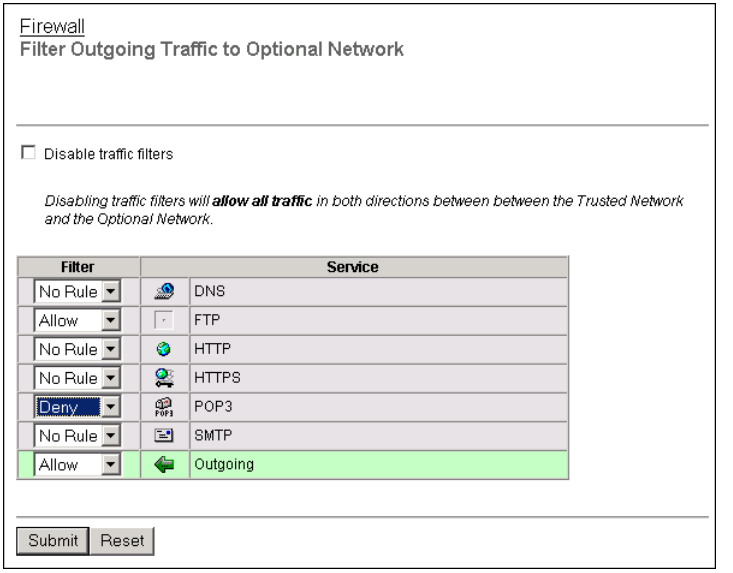
1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox® X Edge.
The default IP address is: https://192.168.111.1

2 From the navigation bar at left, select **Firewall** ⇒ **Optional**.
The Filter Outgoing Traffic to Optional Network page appears.

3 Select **Allow**, **Deny,** or **No Rule** from the **Filter** drop-down lists.

4 Click **Submit**.

You can also select the **Disable traffic filters** checkbox to allow all services between the networks. Note, however, that this allows all traffic in both directions between the trusted and the optional network.




## Blocking External Sites

The Blocked Sites feature of the Firebox® helps you prevent unwanted contact from or to known or suspected hostile systems. After you identify an intruder, you can block all attempted connections from them. You can also configure logging to record all access attempts from these sources so you can collect clues as to what services they are attempting to attack.

A blocked site is an IP address outside the Firebox that is prevented from connecting to hosts behind the Firebox. If any packet comes from a host that is blocked, it does not get past the Firebox.

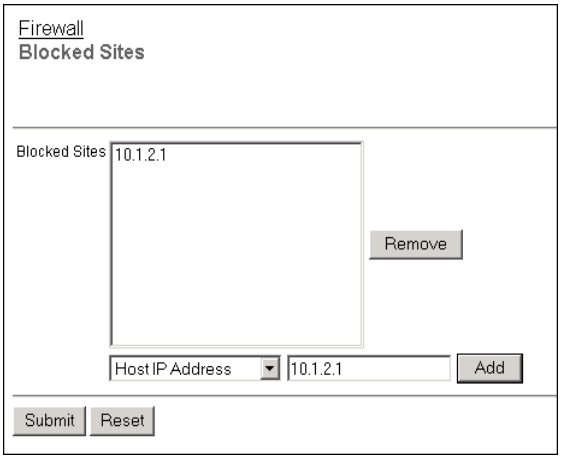
The default configuration of the Firebox X Edge:

- Allows the transmission of all packets from the trusted network to the external network

- Prevents the transmission of all packets from the external network to the trusted network

You can change the configuration to prevent access to specified Internet sites. Follow these steps to configure the blocked sites:

1 From the navigation bar at left, select **Firewall ⇒Blocked Sites**.
The Blocked Sites page appears.




2 Select either **Host IP Address**, **Network IP Address**, or **Host Range** from the drop-down list.

3 Type a single host IP address, a network IP address, or the start and end of a range of host IP addresses in the applicable address field.

4 Click **Add**.
The address information appears in the Blocked Sites field.

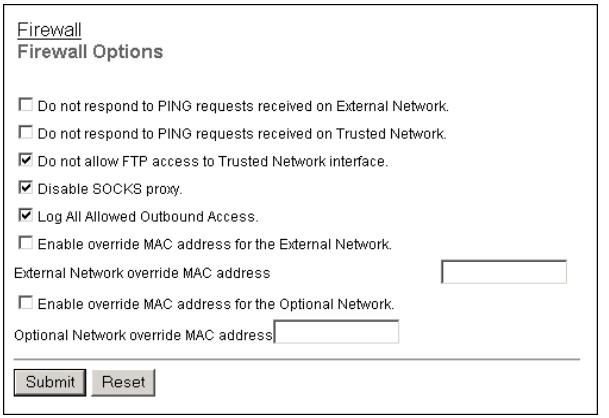
5 Click **Submit**.

## Configuring Firewall Options

The previous sections in this chapter describe how to allow or deny complete classes of services. You use the Firewall Options page to configure general security policies.

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox® X Edge.
The default IP address is: https://192.168.111.1

2 From the navigation bar at left, select **Firewall ⇒ Options**.
The Firewall Options page appears.




## Responding to ping requests

You can configure the Firebox X Edge to deny all ping packets received on the external or trusted interface.

1 Select the **Do not respond to PING requests received on External Network** checkbox or the **Do not respond to PING requests received on Trusted Network** checkbox.

2 Click **Submit**.

## Denying FTP access to the trusted network interface

You can configure the Firebox X Edge to prevent FTP access to the Firebox X Edge itself by the computers on the trusted or external network.

1 Select the **Do not allow FTP access to Trusted Network** checkbox.

2 Click **Submit**.

**NOTE**

If you want to use the Software Update Installer to transfer firmware files to the FIrebox X Edge (as described in "Method 1" on page 149), you must clear this checkbox. The Installer uses FTP to transfer firmware files.

## SOCKS implementation for the Firebox X Edge

The Firebox X Edge functions as a SOCKS network proxy server. An application that uses more than one socket connection and implements the SOCKS version 5 protocol can communicate through the Firebox. SOCKS supplies a secure, two-way communication channel between a computer on the external network and a computer on the trusted network. To use a SOCKS-compatible application, configure the application with the necessary information about the Firebox X Edge.

The Firebox X Edge supports SOCKS version 5 only. The Firebox does not support authentication or DNS (Domain Name System) resolution.

**NOTE**

Configure the SOCKS-compatible application to connect to IP addresses and not to domain names. Applications that can only reference domain names are not compatible with the Firebox X Edge.

Some SOCKS-compatible applications that function correctly when used through the Firebox X Edge are ICQ, IRC, and AOL Messenger.

**NOTE**

When a computer in the trusted network uses a SOCKS-compatible application, other users on the trusted network have free access to the SOCKS proxy on that computer. Disable SOCKS on the Firebox to prevent this security risk. See "Disabling SOCKS on the Firebox" on page 74.

### Configuring your SOCKS application

To allow a SOCKS-compatible application on a computer in the trusted network to communicate with a computer on the external network, configure the application as described below. To make these settings, refer to the user's guide for the application.

**NOTE**

The Firebox X Edge uses port 1080 to communicate with a computer that uses a SOCKS-compatible application. Make sure that port 1080 is not in use by other applications on the computer.

1 If there is a selection of protocols or SOCKS versions, select SOCKS version 5.

2 Select port 1080.

3 Set the SOCKS proxy to the URL or IP address of the Firebox X Edge. The default IP address is: https://192.168.111.1.

### Disabling SOCKS on the Firebox

After a SOCKS-compatible application has connected through the Firebox X Edge, the SOCKS port stays open. After the application terminates, the SOCKS port is available to anyone on your trusted network. The following steps prevent this security problem.

When the SOCKS-compatible application is not in use:

1 From the Firewall Options page, select the **Disable SOCKS proxy** checkbox.
This disables the SOCKS proxy feature of the Firebox.

2 Click **Submit**.

To use the SOCKS-compatible application:

1 Clear the **Disable SOCKS proxy** checkbox.
This enables the Firebox SOCKS proxy server.

2 Click **Submit**.

## Logging all allowed outbound traffic

When in the default configuration, the Firebox X Edge only records unusual events. For example, all denied traffic is recorded in the log file. You can change the configuration of the Firebox to record all outbound traffic events.

**NOTE**

This option records a large number of log entries. WatchGuard recommends that you use this option as a problem-solving aid only.

Follow these steps to enable this option:

1 Select the **Log All Allowed Outbound Access** checkbox.

2 Click **Submit**.

## Enabling the MAC address override

If your ISP has previously registered your computer's MAC address and will only allow connections from that MAC address, enable this option and use the MAC address of the computer that was previously used to connect to the ISP on this line. The MAC address must be entered in this format: hhhhhhhh

where:

- Each of the 12 "h" digits is a hexadecimal character with a value between 0 and 9 or between "a" and "f".
- The MAC address may not conflict with:
  - Another node on the external network
  - The Firebox X Edge trusted network MAC address
  - The Firebox X Edge optional network MAC address
- The MAC address may not be 000000000000
- The MAC address may not be ffffffffffff

**Example: 0012340ABCDE**

To determine your MAC address, use the ipconfig/all and ifconfig commands at the command prompt.

Follow these steps to enable this option:

1 Select the **Enable override MAC address for the External Network** or the **Enable override MAC address for the Optional Network** checkbox.

2 Type the new MAC address for the Firebox X Edge external network in the applicable field.

3 Click **Submit**.

**NOTE**

If the **MAC address for the external network** field is cleared and the Firebox X Edge is rebooted, the Firebox X Edge is reset to the factory-default MAC address for the external network.

To prevent MAC address collisions, the Firebox X Edge searches the external network periodically for the override MAC address. If the Firebox X Edge finds a device that uses the same MAC address, the Firebox resets to the factory-default external MAC address and reboots.

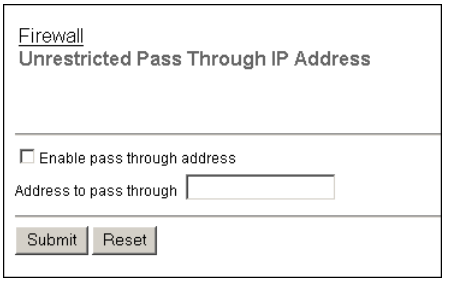
# Creating an Unrestricted Pass Through

The Firebox® X Edge can allow traffic to flow from the external network to a computer on the trusted network that has a public IP address.

Follow these steps to configure a pass through:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
The default IP address is: https://192.168.111.1

2 From the navigation bar at left, select **Firewall ⇒ Pass Through**.
The Unrestricted Pass Through IP Address page appears.




3 Select the **Enable pass through address** checkbox.

4 Type the IP address of the computer to connect to the pass through in the applicable field.
This must be a public IP address.

5 Click **Submit**.

**NOTE**

A pass through connection decreases the security of the trusted network, because the computer with the pass through connection is on the same Ethernet segment as the trusted network. Do not use a pass through connection unless the effect of the pass through connection on the security of the trusted network is known.

CHAPTER 6

# Configuring Logging

An *event* is any single activity that occurs at the Firebox® X Edge, such as denying a packet from passing through the Firebox. *Logging* is the process of recording and storing information about these events.

Because the log keeps a record of events that show possible security problems, logging is an important part of an effective network security policy. For example, a sequence of denied packets can show that an unauthorized person tried to access your network. You can configure your firewall to log a wide variety of events, including specific events that occur at the level of individual services.

**NOTE**

The records in the Firebox X Edge log are erased if the power supply is disconnected or if the Firebox is rebooted from the Firebox X Edge Web pages. The records are not erased if an external syslog or WSEP logging host is configured.

## Viewing Log Messages

The Firebox X Edge event log records a maximum of 150 log messages. New entries are added to the top of the log. If a new entry is added when the event log is full, the oldest log message is removed.

The log messages include the time synchronizations between the Firebox X Edge and the WatchGuard Time Server, packets discarded

because of a packet handling violation, duplicate messages, return error messages, and IPSec messages.

Each log message has three parts:

**Time**
The exact time of the event that triggered the log message.

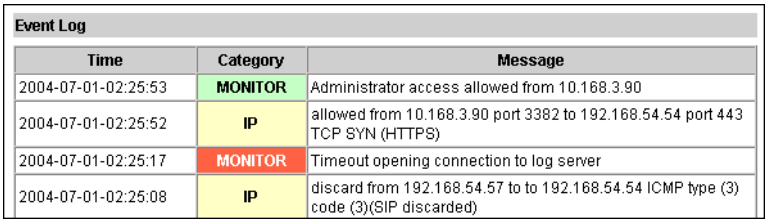
**Category**
The category of the message. For example, whether the message originated from an outside source such as an IP address, from the configuration file, and so on.

**Message**
The text of the message

The following procedure shows how to view the event log:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
The default IP address is: https://192.168.111.1

2 From the navigation bar at left, select **Logging**.
The Logging page appears with the Event Log at the bottom of the page.



Event Log

| Time | Category | Message |
|---|---|---|
| 2004-07-01-02:25:53 | MONITOR | Administrator access allowed from 10.168.3.90 |
| 2004-07-01-02:25:52 | IP | allowed from 10.168.3.90 port 3382 to 192.168.54.54 port 443 TCP SYN (HTTPS) |
| 2004-07-01-02:25:17 | MONITOR | Timeout opening connection to log server |
| 2004-07-01-02:25:08 | IP | discard from 192.168.54.57 to to 192.168.54.54 ICMP type (3) code (3)(SIP discarded) |

## Logging to a WatchGuard Security Event Processor Log Host

The WatchGuard Security Event Processor (WSEP) is an application that is available with the WatchGuard System Manager software. If you have a Firebox® III or Firebox X, configure the WSEP to accept the log messages from your Firebox X Edge. For instructions on how

to do this, see the *WatchGuard System Manager User Guide*. Then follow these instructions to send your event logs to the WSEP.

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox.
The default IP address is: https://192.168.111.1

2 From the navigation bar at left, select **Logging ⇒ WSEP Logging**.
The WatchGuard Security Event Processor Logging page appears.


3 The **Enable WatchGuard Security Event Processor Logging** checkbox should contain a checkmark. If it does not, select it such that the checkmark appears.

4 In the **Log Host IP Address** field, type the IP address of the WSEP server that is your log host.

5 Type a passphrase in the **Log Encryption Key** field and confirm the passphrase in the **Confirm Key** field.

6 In the **Device Name** field, type a friendly name for the Firebox X Edge.
This identifier enables the WSEP log host to distinguish between different devices logging to it. If this field is left blank, the Firebox X Edge will identify itself to the WSEP log host by the IP address currectly assigned to the Firebox's external interface.

7 Click **Submit**.

**NOTE**

Use the same log encryption key recorded in the WSEP application.

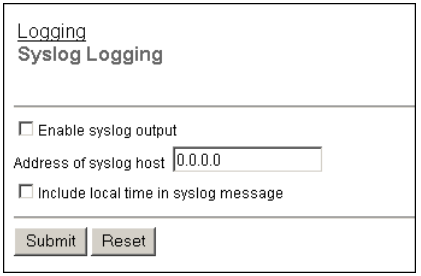
# Logging to a Syslog Host

Syslog is a logging interface, originally developed for UNIX, but now used by a number of computer systems. This option sends the Firebox® X Edge log messages to a syslog host. If you already maintain a syslog host, you can set the Firebox to send log messages to that host.

Follow these steps to configure a syslog host:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
The default IP address is: https://192.168.111.1

2 From the navigation bar at left, select **Logging ⇒ Syslog Logging**.
The Syslog Logging page appears.




3 Select the **Enable syslog output** checkbox.

4 Next to **Address of syslog host**, type the IP address of the computer running syslog.

5 (Optional) Select the **Include local time in syslog message** checkbox if you want to include the local time from your computer in the syslog messages.

6 Click **Submit**.

**NOTE**

Because syslog traffic is not encrypted, syslog messages that are sent through the Internet decrease the security of the trusted network. Use a VPN tunnel to increase the security of syslog message traffic. If the syslog messages are sent through a VPN tunnel, the data is encrypted with IPSec technology.

# Setting the System Time

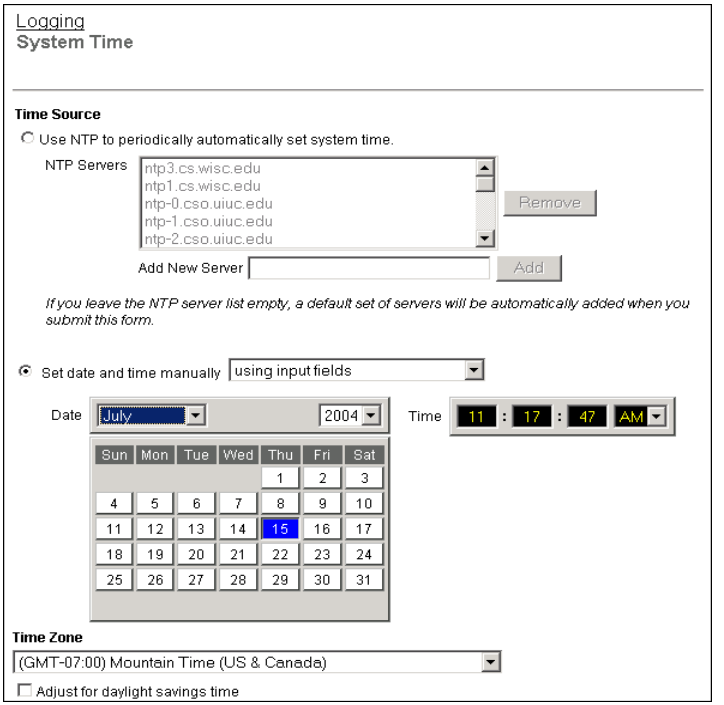
For each log entry, the Firebox® X Edge records the time from its system clock.

You can select one of two ways. You can specify that your system is symchronized using Network TIme Protocol (NTP) or you can set the date and time manually.

Follow these steps to set the system time:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
The default IP address is: https://192.168.111.1

2 From the navigation bar at left, select **Logging ⇒ System Time**.
The System Time page appears.




3 Select a time zone from the drop-down list.

4 (Optional) Select the **Adjust for daylight savings time** checkbox.

5 Select the method you want to set system time, as described in the next two sections.

6 Click **Submit**.

## Setting time using NTP

Network Time Protocol (NTP) synchronizes clocks of computers on a network. For more information on NTP, see http://www.ntp.org.

1 From the System Time page, select **Use NTP to periodically automatically set system time**.

2 Select an NTP server from the list. Or, type the name of a new server and click **Add**. You can add a maximum of 16 NTP servers.

## Setting time manually

1 From the System Time page, select **Set date and time manually**.

2 From the drop-down list, specify whether you want to set the date using input fields or by synchonizing time with the browser.

3 If you chose to set time using input fields, set the date using the calendar provided and set the time using the fields provided.

If you chose to set time by synchronizing, click **Synchronize Now** when you are ready to synchronize.

CHAPTER 7

# Configuring WebBlocker

Allowing network users to access any Web site they choose can lead to problems. An obvious one is loss of productivity. When employees are not guarded from distractions such as sports, entertainment, financial, and other non-work Web sites, their work performance can suffer. Web surfing can also reduce network bandwidth and take up disk space.

Network security is an issue as well. Allowing employees to access hacker sites and other problematic sites can also make your network more vulnerable to hacker attacks and viruses.

Permitting access to certain types of material can potentially have legal liabilities. A company that, for example, does not prevent employees from viewing pornography or racially offensive sites can be guilty of not providing a safe working environment for employees.

WebBlocker is an option for the WatchGuard® Firebox® X Edge that allows you to control which Web sites the users on your network can access.

**NOTE**

You must purchase the WebBlocker upgrade to be able to use this feature. For information on activating upgrade options, see "Activating Upgrade Options" on page 150.

## How WebBlocker Works

WebBlocker uses a database of Web site addresses that is owned and maintained by SurfControl®, a leading Web and e-mail filtering company. The database shows the type of content found on thousands of Web sites. WatchGuard puts the newest version of the SurfControl database on the WebBlocker server at regular intervals.

When a user on your network tries to bring up a Web site, the Firebox® sends to the database a request for the type of content found on the Web site. If the Web site is either not in the WatchGuard WebBlocker database or not in a blocked category, the Web browser opens it. Otherwise, a page appears telling the user that the site is unavilable.

## Configuring Global WebBlocker Settings

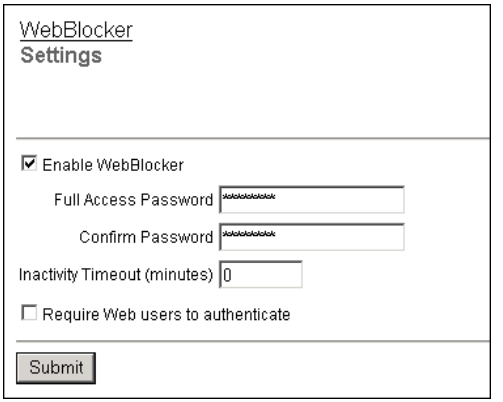
The first WebBlocker page in the Firebox® X Edge Web pages is the WebBlocker Settings page. Use this page to:

- Activate WebBlocker
- Set the full access password
- Set the inactivity timeout
- Require that your Web users authenticate

To configure WebBlocker:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
The default IP address is: https://192.168.111.1

2 From the navigation bar at left, select **WebBlocker ⇒ Settings**.
The WebBlocker Settings page appears.




3 Select the **Enable WebBlocker** checkbox.

4 Type a password in the **Full Access Password** field.
The full access password allows a user to access all Web sites until the password expires or the browser is closed.

5 Retype the same password in the **Confirm Password** field.

6 Type a value, in minutes, in the **Inactivity Timeout field**.
The inactivity timeout disconnects Internet connections that are inactive for the set number of minutes.

7 To require authentication for Internet access, select the **Require Web users to authenticate** checkbox.

8 Click **Submit**.

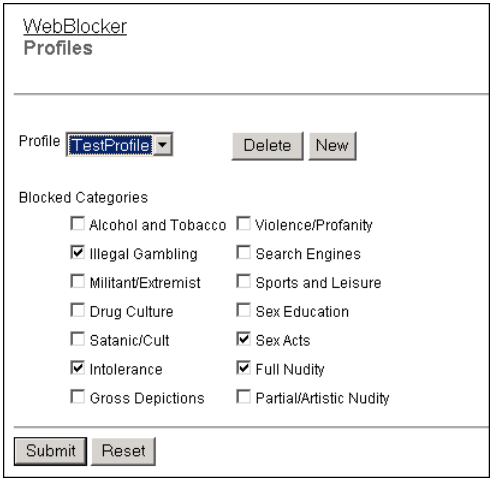
## Creating WebBlocker Profiles

A WebBlocker profile is a unique set of restrictions you can apply to users on your network. For example, you might define a profile containing many restrictions to be used for new employees with less than 90 days tenure and a less restrictive profile for users after the initial probationary period.

After you define profiles, you can apply them to users when you set up user accounts, as described in Chapter 10, “Managing the Firebox X Edge.”

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox® X Edge.
The default IP address is: https://192.168.111.1

2 From the navigation bar at left, select **WebBlocker ⇒ Profiles**.
The Profiles page appears.




3 Click **New**.
The New Profile page appears.

4 In the **Profile Name** field, type a familiar name for the profile.
You will use this name to identify the profile during later configuration. For example, you might call the profile described previously for new employees: 90day.

5 In the **Blocked Categories** portion of the page, click the categories of Web sites you want blocked.
For more information on categories, see the next section.

6 Click **Submit**.

To delete a profile, from the WebBlocker Profiles page, select the profile from the **Profile** drop-down list. Click **Delete**.

# WebBlocker Categories

The WebBlocker database contains 14 categories.

A Web site is added to a category only if the contents of the Web site advocate the subject matter of the category. Web sites that provide opinion or educational material about the subject matter of the category are not included. For example, the drugs/drug culture category blocks sites describing how to grow and use marijuana but does not block sites discussing the historical use of marijuana.

The categories are:

**Alcohol/tobacco**
Pictures or text advocating the sale, consumption, or production of alcoholic beverages and tobacco products.

**Illegal Gambling**
Pictures or text advocating materials or activities of a dubious nature that may be illegal in any or all jurisdictions, such as illegal business schemes, chain letters, copyright infringement, computer hacking, phreaking (using someone's phone lines without permission), and software piracy. Also includes text advocating gambling relating to lotteries, casinos, betting, numbers games, online sports, or financial betting, including non-monetary dares.

**Militant/extremist**
Pictures or text advocating extremely aggressive or combative behavior or advocacy of unlawful political measures. Topic includes groups that advocate violence as a means to achieve their goals. It also includes pages devoted to "how to" information on the making of weapons (for both lawful and unlawful reasons), ammunition, and pyrotechnics.

**Drug Culture**
Pictures or text advocating the illegal use of drugs for entertainment. This category includes substances that are used for other than their primary purpose to alter the individual's state of mind, such as glue sniffing. This does not include (that is, if selected these sites would not be blocked under this category) currently illegal drugs legally prescribed for medicinal purposes (such as drugs used to treat glaucoma or cancer).

**Satanic/cult**
Pictures or text advocating devil worship, an affinity for evil, wickedness, or the advocacy to join a cult. A cult is defined as: a closed society that is headed by a single individual where loyalty is demanded and leaving is punishable.

**Intolerance**
Pictures or text advocating prejudice or discrimination against any race, color, national origin, religion, disability or handicap, gender, or sexual orientation. Any picture or text that elevates one group over another. Also includes intolerant jokes or slurs.

**Gross Depictions**
Pictures or text describing anyone or anything that is either crudely vulgar, grossly deficient in civility or behavior, or shows scatological impropriety. Topic includes depictions of maiming, bloody figures, and indecent depiction of bodily functions.

**Violence/profanity**
Pictures or text exposing extreme cruelty or profanity. Cruelty is defined as: physical or emotional acts against any animal or person that are primarily intended to hurt or inflict pain. Topic includes obscene words, phrases, and profanity in either audio, text, or pictures.

**Search Engines**
Search engine sites such as Google.

**Sports and Leisure**
Pictures or text describing sporting events, sports figures, or other entertainment activities.

**Sex Education**
Pictures or text advocating the proper use of contraceptives. Topic includes sites devoted to the explanation and description of condoms, oral contraceptives, intrauterine appliances, and other types of contraceptives. It also includes discussion sites devoted to conversations with partners about sexually transmitted diseases, pregnancy, and sexual boundaries. Not included in this category are commercial sites selling sexual paraphernalia (topics included under *Sexual Acts*).

**Sexual Acts**
Pictures or text exposing anyone or anything involved in explicit sexual acts and/or lewd and lascivious behavior. Topic includes masturbation, copulation, pedophilia, as well as intimacy involving nude or partially nude people in heterosexual, bisexual, lesbian, or homosexual encounters. It also includes phone sex advertisements, dating services, adult personals, and sites devoted to selling pornographic CD-ROMs and videos.

**Full Nudity**
Pictures exposing any or all portions of human genitalia. Topic does *not* include sites categorized as Partial/Artistic Nudity containing partial nudity of a wholesome nature. For example, it does not include Web sites for publications such as *National Geographic* or *Smithsonian* magazine nor sites hosted by museums such as the Guggenheim, the Louvre, or the Museum of Modern Art.

**Partial/artistic Nudity**
Pictures exposing the female breast or full exposure of either male or female buttocks except when exposing genitalia which is handled under the Full Nudity category. Topic does not include swimsuits, including thongs.

For information on checking specific sites against the SurfControl database, and for more information on WebBlocker categories, see the following FAQs on the WatchGuard Support site at:

https://www.watchguard.com/support/AdvancedFaqs/web_main.asp

- How can I see a list of blocked sites?
- How do different sites map into WebBlocker's 14 categories?

## Allowing Certain Sites to Bypass WebBlocker

Because some sites might be useful to users despite their being denied by WebBlocker, you can specify sites that you want to be allowed regardless of other WebBlocker settings.

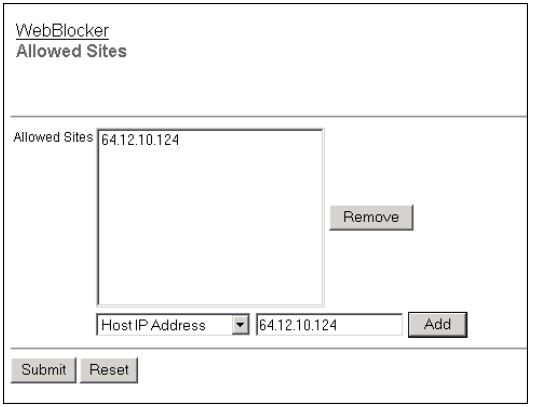
For example, employees in your company might have need to access Web sites that contain medical information. Some of these sites might be forbidden by WebBlocker because they could fall into the category of sex education. You can override the WebBlocker setting by adding the site to the Allowed Sites list.

**NOTE**

This WebBlocker feature is applicable only for outbound requests to access Web sites. You cannot use WebBlocker exceptions to make an internal host exempt from WebBlocker rules.

1 From the navigation bar on the left, select **WebBlocker ⇒ Allowed Sites**.
The WebBlocker Allowed Sites page appears.

2 From the drop-down list at the lower-left portion of the page, select whether the address or addresses you specify are a host IP address, network IP address, or host range.




3 In the box to the right of the drop-down list, type the host or network IP address of the allowed site. If you specified a range, type the start and end point of the range. Click **Add**.

4 Repeat for other allowed sites. When you are done adding sites, click **Submit**.

To remove an item from the list, select the address. Click **Remove**.

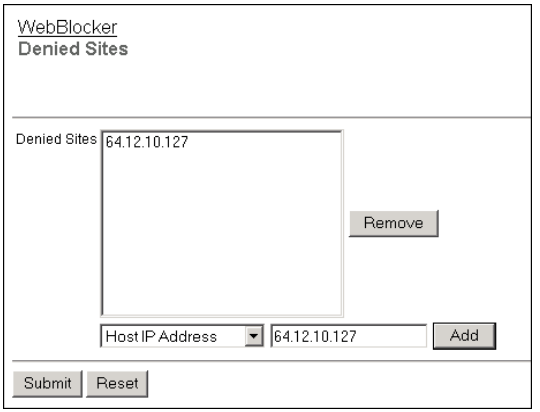
## Blocking Additional Web Sites

You might want to keep your users from viewing certain sites even if WebBlocker allows them. For example, you may receive a LiveSecurity® Service alert telling you that a certain commonly used Web site

is corrupted with hacker code. Using the Denied Sites feature, you can make sure your employees do not access this site.

1 From the navigation bar on the left, select **WebBlocker** ⇒ **Denied Sites**.
The WebBlocker Denied Sites page appears.

2 From the drop-down list at the lower-left portion of the page, select whether the address or addresses you specify are the host IP address, network IP address, or host range.




3 In the box to the right of the drop-down list, type the host or network IP address of the denied site. If you specified a range, type the start and end point of the range. Click **Add**.

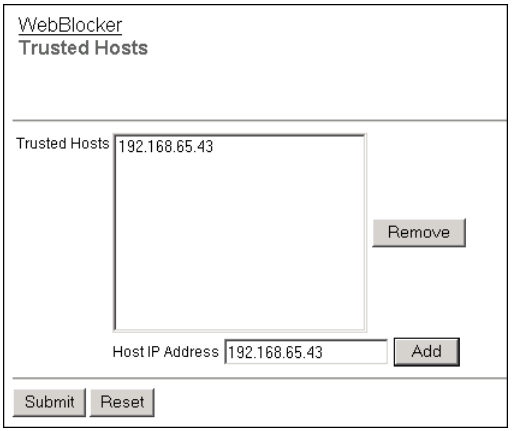
4 Repeat for other denied sites. When you are done adding sites, click **Submit**.

To remove an item from the list, select the address. Click **Remove**.

# Allowing Internal Hosts to Bypass WebBlocker

You can define a list of internal hosts that bypass WebBlocker settings:

1 From the navigation bar on the left, select **WebBlocker** ⇒ **Trusted Hosts**.
The WebBlocker Trusted Hosts page appears.




2 In the text box at the bottom of the page, type the host IP address of the site you want to allow. Click **Add**.

3 Repeat for other allowed hosts. When you are done adding hosts, click **Submit**.

To remove an item from the list, select the address. Click **Remove**.

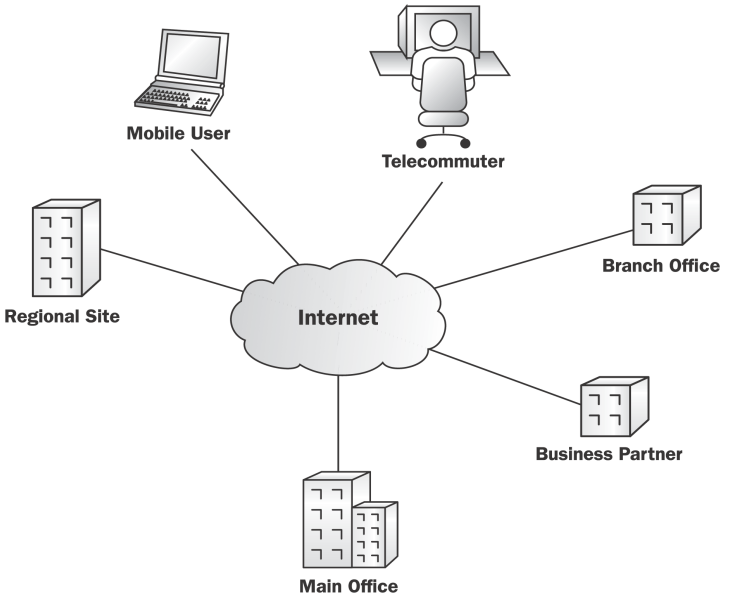
CHAPTER 8

# Configuring Virtual Private Networks

A *virtual private network* (VPN) allows secure connections between computers or networks in separate physical locations. The networks and hosts at the endpoints of a VPN are typically corporate headquarters, branch offices, remote users, telecommuters, and traveling employees. User authentication verifies the identity of both the sender and the receiver. Data sent by way of the Internet is encrypted such that only the sender and the receiver of the message can see it in a clearly readable state.

## What You Need to Create a VPN

- Two properly configured and working Firebox® X Edges or one Firebox X Edge and another IPSec-compliant device such as a Firebox X. Each Firebox X Edge must have the VPN option enabled.




- The static IP address of each Firebox X Edge external interface, the network address of the private (trusted) network located behind each Firebox X Edge (the networks that will communicate through the VPN), and their subnet masks. The base trusted IP address of each Firebox X Edge must be static and unique.
- The DNS and WINS server IP addresses, if used.
- The shared key (passphrase) for the tunnel. The same shared key must be used by both devices.
- The same encryption method for each end of the tunnel (DES or 3DES).
- The same authentication method for each end (MD-5 or SHA-1).

**NOTE**

The trusted networks at either end of the VPN tunnel must have different network addresses.

If the devices that connect through the VPN tunnel are not configured correctly, the VPN tunnel will not function.

## Special considerations

Consider these points before you configure your WatchGuard Firebox X Edge VPN network:

- You can connect a maximum of 10 Firebox X Edge appliances together in a star configuration. To configure more VPN tunnels, a WatchGuard Firebox III or Firebox X with WatchGuard VPN Manager is necessary.
- WatchGuard recommends that both of the VPN appliances have a static IP address. Configuring a VPN tunnel between two appliances using dynamic IP addresses, can pose several problems. See “Network addressing” on page 5 for more information about dynamic IP addresses. However, these issues can be resolved by using Dynamic DNS. For information on configuring the Dynamic DNS feature, see “Registering with the Dynamic DNS Service” on page 59.
- Both appliances must use the same encryption method: either DES or 3DES.
- When two Microsoft Windows NT networks are connected, the two networks must be in the same Microsoft Windows domain or be trusted domains. This is a Microsoft Networking design implementation and not a limitation of the Firebox X Edge.

WatchGuard recommends that you make a record of the configuration information in the following format.

### Sample VPN Address Information Table

| Item | Description | Assigned By |
|---|---|---|
| External IP Address | The IP address that identifies the IPSec-compatible device to the Internet.<br><br>Site A: 207.168.55.2<br>Site B: 68.130.44.15 | ISP |
| External Subnet Mask | The bitmask that shows which part of the IP address identifies the local network. For example, a class C address includes 256 addresses and has a netmask of 255.255.255.0.(Only 254 of the IP addresses in that subnet can be assigned to computers.)<br><br>Site A: 255.255.255.0<br>Site B: 255.255.255.0 | ISP |
| Local Network Address | An address used to identify a local network. A local network address cannot be used as an external IP address. WatchGuard recommends that you use an address from one of the reserved ranges:<br>10.0.0.0/8—255.0.0.0<br>172.16.0.0/12—255.240.0.0<br>192.168.0.0/16—255.255.0.0<br>The numbers after the slashes indicate the subnet masks. /24 means that the subnet mask for the trusted network is 255.255.255.0. For more information on entering IP addresses in slash notation, see the following FAQ:<br>https://www.watchguard.com/support/advancedfaqs/general_slash.asp<br><br>Site A: 192.168.111.0/24<br>Site B: 192.168.222.0/24 | You |
| Shared Secret | The shared secret is a passphrase used by two IPSec-compatible appliances to encrypt and decrypt the data that goes through the VPN tunnel. The two appliances use the same passphrase. If the appliances do not have the same passphrase, they cannot encrypt and decrypt the data correctly.<br>Use a passphrase that contains numbers, symbols, lowercase letters, and uppercase letters for better security. For example, “Gu4c4mo!3” is better than “guacamole”.<br><br>Site A: OurLittleSecret<br>Site B: OurLittleSecret | You |

| Item | Description | Assigned By |
|---|---|---|
| Encryption Method | DES uses 56-bit encryption. 3DES uses 168-bit encryption. The 3DES encryption method gives better security, but decreases the speed of communication. The two IPSec-compatible appliances must use the same encryption method.<br><br>Site A: 3DES<br>Site B: 3DES | You |
| Authentication | The two IPSec-compatible appliances must use the same authentication method.<br><br>Site A: MD5 (or SHA1)<br>Site B: MD5 (or SHA1) | You |

## Using a DVCP server to manage your VPN tunnels

Dynamic VPN Configuration Protocol (DVCP) is the WatchGuard-proprietary protocol that easily creates IPSec tunnels. With managed VPN tunnels, all information for the tunnel settings is stored on the DVCP server. This reduces the load on the administrator because he or she does not need to manually set up tunnels.

You can only use a Firebox III or Firebox X model as a DVCP server. Your Firebox X Edge can be a DVCP client to let you easily manage its VPN tunnels. There are two kinds of DVCP server:

- Basic DVCP - All Firebox III and Firebox X models
- VPN Manager - Firebox III 1000 or above, Firebox X700 or above

For more information, see the FAQ:

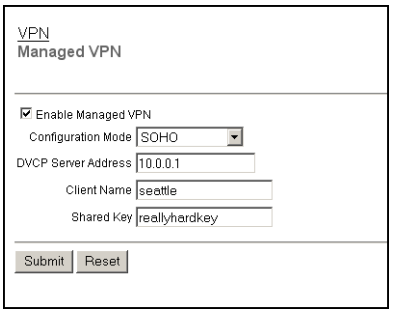
https://www.watchguard.com/support/advancedFAQs/basicdvcp_whatis.asp

## Setting up management for a dynamic Edge device

This procedure is necessary for Edge devices with a dynamic external IP address.

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
The default IP address is: https://192.168.111.1.

2 From the navigation bar at left, select **VPN ⇒ Managed VPN**.
The Managed VPN page appears.




3 Select the **Enable Managed VPN** checkbox.

4 Enter the IP address of the DVCP server.

5 Enter the client name and the shared key. If you have a Basic DVCP server, use the Client Name. If you have a VPN Manager DVCP server, use the Host Name.

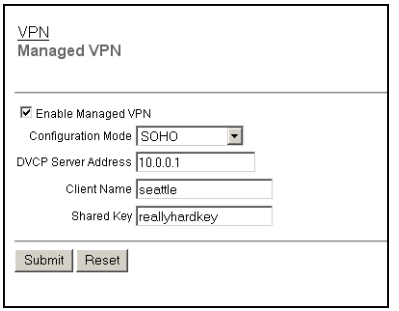
6 Click **Submit**.

## Setting up management for a static Edge device

If you use a Basic DVCP server and the Firebox X Edge external interface uses a static IP address, you must use this procedure:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
The default IP address is: https://192.168.111.1.

2 From the navigation bar at left, select **VPN ⇒Managed VPN**.
The Managed VPN page appears.




3 Select the **Enable Managed VPN** checkbox.

4 Enter the IP address of the DVCP server.

5 Enter the client name and the shared key. Use the Client Name you entered on the Basic DVCP server.

6 Click **Submit**.

## Setting Up Manual VPN Tunnels

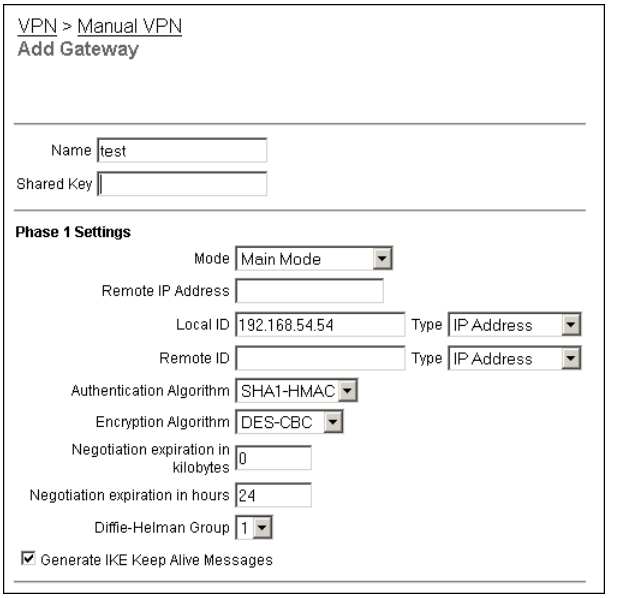
An administrator of a Firebox® X Edge can configure a maximum of 10 VPN tunnels to other Firebox X Edge devices. The VPN Manager software can configure a larger number of Firebox X Edge to Firebox X Edge tunnels.

To define VPN tunnels to other Firebox X Edge devices, follow these steps:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
The default IP address is: https://192.168.111.1.

2 From the navigation bar at left, select **VPN ⇒Manual VPN**.
The Manual VPN page appears.

3 Click **Add**.
The Add Gateway page appears.




4 Type the **Name** and **Shared Key** for the VPN tunnel.

The shared key is a passphrase used by two IPSec-compatible appliances to encrypt and decrypt the data that goes through the VPN tunnel. The two appliances use the same passphrase. If the appliances do not have the same passphrase, they cannot encrypt and decrypt the data correctly.

## Phase 1 settings

Internet Key Exchange (IKE) is a protocol used with VPNs that automates the process of negotiating keys, changing keys, and determining when to change keys. Phase 1, the first stage in the IKE negotiation, authenticates the two parties and sets up a key management security association for protecting the data.

The default Phase 1 settings are the same for all Firebox X devices. These settings are commonly left in their default values.

To modify Phase 1 settings, complete the following steps:

**NOTE**

The Phase 1 settings must be the same on both devices.

1 Select the negotiation mode for Phase 1 from the drop-down list. The mode selections are **Main Mode** and **Aggressive Mode**. If the external IP address is dynamic, select **Aggressive Mode**. If the external IP address is static, use either mode.

2 If you chose Main Mode, enter the remote IP address in the field provided.

3 Select the **Local ID** type and the **Remote ID** type from the drop-down list. These must match the settings used on the remote gateway.

- If you select **Main Mode**, the **Local ID** type and the **Remote ID** type must contain IP addresses.
- If you select **Aggressive Mode**, the **Remote ID** type can be an IP address or a domain name. If your external IP address is static, the **Local ID** type must be an IP address. If your external IP address is dynamic, the **Local ID** type can be either a domain name or an IP address.

4 From the **Authentication Algorithm** drop-down list, select the type of authentication.
The options are MD5-HMAC (128-bit authentication) or SHA1-HMAC (160-bit authentication).

5 From the **Encryption Algorithm** drop-down list, select the type of encryption.
The options are DES-CBC or 3DES-CBC.

6 Type the number of kilobytes and the number of hours until negotiation expiration in the applicable fields.

7 From the **Diffie-Hellman Group** drop-down list, select the group number. WatchGuard supports group 1 and group 2.
Diffie-Hellman is a mathematical technique used to securely negotiate secret keys through a public network. Diffie-Hellman groups are collections of parameters used to achieve this. Group 2 is more secure than group 1, but more time is required to calculate group 2 secret keys.

8 Select the **Generate IKE Keep Alive Messages** checkbox to help detect when the tunnel is down.
Short packets are sent across the VPN tunnel at regular intervals to see if the other side agrees that valid Phase 1 security still exists. If the Keep Alive packets elicit no response three times in a row, the Firebox X Edge does a rekey to open the tunnel again.

**NOTE**

The IKE Keep Alive feature is different from the VPN Keep Alive feature described in"VPN Keep Alive," on page 103.

## Phase 2 settings

Phase 2 negotiates data management security association, which uses the data management policy to set up IPSec tunnels in the kernel for encapsulating and decapsulating data packets.

Use the default Phase 2 settings, or change the Phase 2 settings as shown below:

**NOTE**

Make sure that the Phase 2 settings are the same on both appliances.

1 From the **Authentication Algorithm** drop-down list, select the type of authentication.

2 From the **Encryption Algorithm** drop-down list, select the type of encryption.

3 Select the **Enable Perfect Forward Secrecy** checkbox, if necessary.

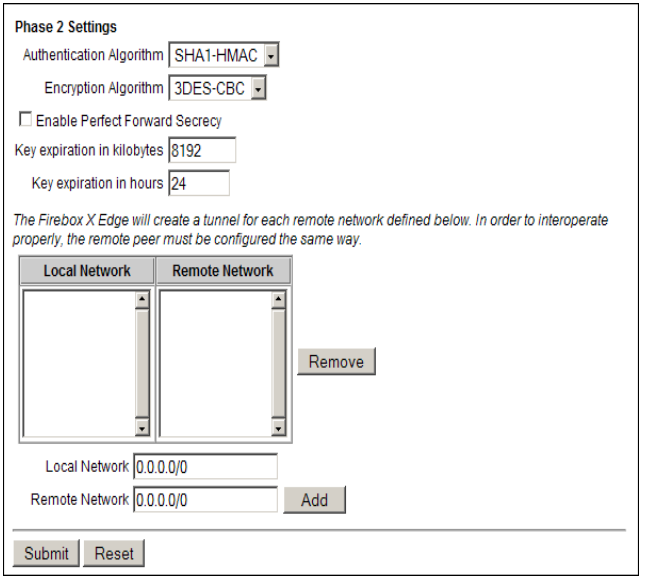
When this option is selected, each new key that is negotiated is derived by a new Diffie-Hellman exchange instead of from only one Diffie-Hellman exchange. This option gives more security, but increases the time necessary for the communication because of the additional exchange.

4 Type the number of kilobytes and the number of hours until negotiation expiration in the applicable fields.

5 Type the IP address of the local network and the remote network that must use Phase 2 negotiation. Network addresses must be entered in "slash" notation (also known as Classless Inter Domain Routing or CIDR notation). For more information on entering IP addresses in slash notation, see the following FAQ: http://www.watchguard.com/support/advancedfaqs/general_slash.asp.

6 Click **Add**.

7 Click **Submit**.

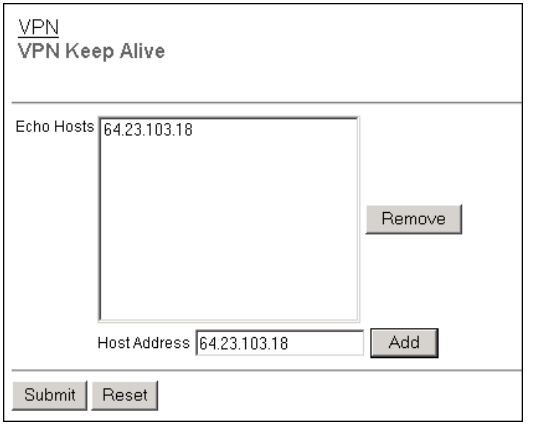



# VPN Keep Alive

To help keep the VPN tunnel open when there is no communication across it, enter the IP address of a computer at the other end of the tunnel as the echo host. The Firebox® X Edge will send a ping once a minute to the specified host. Choose a host IP address that will always be up, and always responds to ping messages. You can enter the trusted interface IP address of the Firebox X Edge (or the trusted interface IP address of the Firebox III or Firebox X) at the other end. Multiple IP addresses can be listed to cause the Firebox X Edge to ping hosts across different VPN tunnels.

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
The default IP address is: https://192.168.111.1

2 From the navigation bar at left, select **VPN ⇒Keep Alive.**
The VPN Keep Alive page appears.




3 Enter the IP address of an echo host. Click **Add.**

4 Click **Submit.**

## Viewing VPN Statistics

The Firebox® X Edge has a configuration page that displays VPN statistics. Use this page to monitor VPN traffic and to solve problems with the VPN configuration.

To view the VPN Statistics page:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
The default IP address is: https://192.168.111.1

2 From the navigation bar at left, select **VPN ⇒VPN Statistics.**
The VPN Statistics page appears.

## Frequently Asked Questions

### Why do I need a static external address?

To make a VPN connection, each of the appliances must know the IP address of the other appliance. If the addresses are dynamic, these

addresses can change. A changing address prevents a connection between the two appliances. However, this issue can be resolved by using Dynamic DNS. For information, see "Registering with the Dynamic DNS Service" on page 59.

### How do I get a static external IP address?

The external IP address for your computer or network is assigned by your ISP. Many ISPs use dynamic IP addresses so that their network is easier to configure and to make the connection of a Web server to their network more difficult. Most ISPs supply a static IP address as an optional service.

### How do I troubleshoot the connection?

If you can ping the trusted interface of the remote Firebox X Edge and the computers on the remote network, the VPN tunnel functions correctly. The configuration of the network software or the applications are possible causes of other problems.

### Why is ping not working?

If you cannot ping the local network address of the remote Firebox X Edge, follow these steps:

1 Ping the external address of the remote Firebox X Edge.

   For example, at Site A, ping 68.130.44.15 (Site B). If the ping does not come back, make sure the external network settings of Site B are correct. (Site B must be configured to respond to ping requests on that interface.) If the settings are correct, make sure that the computers at Site B have access to the Internet. If this procedure does not give a solution, talk to a service person at your ISP.

2 If you can ping the external address of each Firebox X Edge, try to ping a local address in the remote network.

   From Site A, ping 192.168.111.1. If the VPN tunnel functions correctly, the remote Firebox X Edge sends the ping back. If the ping does not come back, make sure the local settings are correct. Make sure that the local DHCP address ranges for the two networks connected by the VPN tunnel do not use any of the same IP addresses. The two networks connected by the tunnel must not use the same IP addresses.

### How do I obtain a VPN upgrade license key?

You can purchase a license key for an upgrade from a reseller or from the WatchGuard Web site:

http://www.watchguard.com/sales/buyonline.asp

### Is the Firebox X Edge compabtible with WatchGuard System Manager?

Yes. The default Firebox X Edge configuration is compatible with WatchGuard System Manager v7.3. To configure the Edge for use with WSM v7.0, v7.1, and v7.2, browse to the VPN Manager Access page. Check the Compatible with pre WFS v.3 VPN Manager.

CHAPTER 9

# Configuring the MUVPN Client

The MUVPN client is a software application that is installed on a remote computer. This application makes a secure connection from the remote computer to your protected network through an unsecured network. The MUVPN client uses Internet Protocol Security (IPSec) to guarantee the security of the connection.

The following is an example of how the MUVPN client can be used. First, the MUVPN client is installed on the remote computer. Then a connection to the Internet is established on the remote computer. The user starts the MUVPN client, which creates an encrypted tunnel to the Firebox X Edge. The Firebox X Edge connects the user to the trusted network. The employee now has remote access to the internal network and does not compromise the security of the network.

ZoneAlarm®, a personal firewall software application, is included as an optional feature with the MUVPN client. ZoneAlarm provides additional security for the remote users of your network by acting as a software firewall.

This chapter shows how to install and configure the MUVPN client on a remote computer. This chapter also includes information about the features of the ZoneAlarm personal firewall.

# Preparing Remote Computers to Use the MUVPN Client

The MUVPN client can be installed only on computers that meet the following requirements:

## System requirements

- A computer with a Pentium processor (or equivalent)
- Compatible operating systems and minimum RAM:
  - Microsoft Windows 98: 32 MB
  - Microsoft Windows ME: 64 MB
  - Microsoft Windows NT 4.0 Workstation: 32 MB
  - Microsoft Windows 2000 Professional: 64 MB
  - Microsoft Windows XP: 64 MB
- The latest service packs for each operating system are recommended, but not required
- 10 MB hard disk space
- Native Microsoft TCP/IP communications protocol
- Microsoft Internet Explorer 5.0 or later
- An Internet service provider account
- A dial-up or broadband (DSL or cable modem) connection

To use Windows file and print sharing through a MUVPN tunnel, the remote computer must be able to communicate with the WINS servers and the DNS servers. These servers are located on the trusted network that is protected by the Firebox X Edge. To communicate with these servers, the remote computer must have the proper Windows components installed and configured.

## Windows 98/ME setup

This section describes how to install and configure the network components that are required for the Windows 98/ME operating system. These components must be installed before the MUVPN client will function correctly on a Windows 98/ME computer.

### Configuring network names

From the Windows desktop:

1 Select **Start** ⇒ **Settings** ⇒ **Control Panel**.

2 Double-click the **Network** icon.
The Network window appears.

3 Make sure the Client for Microsoft Networks is installed.
The Client for Microsoft Networks must be installed before you continue with this procedure. For instructions, see "Installing the Client for Microsoft Networks" on page 109.

4 Click the **Identification** tab.

5 Type a name for the remote computer in the applicable field.
This name must be unique on the remote network.

6 Type the domain name for this connection in the applicable field.

7 Enter a description for the remote computer in the applicable field.
This step is optional.

8 Click **OK** to close the Network window.
Click Cancel if you do not want to save the changes.

9 Reboot the computer.

## Installing the Client for Microsoft Networks

The Client for Microsoft Networks must be installed before you can configure network names. If the Client for Microsoft Networks is not installed, follow these steps.

From the Network window:

1 Click the **Configuration** tab and then click **Add**.
The Select Network Component Type window appears.

2 Select **Client** and then click **Add**.
The Select Network Client window appears.

3 Select **Microsoft** from the list at left. Select **Client for Microsoft Networks** from the list at right and then click **OK**.

4 Select **Client for Microsoft Networks** and then click **Properties**.

5 Select the **Log on to Windows NT domain** checkbox.

6 Type the domain name in the **Windows NT Domain** text field.
Examples of typical domain names are "sales", "office", and "warehouse".

7 Select the **Logon and Restore Network Connections** checkbox.

## Installing Dial-Up Networking

Dial-Up Networking must be installed before the Mobile User VPN Adapter can be installed. If Dial-up Networking is not installed, follow these steps.

From the Windows desktop:

1 Select **Start** ⇒ **Settings** ⇒ **Control Panel**.

2 Double-click the **Add/Remove Programs** icon.
The Add/Remove Properties window appears.

3 Click the **Windows Setup** tab.
The Windows Setup dialog box appears. The operating system searches for installed components.

4 Select the **Communications** checkbox and then click **OK**.
The Copying Files dialog box appears. The operating system copies the necessary files.

5 The Dial-Up Networking Setup window appears. Click **OK** to restart the computer.
The computer reboots.

The Dial-up Networking component of Windows 98 must be updated with the 1.4 patch. This update is available from the Microsoft Web site.

### Configuring the WINS and DNS settings

The remote computer must be able to communicate with the WINS servers and the DNS servers. These servers are located on the trusted network that is protected by the Firebox X Edge.

From the Windows desktop:

1 Select **Start** ⇒ **Settings** ⇒ **Control Panel**.

2 Double-click the **Network** icon.
The Network window appears.

3 Select the network component **TCP/IP** ⇒ **Dial-Up Adapter** and then click **Properties**.
The TCP/IP Properties Information window appears.

4 Click **OK**.

5 Click the **DNS Configuration** tab and then select the **Enable DNS** checkbox.

6 Type the IP address of the DNS server in the **DNS Server Search Order** text field. Click **Add**.
If you have multiple remote DNS servers, repeat steps 5 and 6.

**NOTE**

The DNS server on the private network behind the Firebox X Edge must be the first server in the list.

7 Click the **WINS Configuration** tab and then select the **Enable WINS Resolution** checkbox.

8 Type the IP address of the WINS server in the **WINS Server Search Order** text field and then click **Add**.
If you have multiple remote WINS servers, repeat steps 7 and 8.

9 Click **OK** to close the TCP/IP Properties window. Click **OK** to close the Network window.
The System Settings Change dialog box appears.

10 Click **Yes** to restart the computer.
The computer reboots.

## Windows NT setup

This section describes how to install and configure the network components that are required for the Windows NT operating system. These components must be installed before the MUVPN client will function correctly on a Windows NT computer.

### Installing Remote Access Services on Windows NT

Remote Access Services (RAS) must be installed before the Mobile User VPN Adapter can be installed. If RAS is not installed, follow these steps.

Follow the Windows desktop:

1 Select **Start** ⇒ **Settings** ⇒ **Control Panel**.

2 Double-click the **Network** icon.
The Network window appears.

3 Click the **Services** tab and then click **Add**.

4 Select **Remote Access Services** from the list and then click **OK**.

5 Enter the path to the Windows NT install files or insert your system installation CD and then click **OK**.
The Remote Access Setup window appears.

6 Click **Yes** to add a RAS device, such as a modem, and then click **Add**.

7 Complete the Install New Modem wizard.

**NOTE**

If there is no modem installed, you can select the **Don't detect my modem; I will select it from a list** checkbox. Select the standard 28800 modem. To install RAS, Windows NT requires at least one RAS device, such as a modem, to be installed. If a

modem is not available, you can select **a serial cable between two computers**.

8 Select the modem added in the previous step from the Add RAS Device window.

9 Click **OK**, click **Continue** and then click **Close**.

10 Reboot the computer.

### Configuring the WINS and DNS settings

The remote computer must be able to communicate with the WINS servers and the DNS servers. These servers are located on the trusted network that is protected by the Firebox X Edge.

From the Windows desktop:

1 Select **Start ⇒ Settings ⇒ Control Panel**.

2 Double-click the **Network** icon.
The Network window appears.

3 Click the **Protocols** tab and then select the **TCP/IP** protocol.

4 Click **Properties**.
The Microsoft TCP/IP Properties window appears.

5 Click the **DNS** tab and then click **Add**.

6 Enter the IP address of your DNS server in the applicable field.
To add additional DNS servers, repeat steps 5 and 6.

**NOTE**

The DNS server on the private network behind the Firebox X Edge must be the first server in the list.

7 Click the **WINS Address** tab, type the IP address of your WINS server in the applicable field, and then click **OK**.
To add additional WINS servers, repeat this step.

8 Click **Close** to close the Network window.
The Network Settings Change dialog box appears.

9 Click **Yes** to restart the computer.
The computer reboots.

## Windows 2000 setup

This section describes how to install and configure the network components that are required for the Windows 2000 operating system. These components must be installed before the MUVPN client will function correctly on a Windows 2000 computer.

From the Windows desktop:

1 Select **Start** ⇒ **Settings** ⇒ **Network and Dial-up Connections**.

2 Select the dial-up connection you use to access the Internet.
The connection window appears.

3 Click **Properties** and then click the **Networking** tab.

4 Make sure the following components are installed and enabled:
- Internet Protocol (TCP/IP)
- File and Printer Sharing for Microsoft Networks
- Client for Microsoft Networks

### Installing the Internet Protocol (TCP/IP) network component

From the connection window, Networking tab:

1 Click **Install**.
The Select Network Component Type window appears.

2 Double-click the **Protocol** network component.
The Select Network Protocol window appears.

3 Select the **Internet Protocol (TCP/IP)** network protocol. Click **OK**.

### Installing the File and Printer Sharing for Microsoft Networks

From the connection window, Networking tab:

1 Click **Install**.
The Select Network Component Type window appears.

2 Double-click the **Services** network component.
The Select Network Service window appears.

3 Select the **File and Printer Sharing for Microsoft Networks** network service and then click **OK**.

### Installing the Client for Microsoft Networks

From the connection window, Networking tab:

1 Click **Install**.
The Select Network Component Type window appears.

2 Double-click the **Client** network component.
The Select Network Protocol window appears.

3 Select the **Client for Microsoft Networks** network client and then click **OK**.

### Configuring the WINS and DNS settings

The remote computer must be able to communicate with the WINS servers and the DNS servers. These servers are located on the trusted network that is protected by the Firebox X Edge.

From the connection window, Networking tab:

1 Select the **Internet Protocol (TCP/IP)** component and then click **Properties.**
The Internet Protocol (TCP/IP) Properties window appears.

2 Click **Advanced.**
The Advanced TCP/IP Settings window appears.

3 Click the **DNS** tab and then, from the section labeled **DNS server addresses, in order of use**, click **Add.**
The TCP/IP DNS Server window appears.

4 Enter the IP address of the DNS server in the applicable field and then click **Add.**
To add additional DNS servers, repeat steps 3 and 4.

**NOTE**

The DNS server on the private network behind the Firebox X Edge must be the first server in the list.

5 Select the **Append these DNS suffixes (in order)** checkbox and then click **Add.**
The TCP/IP Domain Suffix window appears.

6 Enter the domain suffix in the applicable field.
To add additional DNS suffixes, go back to step 5.

7 Click the **WINS** tab and then, from the section labeled **WINS addresses, in order of use**, click **Add.**
The TCP/IP WINS Server window appears.

8 Enter the IP address of the WINS server in the applicable field. Click **Add.**
To add additional WINS servers, repeat steps 7 and 8.

9 Click **OK** to close the Advanced TCP/IP Settings window, click **OK** to close the Internet Protocol (TCP/IP) Properties window, and then click **OK.**

10 Click **Cancel** to close the connection window.

## Windows XP setup

This section describes how to install and configure the network components that are required for the Windows XP operating system.

These components must be installed before the MUVPN Client will function correctly on a Windows XP computer.

From the Windows desktop:

1 Select **Start** ⇒ **Control Panel**
The Control Panel window appears.

2 Double-click the **Network Connections** icon.

3 Double-click the connection you use to access the Internet.
The connection window appears.

4 Click **Properties** and then click the **Networking** tab.

5 Make sure the following components are installed and enabled:
- Internet Protocol (TCP/IP)
- File and Printer Sharing for Microsoft Networks
- Client for Microsoft Networks

### Installing the Internet Protocol (TCP/IP) Network Component

From the connection window, Networking tab:

1 Click **Install**.
The Select Network Component Type window appears.

2 Double-click the **Protocol** network component.
The Select Network Protocol window appears.

3 Select the **Internet Protocol (TCP/IP)** network protocol. Click **OK**.

### Installing the File and Printer Sharing for Microsoft Networks

From the connection window, Networking tab:

1 Click **Install**.
The Select Network Component Type window appears.

2 Double-click the **Services** network component.
The Select Network Service window appears.

3 Select the **File and Printer Sharing for Microsoft Networks** network service. Click **OK**.

### Installing the Client for Microsoft Networks

From the connection window, Networking tab:

1 Click **Install**.
The Select Network Component Type window appears.

2 Double-click the **Client** network component.
The Select Network Protocol window appears.

3 Select the **Client for Microsoft Networks** network client. Click **OK**.

### Configuring the WINS and DNS settings

The remote computer must be able to communicate with the WINS servers and the DNS servers. These servers are located on the trusted network that is protected by the Firebox X Edge.

From the connection window, Networking tab:

1 Select the **Internet Protocol (TCP/IP)** component.

2 Click **Properties**.
The Internet Protocol (TCP/IP) Properties window appears.

3 Click **Advanced**.
The Advanced TCP/IP Settings window appears.

4 Click the **DNS** tab and then, from the section labeled **DNS server addresses, in order of use**, click **Add**.
The TCP/IP DNS Server window appears.

5 Enter the IP address of the DNS server in the applicable field. Click **Add**.
To add additional DNS servers, repeat steps 4 and 5.

**NOTE**

The DNS server on the private network behind the Firebox X Edge must be the first server in the list.

6 Select the **Append these DNS suffixes (in order)** checkbox. Click **Add**.
The TCP/IP Domain Suffix window appears.

7 Enter the domain suffix in the applicable field.
To add additional DNS suffixes, go back to step 6.

8 Click the **WINS** tab and then, from the section labeled **WINS addresses, in order of use**, click **Add**.
The TCP/IP WINS Server window appears.

9 Enter the IP address of the WINS server in the applicable field. Click **Add**.
To add additional WINS servers, repeat steps 8 and 9.

10 Click **OK** to close the Advanced TCP/IP Settings window, click **OK** to close the Internet Protocol (TCP/IP) Properties window, and then click **OK**.

11 Click **Cancel** to close the connection window.

# Installing and Configuring the MUVPN Client

The MUVPN installation files are available at the WatchGuard Web site:

http://www.watchguard.com/support

**NOTE**

To install and configure the MUVPN client, you must have local administrator rights on the remote computer.

## Installing the MUVPN client

Follow these steps to install the MUVPN client:

1 Copy the MUVPN installation file to the remote computer.

2 Double-click the MUVPN installation file to start the InstallShield wizard.

3 Click **Next**.
If the InstallShield stops because read-only files are detected, click **Yes** to continue the installation.

4 A welcome message is displayed. Click **Next**.
The Software License Agreement is displayed.

5 Click **Yes** to accept the terms of the License Agreement.
The Setup Type window appears.

6 Select the type of installation. WatchGuard recommends that you use the Typical installation. Click **Next**.

7 On a Windows 2000 computer, the InstallShield will detect the Windows 2000 L2TP component. If the component is installed, the InstallShield does not install it again. Click **OK** to continue.
The Select Components window appears.

8 Do not change the default selections. Click **Next**.
The Start Copying Files window appears.

9 Click **Next** to install the files.
When the `dni_vapmp` file is installed, a command prompt window appears. This is normal. When the file has been installed, the command prompt window will close and the process will continue.

10 When the InstallShield wizard is complete, click **Finish**.

11 The InstallShield wizard searches for a user profile file. Click **Next** to skip this step. The user profile file does not need to be installed.
An information dialog box appears.

12 Click **OK** to continue the installation.

13 The installation of the MUVPN client is complete. Make sure the option **Yes, I want to restart my computer now** is selected. Click **Finish**.
The computer reboots.

**NOTE**

The ZoneAlarm personal firewall may prevent the connection to the network after the computer is restarted. If this occurs, log on to the computer locally the first time after installation. For more information regarding ZoneAlarm, see "The ZoneAlarm Personal Firewall" on page 133.

## Configuring the MUVPN client

When the computer restarts, the WatchGuard Policy Import window opens. Click **Cancel**.

From the Windows desktop system tray:

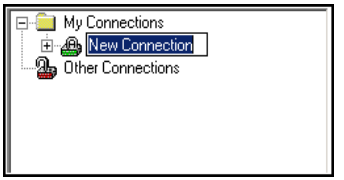
1 Right-click the MUVPN client icon and then select **Activate Security Policy**.

2 Double-click the MUVPN client icon.
The Security Policy Editor window appears.

**NOTE**

The ZoneAlarm personal firewall may display alert messages. For more information regarding ZoneAlarm see "The ZoneAlarm Personal Firewall" on page 133.

3 Select **Edit ⇒ Add ⇒ Connection**.
A new connection appears in the Network Security Policy field at left. The Connection Security, Remote Party Identity, and Addressing settings appear at right.

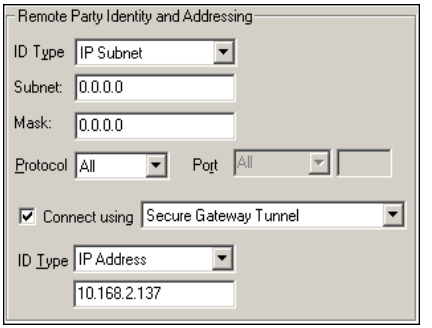


4 Type a unique name for the new connection.
If this will be a unique policy for a specific user, enter a unique name to identify the policy. For example, you may want to include the name of the user.

5 Select the **Secure** option.
This is the default setting.

6 Select the **Only Connect Manually** checkbox.

7 Select the **IP Subnet** option from the **ID Type** drop-down list.
The Remote Party Identity and Addressing fields are updated.




8 When you set the **Subnet** and **Mask** addresses, you define whether or not an MUVPN user accesses the Internet through the tunnel and therefore accesses the Internet through the tunnel. The checkbox **All traffic uses tunnel (0.0.0.0/0 IP Subnet)** as described in "Enabling MUVPN Access for a User Account" on page 127 must be set accordingly when configuring the MUVPN account in the Firebox X Edge setup. If the settings between the client and the Firebox X Edge do not match, the VPN connection will fail.

If you want to access only the trusted network through the tunnel, type the trusted network address in both the **Subnet** and **Mask** fields. The checkbox **All traffic uses tunnel (0.0.0.0/0 IP Subnet)** must not be selected if the client will only send traffic destined for the Firebox X Edge trusted network for through the VPN connection.

If you want to access both the trusted network and the Internet, type 0.0.0.0 in both the **Subnet** and **Mask** fields. The checkbox **All traffic uses tunnel (0.0.0.0/0 IP Subnet)** must be selected if all traffic will be sent from the MUVPN client through the VPN.

Using this option also allows the MUVPN client to access any networks across a VPN that the Firebox X Edge has constructed to another office.

**NOTE**

The addresses you type in the Subnet and Mask fields must be identical to the virtual IP address you typed on the Add MUVPN Client page. See "Preparing Remote Computers to Use the MUVPN Client" on page 108.

9 Select **All** from the **Protocol** drop-down list.
This is the default setting.

10 Select the **Connect using** checkbox and then select **Secure Gateway Tunnel** from the **Connect using** drop-down list.

11 If the Firebox X Edge external interface has a static public address, select **IP Address** from the **ID Type** drop-down list and then type the IP address of the external interface in the applicable field.

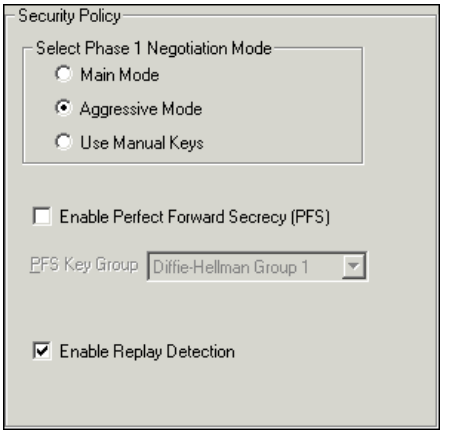
If the Firebox X Edge external public IP address is dynamically assigned and the Firebox X Edge has dynamic DNS configured, select Any from the **ID Type** drop-down list, and then select **Gateway Hostname** in the new box that appears to the right. Enter the fully qualified domain name in the lower-right field.

## Defining the My Identity settings

To define the My Identity settings, follow these steps.

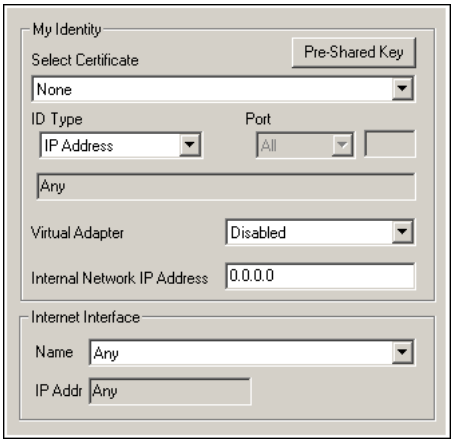
1 Expand the **Network Security Policy** to display the new entry.
The My Identity and Security Policy entries appear.


2 Select **Security Policy**.
The Security Policy dialog box appears.

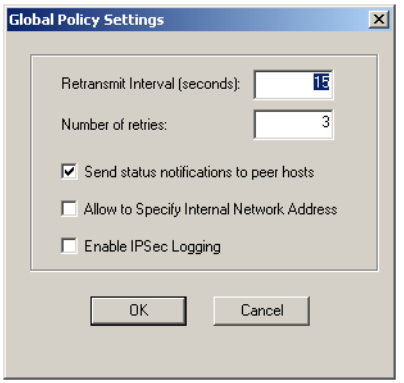



3 Select **Aggressive Mode.** Make sure the **Enable Perfect Forward Secrecy (PFS)** checkbox is clear and the **Enable Replay Detection** checkbox is selected.

4 Select **My Identity.**
The My Identity and Internet Interface settings appear to the right.

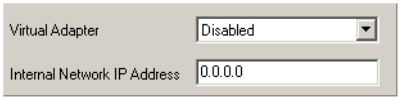



5 Select **Options ⇒ Global Policy Settings.**
The Global Policy Settings window appears.




6 Clear the **Allow to Specify Internal Network Address** checkbox. Click **OK**.

It is not necessary to specify the MUVPN client's internal IP address. The Firebox X Edge assigns this address automatically. Because setting the internal address improperly causes the VPN to fail, clearing this checkbox prevents that possible error by making it impossible to set the internal IP address.




7 Select **None** from the **Select Certificate** drop-down list.

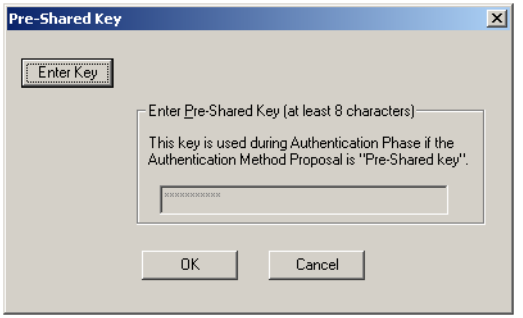
8 Select **E-mail Address** from the **ID Type** drop-down list and then enter the user name defined on the Firebox X Edge in the applicable field.

9 Select **Disabled** from the **Virtual Adapter** drop-down list if the Firebox X Edge will not assign private WINS and DNS Server IP addresses to the MUVPN client. Select **Preferred** or **Required** if the Firebox X Edge will assign the client private WINS and DNS Server IP addresses automatically.

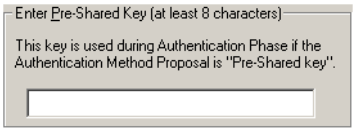
Preferred means that if the connection launch using the virtual adapter fails, the VPN can still be constructed using address substitution instead. (In this case, no WINS or DNS address will be assigned but the tunnel can still build.) Required means that if the client computer cannot create the virtual adapter for some reason, the connection will fail. (This is rare and usually indicates a problem with the client's IP networking stack, or an incompatibility with another IPSec client software previously installed).

10 Select **Any** from the **Name** drop-down list.
This is the default setting.

11 Click **Pre-Shared Key.**
The Pre-Shared Key dialog box appears.




12 Click **Enter Key.**
The text field is enabled.




13 Type the exact text of the MUVPN client passphrase entered on the Firebox X Edge. Click **OK.**

**NOTE**

Both the pre-shared key and the e-mail address must exactly match the system passphrase and system administrator name settings of the Firebox X Edge. If they do not match, the connection will fail. Normally, the pre-shared key and e-mail address must match the user name and shared key specified in the MUVPN account setup on the Firebox X Edge as described in "Enabling MUVPN Access for a User Account" on page 127.

## Defining Phase 1 and Phase 2 settings

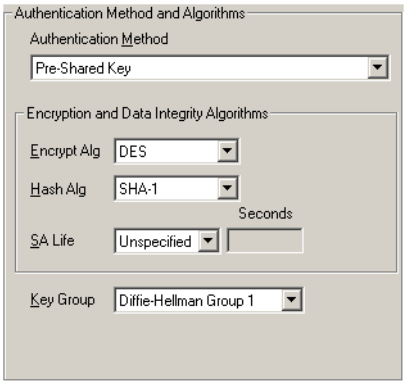
Follow these steps to define the Phase 1 and Phase 2 settings. Phase 1 settings for MUVPN clients are not configurable on the Firebox X

Edge and must match exactly as described below. Phase 2 settings must match the settings of the Firebox X Edge.

1 From the **Network Security Policy** field, expand **Security Policy**.
Both Phase 1 and Phase 2 negotiations appear.


2 Expand **Authentication (Phase 1)**.
A Proposal entry appears.

3 Select **Proposal 1**.
The Authentication Method and Algorithms settings appear to the right.




4 Select **Pre-Shared** Key from the **Authentication Method** drop-down list.

**NOTE**

Phase 1 values must be as specified in the following steps. Phase 2 values must match the settings of the Firebox X Edge.

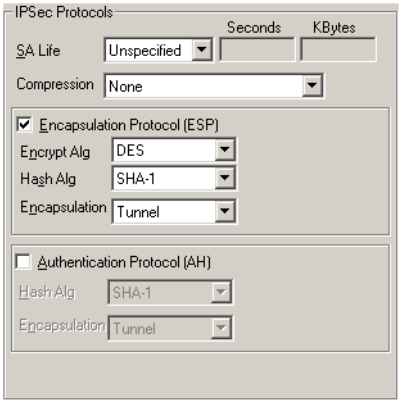
5 Select **DES** from the **Encrypt Alg** drop-down list and then select **SHA-1** from the **Hash Alg** drop-down list.

6 Select **Unspecified** from the **SA Life** drop-down list.
This is the default setting.

7 Select **Diffie-Hellman Group 1** from the **Key Group** drop-down list.

8 Expand **Key Exchange (Phase 2)**.
A Proposal entry appears.

9 Select **Proposal 1**.
The IPSec Protocols settings appear to the right.




10 Select **Both** from the **SA Life** drop-down list.

11 Type `86400` in the **Seconds** field and `8192` in the **KBytes** field.

12 Select **None** from the **Compression** drop-down list.
This is the default setting. The Firebox X Edge does not support compression.

13 Select the **Encapsulation Protocol (ESP)** checkbox.

14 Select a value for the **Encrypt Alg** and **Hash Alg** drop-down lists.

**NOTE**

The encrypted and hash values must match the settings of the Firebox X Edge. If the settings do not match, the connection will fail.

15 Select **Tunnel** from the **Encapsulation** drop-down list.
This is the default setting.

16 Make sure the **Authentication Protocol (AH)** checkbox is not selected.

17 Select **File ⇒Save** or click the button shown at the right. 

## Uninstalling the MUVPN client

Follow these directions to uninstall the MUVPN client. WatchGuard recommends that you use the Windows Add/Remove Programs tool.

Disconnect all existing tunnels and dial-up connections. Reboot the remote computer. Perform these steps from the Windows desktop:

1 Select **Start** ⇒ **Settings** ⇒ **Control Panel.**
The Control Panel window appears.

2 Double-click the **Add/Remove Programs** icon.
The Add/Remove Programs window appears.

3 Select **Mobile User VPN** and then click **Change/Remove**.
The InstallShield wizard appears.

4 Select **Remove**. Click **Next.**
The Confirm File Deletion dialog box appears.

5 Click **OK** to remove all of the components.
When the `dni_vapmp` file is removed, a command prompt window appears. This is normal. When the file has been removed, the command prompt window will close and the process will continue.
The Uninstall Security Policy dialog box appears.

6 Click **Yes** to delete the Security Policy Personal Certificates and the Private/Public Keys.
The InstallShield Wizard window appears.

7 Select the **Yes, I want to restart my computer now.** Click the **Finish** option.
The computer reboots.

**NOTE**

The ZoneAlarm personal firewall settings are stored in the following directories by default.

Windows 98: `c:\windows\internet logs\`
Windows NT and 2000: `c:\winnt\internet logs\`
Windows XP: `c:\windows\internet logs`

To remove these settings, delete the contents of the appropriate directory.

8 When the computer has restarted, select **Start** ⇒ **Programs**.

9 Right-click **Mobile User VPN** and select **Delete** to remove this selection from your **Start** menu.

# Enabling MUVPN Access for a User Account

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
The default trusted IP address is https://192.168.111.1.

2 Add a new user or edit an existing user, as described in “Adding or Editing a User Account” on page 143.

3 Click the **MUVPN** tab.

4 Select the **Enable MUVPN for this account** checkbox.

5 Type a shared key in the applicable field.

6 Type the virtual IP address in the applicable field.
The virual IP address must be an address from the Firebox X Edge's trusted network that will not be used by any other computer behind the Firebox. This address is used by the remote computer to connect to the Firebox X Edge.

7 From the **Authentication Algorithm** drop-down list, select the type of authentication.
The options are MD5-HMAC and SHA1-HMAC.

8 From the **Encryption Algorithm** drop-down list, select the type of encryption.
The options are DES-CBC and 3DES-CBC.

9 Set MUVPN key expiration in either kilobytes or hours. The default values are 8192 KB and 24 hours, respectively.

10 Select **Mobile User** from the **VPN Client Type** drop-down list.

11 Select the **All traffic uses tunnel (0.0.0.0/0 IP Subnet)** checkbox only if you want the remote client to send all its traffic (including normal Web serving) through the VPN to the Firebox X Edge. This allows the MUVPN client to communicate with networks across a VPN that the Firebox X Edge has constructed to another office. Note that if this checkbox is selected, the MUVPN client software must be configured accordingly with the subnet and mask fields set to 0.0.0.0. For more information, see “Configuring the MUVPN client” on page 118.

12 Click **Submit**.

# Configuring the Firebox for MUVPN Clients Using Pocket PC

To create a MUVPN tunnel between the Firebox X Edge and your Pocket PC, you must configure the MUVPN Clients feature on the Firebox. Follow the previous procedure, except select **Pocket PC** from the **VPN Client Type** drop-down list.

For additional information about configuring your Pocket PC to serve as an MUVPN client, go to the WatchGuard Web site:

https://www.watchguard.com/support/sohoresources/soinstallhelp.asp

# Connecting and Disconnecting the MUVPN Client

The MUVPN client software makes a secure connection from a remote computer to your protected network through the Internet. To establish this connection, you must connect to the Internet and use the MUVPN client to connect to the protected network.

## Connecting the MUVPN client

1 Connect to the Internet through a Dial-Up Networking connection, a LAN connection, or a WAN connection.

From the Windows desktop system tray:

2 If the MUVPN client is not active, right-click the icon and select **Activate Security Policy**.

For information about how to determine the status of the MUVPN icon, see "The MUVPN client icon" on page 128.

From the Windows desktop:

3 Select **Start** ⇒ **Programs** ⇒ **Mobile User VPN** ⇒ **Connect**.
The WatchGuard Mobile User Connect window appears.

4 Click **Yes**.

## The MUVPN client icon

The MUVPN icon appears in the Windows desktop system tray. The icon image provides information about the status of the connection.

**Deactivated**

The MUVPN Security Policy is deactivated. This icon may appear if the Windows operating system did not start a required MUVPN service. If this occurs, the remote computer must be restarted. If the problem continues, reinstall the MUVPN client.

**Activated**

The MUVPN client is ready to establish a secure, MUVPN tunnel connection.

**Activated and Transmitting Unsecured Data**

The MUVPN client is ready to establish a secure, MUVPN tunnel connection. The red bar on the right of the icon indicates that the client is transmitting unsecured data.

**Activated and Connected**

The MUVPN client has established at least one secure, MUVPN tunnel connection, but is not transmitting data.

**Activated, Connected and Transmitting Unsecured Data**

The MUVPN client has established at least one secure, MUVPN tunnel connection. The red bar on the right of the icon indicates that the client is only transmitting unsecured data.

**Activated, Connected and Transmitting Secured Data**

The MUVPN client has established at least one secure, MUVPN tunnel connection. The green bar on the right of the icon indicates that the client is only transmitting secured data.

**Activated, Connected and Transmitting both Secured and Unsecured Data**

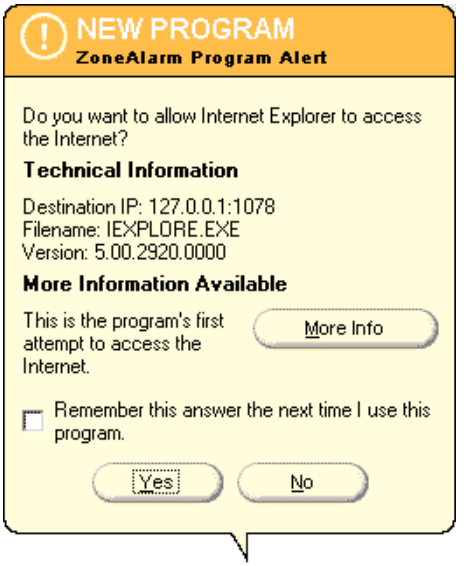
The MUVPN client has established at least one secure, MUVPN tunnel connection. The red and green bars on the right of the icon indicate that the client is transmitting both secured and unsecured data.

## Allowing the MUVPN client through a personal firewall

The following programs are associated with the MUVPN client. To establish the MUVPN tunnel, you must allow these programs through the personal firewall:

- MuvpnConnect.exe
- IreIKE.exe

The personal firewall detects when these programs attempt to access the Internet. A New Program alert window appears to request access for the MuvpnConnect.exe program.



From the New Program alert window:

1 Select the **Remember this answer the next time I use this program** checkbox and the click **Yes**.
With the option selected, the ZoneAlarm personal firewall will allow this program to access the Internet each time you attempt to make a MUVPN connection.
The New Program alert window appears to request access for the IreIKE.exe program.

2 Set the **Remember this answer the next time I use this program** check box and then click **Yes**.
With the option selected, the ZoneAlarm personal firewall will allow this program to access the Internet each time you attempt to make a MUVPN connection.

### Disconnecting the MUVPN client

From the Windows desktop system tray:

1 Right-click the MUVPN client icon and then select **Deactivate Security Policy**.
The MUVPN client icon with a red bar is displayed to indicate that the transmitted data is not secure.

If the ZoneAlarm personal firewall is active, deactivate it now.

From the Windows desktop system tray:

1 Right-click the ZoneAlarm icon shown at right. 

2 Select **Shutdown ZoneAlarm**.
The ZoneAlarm window appears.

3 Click **Yes**.

## Monitoring the MUVPN Client Connection

The Log Viewer and the Connection Monitor are installed with the MUVPN client. These tools can be used to monitor the MUVPN connection and to diagnose problems that may occur.

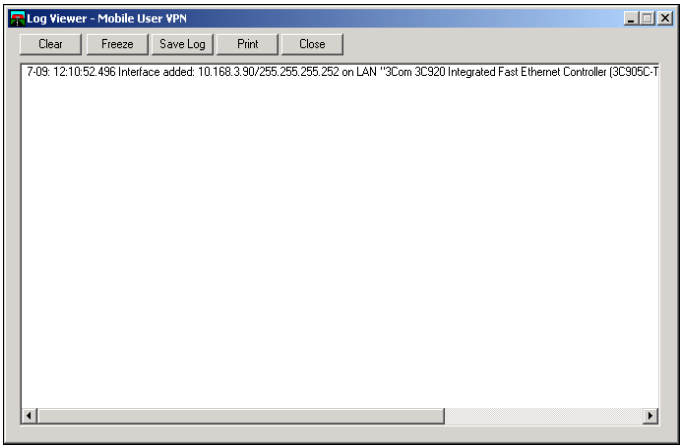
### Using Log Viewer

The Log Viewer displays the communications log. This log shows the events that occurred during the connection of the MUVPN tunnel.

From the Windows desktop system tray:

1 Right-click the **Mobile User VPN** client icon.

2 Select **Log Viewer.**
The Log Viewer window appears.




## Using Connection Monitor

The Connection Monitor displays statistical and diagnostic information for each active connection in the security policy. This display shows the security policy settings and the security association (SA) information. The displayed information is determined during the phase 1 IKE negotiations and the phase 2 IPSec negotiations.

From the Windows desktop system tray:

1 Right-click the **Mobile User VPN** client icon.

2 Select **Connection Monitor.**
The Connection Monitor window appears.

An icon appears to the left of the connection name:

- SA indicates that the connection only has a phase 1 SA. A phase 1 SA is assigned in the following situations:
  - for a connection to a secure gateway tunnel
  - when a phase 2 SA connection has not yet been made
  - when a phase 2 SA connection cannot be made
- A key indicates that the connection has a phase 2 SA. This connection may also have a phase 1 SA.

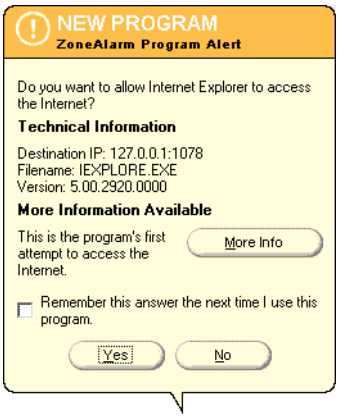
- An animated black line underneath a key indicates that the client is processing secure IP traffic for the connection.
- A single SA icon with several key icons above it indicates a single phase 1 SA to a gateway that protects multiple phase 2 SAs.

## The ZoneAlarm Personal Firewall

A personal firewall is a barrier between your computer and the outside world. A computer is most vulnerable at the connection points. These connection points are called ports. Without ports, your computer cannot connect to the Internet. For more information about ports, see “Ports” on page 7.

ZoneAlarm protects these ports by following a simple rule: Block all incoming and outgoing traffic unless you explicitly allow that traffic for trusted programs.

When you use ZoneAlarm you often see New Program alert windows similar to the following image.



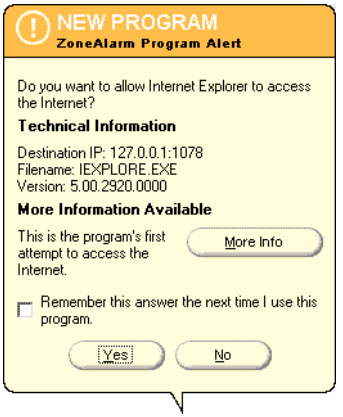

This alert appears whenever one of your programs attempts to access the Internet or your local network. This alert ensures that no information leaves your computer without your authorization.

The ZoneAlarm personal firewall provides a brief tutorial after the MUVPN client is installed. Follow the tutorial to learn how to use this program.

For more information about the features and configuration of ZoneAlarm, refer to the ZoneAlarm help system. To access the help system, select **Start ⇒Programs ⇒Zone Labs ⇒ZoneAlarm Help**.

## Allowing traffic through ZoneAlarm

When an application requires access through the ZoneAlarm personal firewall, a New Program alert will be displayed on the Windows desktop. This alert tells the user which program requires access. The name of the program may not clearly indicate which application requires access.




In the example above, the Internet Explorer Web browser application has been launched. The application attempts to access the user's home page. The program that actually needs to pass through the firewall is "IEXPLORE.EXE".

To allow this program access to the Internet each time the application is started, select the **Remember the answer each time I use this program** checkbox.

Here is a list of some programs that need to pass through the ZoneAlarm personal firewall when you use their associated applications.

| | | |
|---|---|---|
| **Programs That Must Be Allowed** | | |
| | MUVPN client | IreIKE.exe<br>MuvpnConnect.exe |
| | MUVPN Connection Monitor | CmonApp.exe |
| | MUVPN Log Viewer | ViewLog.exe |
| **Programs That May be Allowed** | | |
| | MS Outlook | OUTLOOK.exe |
| | MS Internet Explorer | IEXPLORE.exe |
| | Netscape 6.1 | netscp6.exe |
| | Opera Web browser | Opera.exe |
| | Standard Windows network applications | lsass.exe<br>services.exe<br>svchost.exe<br>winlogon.exe |

## Shutting down ZoneAlarm

From the Windows desktop system tray:

1. Right-click the ZoneAlarm icon shown at right. 
2. Select **Shutdown ZoneAlarm.**
   The ZoneAlarm window appears.
3. Click **Yes.**

## Uninstalling ZoneAlarm

From the Windows desktop:

1. Select **Start** ⇒ **Programs** ⇒ **Zone Labs** ⇒ **Uninstall ZoneAlarm.**
   The Confirm Uninstall dialog box appears.
2. Click **Yes.**
   The ZoneLabs TrueVector service dialog box appears.
3. Click **Yes.**
   The Select Uninstall Method window appears.
4. Make sure **Automatic** is selected and then click **Next.**
5. Click **Finish.**

**NOTE**

The Remove Shared Component window may appear. During the initial installation of ZoneAlarm, some files were installed that

could be shared by other programs on the system. Click **Yes to All** to completely remove all of these files.

6 The Install window appears and prompts you to restart the computer. Click **OK** to reboot your system.

## Troubleshooting Tips

Additional information about how to configure the MUVPN client is available from the WatchGuard Web site:

www.watchguard.com/support

The answers to several frequently asked questions about the MUVPN client are answered below.

### My computer hangs immediately after installing the MUVPN client...

This problem may be caused by one of the following two problems:

- The ZoneAlarm personal firewall application is disrupting the normal traffic on the local network.
- The MUVPN client is active and is unsuccessfully attempting to create VPN tunnels.

When the MUVPN client is not in use, both ZoneAlarm and the MUVPN client should be deactivated.

From the Windows desktop system tray:

1 Reboot your computer.

1 Right-click the MUVPN client icon and then select **Deactivate Security Policy**.
The MUVPN client icon with a red bar is displayed to indicate that the Security Policy has been deactivated.

1 Right-click the ZoneAlarm icon shown at right. 

2 Select **Shutdown ZoneAlarm**.
The ZoneAlarm dialog box appears.

3 Click **Yes**.

### I have to enter my network login information even when I'm not connected to the network...

When you start your computer, you are prompted to enter your Windows network user name, password, and domain. It is very impor-

tant that you enter this information correctly, just as you would at the office. Windows stores the information for use by network adapters and network applications. Later, when you connect to your ISP and start the MUVPN client, your computer uses the stored information to connect to the company network.

### I am not prompted for my user name and password when I turn my computer on...

This is probably caused by the ZoneAlarm personal firewall application. This program is very good at what it does. ZoneAlarm keeps your computer secure from unauthorized incoming and outgoing traffic. Unfortunately, it may prevent your computer from broadcasting its network information. This prevents the transmission of the login information. Make sure you deactivate ZoneAlarm each time you disconnect the MUVPN connection.

### Is the MUVPN tunnel working?

The MUVPN client icon appears in the Windows desktop system tray once the application has been launched. The MUVPN client displays a key in the icon when the client is connected.

To test the connection, ping a computer on your company network.

- Select **Start** ⇒ **Run** and then type `ping` followed by the IP address of a computer on your company network.

### My mapped drives have a red X through them...

Windows 98/ME, NT, and 2000 verify and map network drives automatically when the computer starts. Because you cannot establish a remote session with the company network before the computer starts, this process fails. This causes a red X to appear on the drive icons. To correct this problem, establish a MUVPN tunnel and open the network drive. The red X for that drive should disappear.

### How do I map a network drive?

Due to a Windows operating system limitation, mapped network drives must be remapped when you work remotely. To remap a network drive from the Windows desktop:

1 Right-click **Network Neighborhood**.

2 Select **Map Network Drive**.
The Map Network Drive window appears.

3 Use the drop-down list to select a drive letter.
Select a drive from the drop-down list or type a network drive path.

4 Click **OK**.

The mapped drive appears in the My Computer window. Even if you select the **Reconnect at Logon** checkbox, the mapped drive will only appear the next time you start your computer if the computer is directly connected to the network.

### I am sometimes prompted for a password when I am browsing the company network...

Due to a Windows networking limitation, remote user virtual private networking products can allow access only to a single network domain. If your company has multiple networks connected together, you will only be able to browse your own domain. If you try to connect to other domains, a password prompt will appear. Unfortunately, even providing the correct information will not allow you to access these additional networks.

### It takes a *very* long time to shut down the computer after using the MUVPN client...

If you access a mapped network drive during an MUVPN session, the Windows operating system will wait for a signal from the network before the shutdown can be completed.

### I lost the connection to my ISP, and now I can't use the company network...

If your Internet connection is interrupted, the connection to the MUVPN tunnel may be lost. Follow the procedure to close the tunnel. Reconnect to the Internet. Restart the MUVPN client.

CHAPTER 10

# Managing the Firebox® X Edge

Firebox® X Edge provides a number of ways for you to manage your network and users, such as:

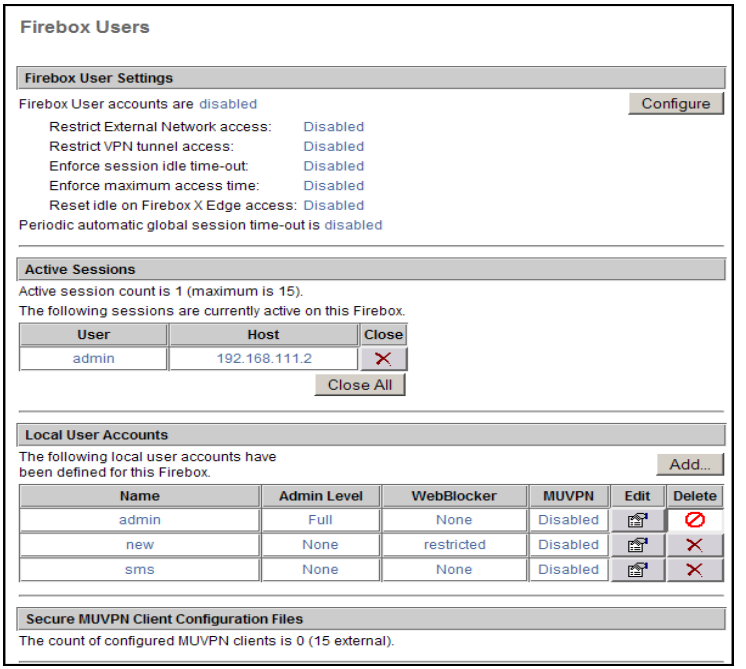
- Viewing current users and settings
- Configuring users and customizing individual user accounts
- Upgrading the Firebox
- Viewing the current configuration file in a text format

## Viewing Current Sessions and Users

A session is the period of time a user views or communicates with a piece of software. Using the Firebox Users page, you can view informa-

tion on the sessions currently active on your Firebox. You can also see information on the users that have been defined for this Firebox.

1 From the navigation bar at left, select **Firebox Users**.




Under **Firebox User Settings**, view the current status of global Firebox User settings. Click the Configure button, to open the Settings page.

Under **Active Sessions**, the sessions that are currently active on the Firebox are listed along with the following information:

- The name of the user running the session
- The computer running the session
- The number of hours and minutes the session has been active
- The amount of idle time that elapses before the session automatically expires. If set to 0 hr: 0 min, the session does not automatically expire.

Under **Local User Accounts**, you can view the following information on users defined for this Firebox:

- The name of the user
- Whether Internet access is allowed for the user
- Whether the user has full administrative access
- Whether the User is configured to use WebBlocker, MUVPN, or VPN.

### Closing a session

To close a session, click **X** in the **Close** column of the session you want to close. When prompted, confirm that you indeed want to close the session.

### Editing a user account

To edit a user account, click the icon in the **Edit** column of the user you want to edit.

For descriptions of the fields you can edit, see "Adding a New User," below.

### Deleting a user account

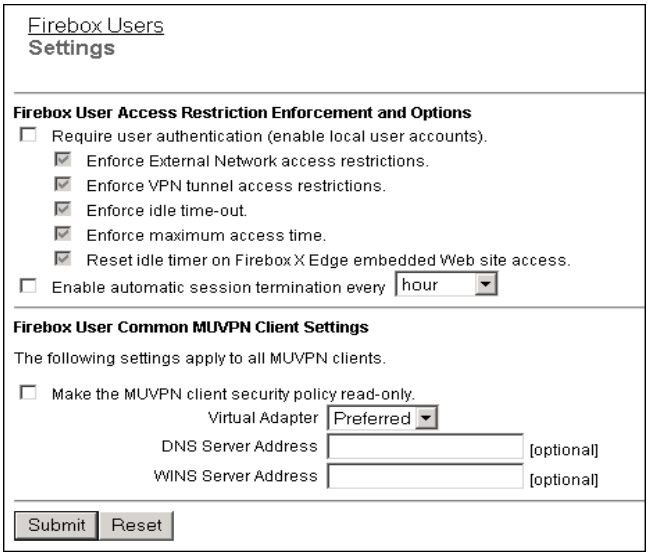
To delete a user account, click **X** in the **Delete** column of the user you want to delete. When prompted, confirm that you indeed want to delete the user.

## Configuring Global Settings

The options on the Settings page apply to all Firebox X Edge users:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox.
The default IP address is: https://192.168.111.1

2 From the navigation bar at left, select **Firebox ⇒ Settings**.
The Settings page appears.




3 The **Require user authentication** checkbox under **Firebox User Access Restriction Enforcement and Options** specify whether users must log in at local computers and, if so, whether certain options apply. Select any checkboxes for options you want to enforce.

4 To set a timeout value for sessions, select the **Enable automatic session termination every** checkbox. From the drop-down list, select either **hour**, **8 hours**, or **24 hours**.

5 To lock the MUVPN client security policy (.wgx file) such that users cannot make changes to it, select the **Make the MUVPN client security policy read-only** checkbox.

6 A virtual adapter is used for assigning client IP addresses and network parameters such as WINS and DNS. Select the virtual adapter rule for the mobile user:

**Disabled**
The mobile user will not use a virtual adapter to connect to the MUVPN client.

**Preferred**
(Default value) If the virtual adapter is already in use or otherwise unavailable, address assignment is performed without it.

**Required**
The mobile user must use a virtual adapter to connect to the MUVPN client.

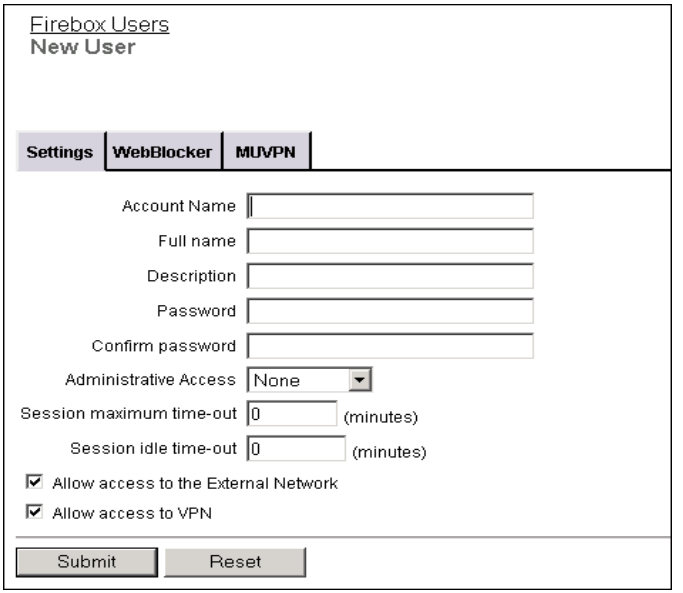
7 Specify, if you choose, DNS and WINS server addresses for MUVPN clients.

## Adding or Editing a User Account

When you define a user for the Firebox® X Edge, you specify the types of access permitted for that user. You can also specify a WebBlocker profile and allow MUVPN access.

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox.
The default IP address is: https://192.168.111.1

2 From the navigation bar at left, select **Firebox Users**.
The Firebox Users page appears.



3 Under **Local User Accounts**, click **Add**.
The New User page appears with the Settings tab visible.

4 In the **Account Name** field, enter a name for the account.

5 In the **Full Name** field, enter the user's full name.

6 In the **Description** field, enter a description for the user.

7 In the **Password** field, enter a password of up to eight characters.
Select a combination of eight letters, numbers, and symbols. Do not use an English or foreign word. Use at least one special symbol, a number, and a mixture of upper case and lower case letters for increased security.

8 Reenter the password in the **Confirm Password** field.

9 In the **Administrative Access** drop-down list, select the type of administrative access you want the user to have.
For more information, see "Creating a read only administrative account," on page 144.

10 Set maximum and minimum time-out values in the fields provided.

11 If you want this user to have Internet access, select the **Allow access to the External Network** checkbox.

12 If you want this user to have access to virtual private networking, select the **Allow access to VPN** checkbox.

13 Click **Submit**.

## Creating a read only administrative account

You can create a local user account with limited access to view Firebox configuration pages. When you log in as a read-only adminsitrator, you can not:

- Click the Reboot button on the System Status page.
- Change the Configuration Mode on the External page.
- Click the Reset Event Log and Sync Time with Browser Now buttons on the Logging page.
- Click the Synchronize Now button on the System Time page.
- Click the Regenerate IPSec Keys button on the VPN page.
- Change the Configuration Mode on the Managed VPN page.
- Click the Launch Wizard button from the Wizard page.

To create a read-only user account, edit the User Account. Use the Administrative Access drop-down list to select Read Only.

## Setting a WebBlocker profile for a user

A WebBlocker profile is a unique set of restrictions you can apply to users on your network. To set a WebBlocker profile for a new user, click the WebBlocker tab and select a profile from the drop-down list. For more information on WebBlocker profiles, see "Creating WebBlocker Profiles" on page 85.

## Enabling MUVPN for a user

To enable MUVPN for a new user, see "Enabling MUVPN Access for a User Account" on page 127.

## The Administrator account

The Firebox X Edge has a built-in administrator account that cannot be deleted. You can, however, change some of the administrator account's settings. On the Firebox Users page, click the icon in the **Edit** column of the administrator account.

For descriptions of the fields, see the previous section, "Adding a New User."

Make sure you record the administrator name and password in a safe location. These are required to access the configuration pages. If the system administrator name and password are unknown or you have forgotten them, you must reset the Firebox to the factory default settings. For more information, see "Resetting the Firebox to the factory default settings" on page 40.

WatchGuard recommends that you change the administrator password every month. Select a combination of eight letters, numbers, and symbols. Do not use an English or foreign word. Use at least one special symbol, a number, and a mixture of upper case and lower case letters for increased security.

## Resetting the user list

A Firebox uses a session when it makes a connection between a computer on the trusted interface and a computer on the external interface. The Firebox releases the session when:

- the session reaches the idle timeout limit;
- the session reaches the maximum time limit;

- the Firebox administrator uses the Firebox Users page to end the session;
- the user ends the session by closing all browser windows; or
- the Firebox restarts.

To end a session manually:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox.
The default IP address is: https://192.168.111.1
2 From the navigation bar at left, select **Firebox Users**.
The Firebox Users page appears.
3 Find the session in Active Sessions list. Click the close button. To end all sessions, click the **Close All** button.

### Changing a user password

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox.
The default IP address is: https://192.168.111.1
2 From the navigation bar at left, select **Firebox Users**.
The Firebox Users page appears.
3 Under **Local User Accounts**, click **Edit** for the account whose password you want to change.
The Edit User page appears with the Settings tab visible.
4 Click **Change Password**.
5 Type the old password and a new password. Confirm the new password.
6 Click **Submit**.

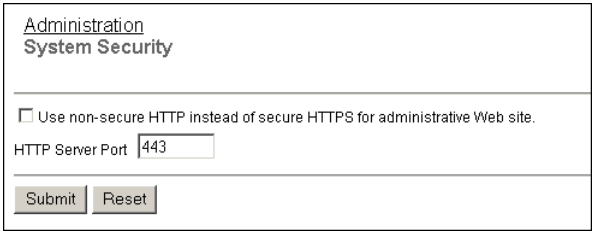
## Selecting HTTP or HTTPS for Firebox Management

HTTP (Hypertext Transfer Protocol) is the “language” used for transferring files (text, graphic images, and multimedia files) on the Internet. HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) is similar except that it enhances computer security by encrypting and decrypting the names of Web pages you type into your browser. For greater security, the Firebox® X Edge uses HTTPS by default.

Follow these instructions to use HTTP instead of HTTPS:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox.
The default IP address is: https://192.168.111.1

2 From the navigation bar at left, select **Administration ⇒ System Security.**
The System Security page appears.




3 Select the **Use non-secure HTTP instead of secure HTTPS for administrative Web site** checkbox.

4 Verify that the **HTTP Server Port** is set to 80.

5 Click **Submit.**

## Setting up VPN Manager Access

Use the VPN Manager Access page to allow your Firebox X Edge to be remotely managed by WatchGuard VPN Manager.

VPN Manager does not run directly on your Firebox X Edge; it is separate software that runs on a WatchGuard Firebox III or Firebox X. It configures and manages VPN tunnels.

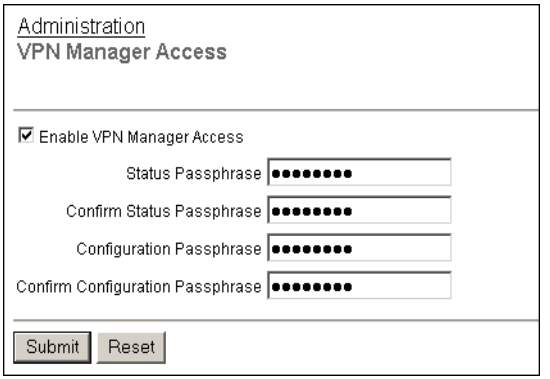
For more information about VPN Manager, see the WatchGuard Web site:

https://www.watchguard.com/products/vpnmanager.asp

Follow these instructions to configure VPN Manager access:

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
The default IP address is: https://192.168.111.1

2 From the navigation bar at left, select **Administration ⇒ VPN Manager Access**.
The VPN Manager Access page appears.




3 Select the **Enable VPN Manager Access** checkbox.

4 Type the status passphrase and then type it again to confirm in the applicable fields.

5 Type the configuration passphrase and then type it again to confirm in the applicable fields.

**NOTE**

These passphrases must match the passphrases used in the VPN Manager software or the connection will fail.

6 Click **Submit**.

## Updating the Firmware

Check regularly for Firebox® X Edge updates on the WatchGuard Web site:

https://www.watchguard.com/support/sohoresources

Two different methods exist for updating the firmware. One method uses a slightly larger download and automatically updates the firmware on the Firebox X Edge when run from any computer running Windows. The other method uses a smaller download and allows you to update the firmware through the Firebox X Edge Web pages. If you configure your Firebox X Edge from a computer that does not use the Windows operating system, such as Macintosh or Linux, you

must update your firmware with the second procedure because those operating systems cannot run Windows executable files.

## Method 1

The first method uses an auto-executable file and is the preferred method for updating the Firebox X Edge firmware from a Windows computer. Download the Software Update Installer to use this method. To use the Software Update Installer:

1 Launch the installer on a computer running Windows that is on the trusted side of the Firebox X Edge.

2 The installer prompts for an IP address and a user name and password. Enter the Firebox X Edge's trusted interface IP address.
By default this is 192.168.111.1

3 Enter the administrator name and password. Click **OK**.
The installer updates the firmware on the Firebox X Edge. As part of the update process, the Firebox X Edge will reboot once or twice— this is normal.

4 When the **Finish** button appears, click it.

**NOTE**

Because the Installer uses FTP to transfer files, make sure your Firebox X Edge is not configured to deny FTP access, as described in "Denying FTP access to the trusted network interface" on page 72.

## Method 2

The second method uses the Firebox X Edge Web pages. You can use this method regardless of the operating system your computer is running. You must first download the Software Update file, a small Zip file.

1 Extract the "wgrd" file from the Zip file you downloaded using an archiving utility such as Winzip (for Windows computers), Stuffit (for Macintosh), or Linux's archive capabilities.

2 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
The default IP address is: https://192.168.111.1

3 From the navigation bar at left, select **Administration** => **Update**.
The Administration Page appears with the End User License Agreement (EULA).

4 Read the text of the EULA. If you agree, select the **I accept the above license agreement** checkbox.

5 Type the name of the file containing the new Firebox X Edge software in the **Select file** box. Or click **Browse** to locate the file on the network.

6 Click **Update** and folloow the instructions.

## Activating Upgrade Options

Every Firebox® X Edge includes the software for all upgrade options, although they are not available for your use until you enter a license key for them in the configuration of the Firebox. To receive a license key, purchase and activate an upgrade option at the LiveSecurity Service Web site or from a WatchGuard-authorized reseller. See "Registering Your Firebox and Activating LiveSecurity Service" on page 25 for more information.

After you have purchased an upgrade option, follow these steps to activate it:

1 Go to the upgrade page of the WatchGuard Web site:
http://www.watchguard.com/upgrade

2 Type your LiveSecurity Service user name and password in the fields provided.

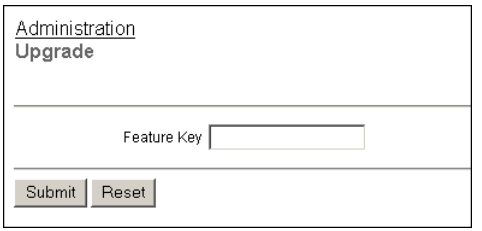
3 Click **Log In**.

4 Follow the instructions provided on the Web site to activate your license key and to retrieve the feature key.

5 Copy the feature key from the LiveSecurity Service Web site.

6 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
The default IP address is: https://192.168.111.1

7 From the navigation bar at left, select **Administration** => **Upgrade**.
The Upgrade page appears.




8 Paste the feature key in the applicable field.

9 Click **Submit**.

### Upgrade options

**User licenses**
A seat license upgrade allows more connections between the trusted network and the external network. For example, a 25-seat license allows 25 connections instead of the standard 10 connections.

**MUVPN Clients**
The MUVPN Clients upgrade allows remote users to connect to the Firebox X Edge through a secure (IPSec) VPN tunnel. These users have access to trusted network resources.

**WebBlocker**
The WebBlocker upgrade enables the Web filtering option. For more information on WebBlocker, see the "Configuring WebBlocker" chapter.

## Configuring Additional Options

Other options for your Firebox® X Edge do not require that you purchase them separately. However, they are initially disabled on your Firebox, and you must configure them. These options are as follows:

**Managed VPN**
The managed VPN feature allows you to set up VPN tunnels using DVCP. For more information, see Chapter 8, "Configuring VPNs."

**Manual VPN**
The manual VPN feature allows you to set up VPN tunnels manually. For more information, see Chapter 8, “Configuring VPNs.”

**WAN Failover**
The WAN failover feature adds redundant support for the external interface. For more information, see “Enabling the WAN Failover Option” on page 61.

## Viewing the Configuration File

You can view the contents of the Firebox® X Edge configuration file in text format from the View Configuration page.

1 Type the IP address of the trusted network in your browser window to connect to the System Status page of the Firebox X Edge.
The default IP address is: https://192.168.111.1

2 From the navigation bar on the left side, select **Administration ⇒ View Configuration File**.

Administration
View Configuration File

```
FDATE: Jun  4 2004
FTIME: 09:19:22
FVER: 7.0.0
admin.external_access: 1
admin.ha1hash: e80721f9ad6f03b50e89c8a08d082dc3
admin.idle_timeout: 0
admin.ipsec_access: 1
admin.max_access: 0
admin.muvpn_access: 0
admin.name: admin
admin.pass: pass
config.version: 0.1
networking.dhcp_client.enable: 0
networking.dhcpd.enable: 0
networking.dhcpd.firstip: 192.168.111.2
networking.dhcpd.lastip: 192.168.111.252
networking.dhcpd.optional.enable: 0
networking.dhcpd.optional.firstip: 192.168.112.2
networking.dhcpd.optional.lastip: 192.168.112.252
networking.ethernet.00: eth0 192.168.54.54 192.168.54.0 255.255.255.0 192.168.54.254
networking.ethernet.00.linkspeed: 1
networking.ethernet.01: eth1 192.168.111.1 192.168.111.0 255.255.255.0 192.168.111.1
networking.ethernet.02: eth2 192.168.112.1 192.168.112.0 255.255.255.0 192.168.112.1
networking.nameservice.dhcpd.dns.0: 192.168.130.131
networking.nameservice.dhcpd.dns.1: 192.168.130.245
networking.nameservice.dhcpd.domain_suffix: wgti.net
```

APPENDIX A

# Firebox® X Edge Hardware

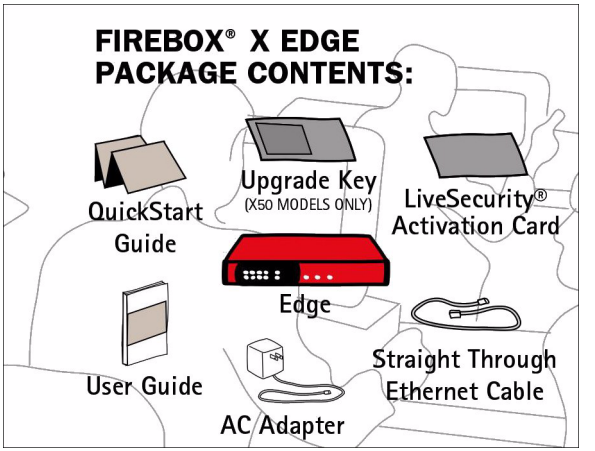
The WatchGuard® Firebox® X Edge is a firewall for small businesses and branch or remote offices.


## Package Contents

The Firebox® X Edge package also has:

- The Firebox X Edge *User Guide*
- The Firebox X Edge *QuickStart Guide*
- A LiveSecurity® Service activation card
- A Hardware Warranty Card

- An AC adapter (12 V)
- One straight-through Ethernet cable




## Hardware Specifications

| | |
|---|---|
| Processor | 64 bit MIPS |
| Memory - Flash | 16 MByte |
| Memory - RAM | 64 MByte |
| Network Interfaces | 10 x 10/100 |
| Serial ports | 1 DB9 |
| Power supply | 12V DC |
| Operating Temperature | 0 - 40C |
| Dimensions | Depth = 5.75 inches<br>Width = 8.75 inches<br>Height = 1.25 inches |
| Weight | 1.9 U.S. pounds |

## Hardware Description

The Firebox® X Edge has a straight-forward hardware design. All indicator lights appear on the front panel while all ports and connectors are on the rear of the device.

## Front panel

The front panel of the Firebox X Edge has 24 indicator lights to provide link and status information. The top light in each link pair indicates traffic passing through the designated interface. The bottom light in each pair indicates negotiation speed. The bottom light turns on when the speed is 100 mpbs.


**WAN 1, 2**

Indicates a physical connection to the external (WAN) ports. The indicator blinks yellow when traffic is passing through the interface.

**WAP**

Indicates a wireless connection to the Firebox. The indicator blinks green when traffic is passing through the wireless interface on Firebox X Edge wireless models.

**F/O**

Indicates a WAN failover. The indicator is green when there is a failover from WAN1 to WAN2. The indicator is dark when the external interface connection returns to WAN1.

**Link**

The link indicators indicate a physical connection to any of the numbered (0–6) interfaces of the trusted network. The indicator blinks when traffic is passing through the interface.

**100**

When a trusted network interface runs at 100 Mb, the corresponding 100 indicator is lit. When it runs at 10 Mb, the indicator is not lit.

**Status**
Indicates that a management connection has been made. This light turns off a few minutes after you close the browser connection to the Firebox X Edge Web pages.

**Mode**
When lit and steady, indicates that the Firebox X Edge is operational and has connected to the Internet. When lit and flashing, indicates that the WAN is connected but the Firebox cannot establish a connection to the Internet.

**Attn**
Reserved for future use.

**Power**
Indicates that the Firebox X Edge is currently powered up.

**RESET button**
Press the RESET button to reset the Firebox X Edge to the factory default configuration. For more information, see "Factory Default Settings" on page 39.

## Back view

The back of the Firebox X Edge has several Ethernet ports and inputs:

**Serial port (DB9)**
For modem connectivity.

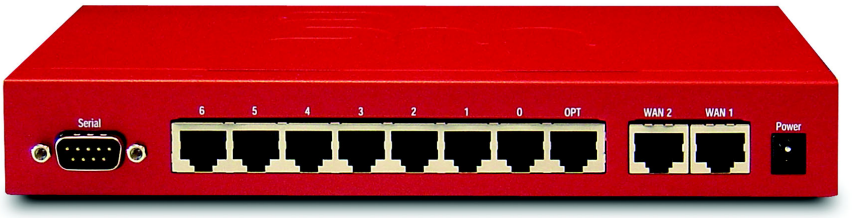
**Seven numbered Ethernet ports (0-6)**
These Ethernet ports are for the trusted network interface.

**OPT port**
This Ethernet port is for the optional network interface.

**Two WAN Ethernet ports (WAN, WAN2)**
The WAN ports are for the external network interface.

### Power input

Connect the power input to a power supply using the 12-volt AC adapter supplied with the Firebox X Edge. The power supply tip is plus (+) polarity.




## Side panels

On both side panels of the Firebox X Edge is a slot for a personal computer locking system.

APPENDIX B

# Glossary

This glossary contains a list of terms, abbreviations, and acronyms frequently used when discussing networks, firewalls, and WatchGuard products.

**access control**
A method of restricting access to resources, allowing access only to privileged entities.

**active mode FTP**
One of two ways an FTP data connection is made. In active mode, the FTP server establishes the data connection. In passive mode, the client establishes the connection. In general, FTP user agents use active mode and Web user agents use passive mode.

**activity light**
An LED (light-emitting diode) that verifies that a piece of hardware is working, communicating with the network, and transmitting data.

**address learning**
A method by which hubs, switches, and routers determine the unique address number for each node on a network to enable accurate transmission to and from each node.

**Address Resolution Protocol (ARP)**
A TCP/IP protocol used to convert an IP address into a physical address such as an Ethernet address.

**address space probe**
An intrusion measure in which a hacker sequentially attacks IP addresses. These probes are usually attempts to map IP address space to look for security holes that a sender might exploit to compromise system security.

**agent**
A computer program that reports information to another computer or allows another computer access to the local system. Agents can be used for good or malice. Many security programs have agent components that report security information back to a central reporting platform. However, agents can also be remotely controlled programs hackers use to access machines.

**AH (authentication header)**
A protocol used in IPSec available for use with IPSec Branch Office VPN. AH provides authentication for as much of the IP header as possible (except for mutable fields that are nondeterministic, such as TTL fields) and all upper protocols and payload. It offers the functionality of ESP except for confidentiality, which ESP's encryption provides.

**algorithm (encryption)**
A set of mathematical rules (logic) used in the processes of encryption and decryption.

**algorithm (hash)**
A set of mathematical rules (logic) used in the processes of message digest creation and key/signature generation.

**alias**
A shortcut that enables a user to identify a group of hosts, networks, or users with one identifying name. Aliases are used to speed user authentication and service configuration.

**Application Program Interface (API)**
Software that allows dissimilar software products to interact upon one another.

**armed**
A state of a Firebox in which it is actively guarding against intrusion and attack.

**ARP**
See *Address Resolution Protocol*.

**ARP table**
A table of active ARP addresses on a computer.

**ascending**
A method of ordering a group of items from lowest to highest, such as from A to Z.

**ASN.1 (Abstract Syntax Notation One)**
ISO/IEC standard for encoding rules used in ANSI X.509 certificates. Two types exist: DER (Distinguished Encoding Rules) and BER (Basic Encoding Rules).

**asymmetric keys**
A separate but integrated user key pair, composed of one public key and one private key. Each key is one way, meaning that a key used to encrypt information cannot be used to decrypt the same data.

**attack**
An attempt to hack into a system. Because not all security issues represent true attacks, most security vendors prefer the use of the word “event” or “incident.”

**ATM (asynchronous transfer mode)**
High-speed packet switching with dynamic bandwidth allocation.

**authentication**
A method of mapping a user name to a workstation IP address, allowing the tracking of connections based on name rather than IP address. With authentication, it does not matter which IP address is used or from which machine a person chooses to work.

**autopartitioning**
A feature on some network devices that isolates a node within the workgroup when the node becomes disabled, so as to not affect the entire network or group.

**authorization**
To convey official access or legal power to a person or entity.

**backbone**
A term often used to describe the main network connections composing the Internet.

**backdoor**
A cipher design fault, planned or accidental, that allows the apparent strength of the design to be easily avoided by those who know the trick. When the design background of a cipher is kept secret, a back door is often suspected.

**bandwidth**
The rate at which a network can transfer data.

**Bandwidth Meter**
A monitoring tool that provides a real-time graphical display of network activities across a Firebox. Formerly known as the Mazameter.

**bastion host**
A computer placed outside a firewall to provide public services (such as WWW and FTP) to other Internet sites. The term is sometimes generalized to refer to any host critical to the defense of a local network.

**bitmask**
A pattern of bits for an IP address that determines how much of the IP address identifies the host and how much identifies the network.

**block cypher**
A symmetric cipher operating on blocks of plain text and cipher text, usually 64 bits.

**blocked port**
A security measure in which a specific port associated with a network service is explicitly disabled, blocking users outside the firewall from gaining access to that service port. A blocked port takes precedence over any service settings that are generally enabled.

**blocked site**
An IP address outside the Firebox explicitly blocked so it cannot connect with hosts behind the Firebox. Blocked sites can be manual and permanent, or automatic and temporary.

**Blue Screen of Death (BSoD)**
A condition in which a Windows NT–based system encounters a serious error, the entire operating system halts, and a screen appears with information regarding the error. The name comes from the blue color of the error screen.

**boot up**
To start a computer.

**Branch Office Virtual Private Networking (BOVPN)**
A type of VPN that creates a secure tunnel over an unsecure network, between two networks that are protected by the WatchGuard Firebox System, or between a WatchGuard Firebox and an IPSec-compliant device. It allows a user to connect two or more locations over the Internet while protecting the resources on the trusted network and the optional or a less trusted network.

**bridge**
A piece of hardware used to connect two or more networks so that devices on the network can communicate. Bridges can only connect networks running the same protocol.

**broadcast**
A network transmission sent to all nodes on a network.

**broadcast address**
An address used to broadcast a request to a network, usually to discover the presence of a machine.

**browser**
See *Web browser.*

**bus topology**
A networking setup in which a single cable, such as thin Ethernet, is used to connect one computer to another.

**cable segment**
A section of network cable separated by hubs, routers, or bridges to create a subnet.

**cascade**
A command that arranges windows so that they are overlapped, with the active window in front.

**cascading**
Connecting hubs with 10BASE-T cable; sometimes requires a crossover cable.

**Category 3 cabling**
A 10BASE-T unshielded twisted-pair cabling type commonly used in today's 10Mbps Ethernet networks.

**Category 5 cabling**
A higher grade of unshielded twisted-pair cabling required for networking applications wich as 100Mbps Fast Ethernet.

**CBC**
See *cipher block chaining*.

**CD-ROM (Compact Disc Read-Only Memory)**
A disk on which data is stored.

**certificate**
An electronic document attached to a public key by a trusted third party, which provides proof that the public key belongs to a legitimate owner and has not been compromised.

**certificate authority (CA)**
A trusted third party (TTP) who creates certificates that consist of assertions on various attributes and binds them to an entity and/or to their public key.

**certificate revocation list (CRL)**
An online, up-to-date list of previously issued certificates that are no longer valid.

**certification**
Endorsement of functionality by a trusted entity.

**Challenge Authentication Protocol (CHAP)**
A session-based, two-way password authentication scheme.

**channel**
A communications path between two computers or devices.

**checkbox**
A dialog box option that is not mutually exclusive with other options. Selecting a checkbox inserts or removes an X or a checkmark; clearing a checkbox removes it.

**CIDR (Classless Inter-Domain Routing)**
A routing mechanism designed to deal with the exhaustion of Class B network addresses, and the subsequent allocation of multiple Class C addresses to sites. CIDR is described in RFC 1519.

**cipher block chaining**
A form of DES encryption that requires the entire message to decrypt rather than a portion of the message.

**cipher text**
The result of manipulating either characters or bits by way of substitution, transposition, or both.

**Class A, Class B, Class C**
See *Internet address class*.

**clear-signed message**
A message that is digitally signed but not encrypted.

**clear text**
Characters in a human readable form prior to or after enryption. Also called *plain text*.

**client**
A computer process that requests a service of another computer and accepts the server's responses.

**Client/Server**
A network computing system in which individual computers (clients) use a central computer (server) for services such as file storage, printing, and communications. See *peer-to-peer*.

**coax (coaxial) cable**
A type of cable, used in Ethernet networking, with a solid central conductor surrounded by insulator, in turn surrounded by a cylindrical shield woven from fine wires.

**cold boot**
The process of starting a computer by turning on the power to the system unit.

**collisions**
Conflicts that occur when two packets are sent over the network simultaneously. Both packets are rejected; Ethernet will automatically resend them at altered timing.

**communications software**
Software such as email and faxing software that allows users to send or receive data.

**compress**
To compact a file or group of files so that they occupy less disk space. See also *decompress*.

**compression function**
A function that takes a fixed-size input and returns a shorter, fixed-sized output.

**connected enterprise**
A company or organization with a computer network exchanging data with the Internet or some other public network.

**Control Center**
See *System Manager*.

**Control Panel**
The set of Windows NT, Windows 2000, and Windows XP programs used to change system hardware, software, and Windows settings.

**conventional encryption**
Encryption that relies on a common passphrase instead of a public key cryptography. The file is encrypted using a session key, which encrypts using a passphrase that a user is asked to choose.

**cookie**
A file or token passed from the Web server to the Web client (a user's browser) that is used to identify a user and could record personal information such as ID and password, mailing address, or credit card number.

**coprocessor**
A separate processor designed to assist in specific functions, such as handling complex mathematics or graphics, and to temporarily reduce the workload of the microprocessor.

**corporate signing key**
A public key that is designated by the security officer of a corporation as the system-wide key that all corporate users trust to sign other keys.

**CPU (central processing unit)**
The microprocessor chip that interprets and carries out instructions. Also, simply, a term for a computer.

**cracker**
A codebreaker; a person who attempts to break encryption, software locks, or network security. Can also be used as a synonym for hacker.

**CRL**
See *certificate revocation list*.

**cross-certification**
Two or more organizations or certificate authorities that share some level of trust.

**crossover cable**
A cable in which the receive and transmit lines (input and output) are crossed. Crossover cables are necessary to connect hubs.

**cryptanalysis**
The art or science of transferring cipher text into plain text without initial knowledge of the key used to encrypt the plain text.

**CRYPTOCard**
An authentication system that uses an offline card to hash encryption keys, which increases their safety against unauthorized decryption.

**cryptography**
The art and science of creating messages that have some combination of being private, signed, and unmodified with non-repudiation.

**CSLIP (Compressed Serial Line Internet Protocol)**
A protocol for exchanging IP packets over a serial line, which compresses the headers of many TCP/IP packets.

**custom filter rules**
Filter rules created in WatchGuard Policy Manager to allow specific content types through the Firebox.

**data**
Distinct pieces of information, usually formatted in a special way.

**data compression**
A way of storing data in a format that requires less space than usual. Data compression is particularly useful in communications because it enables devices to transmit the same amount of data in fewer bits.

**datagram**
A packet of data that stands alone. Generally used in reference to UDP and ICMP packets when talking about IP protocols.

**data transmission speed**
The number of bits that are transmitted per second over a network cable.

**DCERPC (Distributed Computing Environment Remote Procedure Call)**
A call that allows connections bound for port 135 on a machine. These initial calls typically result in a response from the trusted machine that redirects the client to a new port for the actual service the client wants.

**decompress**
To expand a compressed file or group of files so that the file or files can be opened. See also *compress*.

**decrypt**
To decode data that has been encrypted and turn it back into plain text.

**dedicated server**
A computer on a network that is assigned to function only as a resource server and cannot be used as a client.

**default**
A predefined setting that is built into a program and is used when an alternative setting is not specified.

**default packet handling**
The practice of automatically and temporarily blocking hosts that originate probes and attacks against a network.

**denial of service attack (DoS)**
A way of monopolizing system resources so that other users are ignored. For example, someone could Finger an unsecured host continuously so that the system is incapable of running or executing other services.

**DES (Data Encryption Standard)**
A block-oriented cipher that encrypts blocks of 64 bits. The encryption is controlled by a key of 56 bits. See also *Triple DES*.

**descending**
A method of ordering a group of items from highest to lowest, such as from Z to A.

**device**
Networking equipment such as a hub, switch, bridge, or router.

**DHCP (Dynamic Host Configuration Protocol)**
A means of dynamically allocating IP addresses to devices on a network.

**DHCP server**
A device that automatically assigns IP addresses to network computers from a defined pool of numbers.

**dialog box**
A box that displays additional options when a command is chosen from a menu.

**dial-up connection**
A connection between a remote computer and a server using software, a modem, and a telephone.

**dictionary attack**
An attack that attempts to reveal a password by trying logical combinations of words.

**Diffie-Hellman**
A mathematical technique for securely negotatiating secret keys over a public medium.

**digital signature**
An electronic identification of a person or thing created by using a public key algorithm. Intended to verify to a recipient the integrity of data and identity of the sender of the data.

**dimmed**
The grayed appearance of a command or option that is unavailable.

**disarmed**
The state of a Firebox when it is not actively protecting a network.

**DMZ (Demilitarized Zone)**
Another name for the optional network. One common use for this network is as a public Web server.

**DNS (Domain Name System)**
A network system of servers that converts numeric IP addresses into readable, hierarchical Internet addresses.

**DoS**
See *denial of service attack*.

**dotted notation**
The notation used to write IP addresses as four decimal numbers separated by dots (periods), sometimes called dotted quad—123.212.12.4 is an example.

**double-click**
To press the primary mouse button twice rapidly.

**download**
To transfer a file from a remote computer to a local computer.

**driver**
A software program that manipulates the computer hardware in order to transmit data to other equipment.

**drop-in configuration**
A configuration in which the Firebox is physically located between the router and the LAN without any of the computers on the Trusted interface being reconfigured. This protects a single network that is not subdivided into smaller networks.

**drop-in network**
A configuration that allows for distribution of logical address space across the Firebox interface.

**DSA (Digital Signature Algorithm)**
A public key digital signature algorithm proposed by the National Institute of Standards and Technology for DSS.

**DSS (Digital Signature Standard)**
A standard for digital signatures using DSA proposed by the National Institute of Standards and Technology.

**DVCP (Dynamic VPN Configuration Protocol)**
A WatchGuard proprietary protocol that simplifies configuration of VPNs.

**dynamic NAT**
(Also known as IP masquerading or port address translation) A method of hiding network addresses from hosts on the external or on a less trusted network. Hosts elsewhere on the Internet see only outgoing packets from the Firebox itself.

**dynamic packet filtering**
Filtering based not only on service types, but also on conditions surrounding the initiation of a connection.

**ECC (Elliptic Curve Cryptosystem)**
A method for creating public key algorithms based on mathematical curves over finite fields or with large prime numbers.

**encryption**
The process of disguising a message to hide its substance.

**entropy**
A mathematical measurement of the amount of uncertainty or randomness.

**ESMTP (Extended Simple Mail Transfer Protocol)**
A protocol that provides extensions to SMTP for sending email that supports graphics, audio, and video files, and text in various foreign languages.

**ESP (Encapsulation Security Payload)**
A protocol used in IPSec used with IPSec Branch Office VPN and MUVPN. ESP encapsulates and authenticates IP packets to be passed over the tunnel, providing confidentiality, data integrity, and origin authentication. ESP is similar to AH, except that it provides encryption.

**Ethernet**
Networking standards, originally developed in 1973 and formalized in 1980, involving the transmission of data at 10 Mbps using a specified protocol.

**Ethernet address**
A unique address that is obtained automatically when an Ethernet adapter is added to the computer. This address identifies the node as a unique communication item and enables direct communications to and from that particular computer.

**event**
Any network incident that prompts some kind of notification.

**event processor**
See *WatchGuard Security Event Processor*.

**expand**
To display all subordinate entries in an outline or in a folder.

**extension**
See *file extension*.

**external interface**
An interface connected to the external network that presents the security challenge, typically the Internet.

**external network**
The network presenting the security challenge.

**failover**
Configuration that allows a secondary machine to take over in the event of a failure in the first machine, allowing normal use to return or continue.

**failover logging**
A process in which contact is automatically established with a secondary log host, in the event that the Firebox cannot communicate with the primary log host.

**fail-shut mode**
A condition in which a firewall blocks all incoming and outgoing traffic in the event of a firewall failure. This is the opposite of fail-open mode, in which a firewall crash opens all traffic in both directions. Fail-shut is the default failure mode of the WatchGuard Firebox System.

**fast Ethernet**
An Ethernet networking system that transmits data at 100 Mbps, based on the Ethernet 802.3 standard.

**field**
An area in a form or Web page in which to enter or view specific information about an individual task or resource.

**file extension**
A period and up to three characters at the end of a file name. The extension can help identify the kind of information a file contains.

**file server**
A dedicated network computer used by client computers to store and access files.

**filtering process**
An Ethernet switch or bridge process that reads the contents of a packet and discards it if it does not need to be forwarded.

**filtering rate**
The rate at which an Ethernet device can receive packets and drop them without any loss of incoming packets or delay in processing.

**filters**
Small, fast programs in a firewall that examine the header files of incoming packets and route or reject the packets based on the rules for the filter.

**fingerprint**
A unique identifier for a key that is obtained by hashing specific portions of the key data.

**FIPS (Federal Information Processing Standard)**
A U.S. government standard published by the National Institute of Standards and Technology.

**Firebox**
The WatchGuard firewall appliance, consisting of a red box with a purpose-built computer and input/output architecture optimized as the resident computer for network firewall software.

**Firebox System Manager**
A WatchGuard toolkit of applications run from a single location, enabling configuration, management, and monitoring of a network security policy. Formerly called *Control Center*.

**firewall**
Any technological measures taken to secure a computer network against unwanted use and abuse by way of net connections.

**firewalling**
The creation or running of a firewall.

**flash disk**
An 8-megabyte, on-board flash ROM disk that acts like a hard disk in a Firebox.

**FTP (File Transfer Protocol)**
The most common protocol for copying files over the Internet. See also *active mode FTP*.

**gateway**
A system or host that provides access between two or more networks. Gateways are typically used to connect networks that are dissimilar.

**graphical user interface (GUI)**
The visual representation on a computer screen that allows users to view, enter, or change information.

**hack**
To use a computer or network to perform illegal acts or gain unauthorized access.

**hacker**
An individual who uses a computer or network to perform illegal acts or gain unauthorized access. The term also can refer to an individual who is simply a computer enthusiast or expert; however, WatchGuard publications use the former definition.

**hash code**
A unique, mathematical summary of a document that serves to identify the document and its contents. Any change in the hash code indicates that the document's contents have been altered.

**header**
A series of bytes at the beginning of a communication packet that provide identification information about the packet such as its computer of origin, the intended recipient, packet size, and destination port number.

**Help system**
A form of online information about a software or hardware system.

**hexadecimal**
A numbering system containing 16 sequential numbers as base units before adding a new position for the next number. Hexadecimal uses the numbers 0–9 and the letters A–F.

**hierarchical trust**
A graded series of entities that distribute trust in an organized fashion, commonly used in ANSI X.509 to issue certifying authorities.

**High Availability**
A WatchGuard Firebox System option that enables the installation of two Fireboxes on one network in a failover configuration. At any given moment, one Firebox is in active mode while the other is in standby mode, ready to take over if the first box fails.

**Historical Reports**
A WatchGuard Firebox System application that creates HTML reports displaying session types, most active hosts, most used services, and other information useful in monitoring and troubleshooting a network.

**HMAC**
A key-dependent, one-way hash function specifically intended for use with MAC (Message Authentication Code), and based upon IETF RFC 2104.

**home page**
The first page of a Web site used as an entrance into the site.

**honeypot**
Programs that simulate one or more network services that you designate on your computer's ports. An attacker assumes you're running vulnerable services that can be used to break into the machine. A honeypot can be used to log access attempts to those ports including the attacker's keystrokes. This could give you advanced warning of a more concerted attack.

**host**
A computer connected to a network.

**host route**
A setup in which an additional router is behind the Firebox and one host is behind that router. A host route must be configured to inform the Firebox of this additional host behind the additional router.

**HostWatch**
A WatchGuard Firebox System application that provides a real-time display of the hosts that are connected from behind the Firebox to hosts on the Internet.

**HTML (HyperText Markup Language)**
A set of rules used to format Web pages, including methods to specify text characteristics, graphic placement, and links. HTML files are read and interpreted by a Web browser.

**HTTP (HyperText Transfer Protocol)**
A communications standard designed and used to transfer information and documents between servers or from a server to a client.

**HTTPS (Secure HTTP)**
A variation of HTTP enabling the secure transmission of data and HTML files. Generally used in conjunction with Secure Sockets Layer (SSL).

**hub**
A device that receives and sends signals along the network between the nodes connected to it.

**hyperlink**
An object on a Web page such as a graphic or underlined text that represents a link to another location in the same file or a different file. When clicked, the page or graphic appears.

**IANA (Internet Assigned Number Authority)**
The central authority charged with assigning parameter values to Internet protocols. For example, IANA controls the assignment of well-known TCP/IP port numbers. Currently IANA manages port numbers 1 through 1023.

**ICMP (Internet Control Message Protocol)**
A protocol used to pass control and error messages back and forth between nodes on the Internet.

**identity certificate**
A signed statement that binds a key to the name of an individual and therefore delegates authority from that individual to the public key.

**IDS**
See *Intrusion Detection System*.

**IETF**
See *Internet Engineering Task Force*.

**IKE (Internet Key Exchange)**
A protocol used with IPSec virtual private networks. Automates the process of negotiating keys, changing keys, and determining when to change keys.

**implicit trust**
A condition reserved for pairs located on a local keyring. If the private portion of a key pair is found on a user's keyring, PGP assumes that user is the owner of the key pair and implicitly trusts himself or herself.

**initialization vector**
A block of arbitrary data that serves as the starting point for a block cipher using a chaining feedback mode. See also *cipher block chaining*.

**initialize**
To prepare a disk for information storage.

**installation wizard**
A wizard specifically designed to guide a user through the process of installing software. See *wizard*.

**integrity, data integrity**
Assurance that data is not modified by unauthorized persons during storage or transmittal.

**interface**
A boundary across which two independent systems meet and act on or communicate with each other. The term generally refers to a hardware interface—the wires, plugs, and sockets that hardware devices use to communicate with each other.

**Internet address class**
To efficiently administer the 32-bit IP address class space, IP addresses are separated into three classes that describe networks of varying sizes:
*Class A*—If the first octet of an IP address is less than 128, it is a Class A address. A network with a Class A address can have up to about 16 million hosts.
*Class B*—If the first octet of an IP address is from 128 to 191, it is a Class B address. A network with a Class B address can have up to 64,000 hosts.
*Class C*—If the first octet of an IP address is from 192 to 223, it is a Class C address. A network with a Class C address can have up to 254 hosts.

**Internet Engineering Task Force (IETF)**
A large, open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

**intranet**
A self-contained network that uses the same communications protocols and file formats as the Internet.

**Intrusion Detection System (IDS)**
A class of networking products devoted to detecting, monitoring, and blocking attacks from hackers. IDSs that operate on a host to detect malicious activity on that host are called host-based IDSs. IDSs that operate on network data flows are called network-based IDSs.

**IP (Internet Protocol)**
A protocol used by the Internet that enables computers to communicate over various physical media.

**IP address host**
The 32-bit address that identifies a host. Technically, a host is a network device connected to the Internet. In common usage, a host is a computer or some other device that has a unique IP address. Computers with more than one IP address are known as multihomed hosts.

**IP fragment**
An IP datagram that is actually part of a larger IP packet. IP fragments are typically used when an IP packet is too large for the physical media that the data must cross. For example, the IP standard for Ethernet limits IP packets to about 1,500 bytes, but the maximum IP packet size is 65,536 bytes. To send packets larger than 1,500 bytes over an Ethernet, IP fragments must be used.

**IP masquerading**
*See dynamic NAT.*

**IP options**
Extensions to the Internet Protocol used mainly for debugging and special applications on local networks. In general, there are no legitimate uses of IP options over an Internet connection.

**IP options attack**
A method of gaining network access by using IP options.

**IPSec (Internet Protocol Security)**
An open-standard methodology of creating a secure tunnel through the Internet, connecting two remote hosts or networks. IPSec provides several encryption and authentication options to maximize the security of the transmission over a public medium such as the Internet.

**IP spoofing**
The act of inserting a false sender IP address into an Internet transmission to gain unauthorized access to a computer system.

**ISA (Industry Standard Architecture)**
A unique network interface card on the motherboard of a computer.

**ISAKMP (Internet Security Association Key Management Protocol)**
Defines the procedures for authenticating a communicating peer, creation and management of security associations, key generation techniques, and threat mitigation; for example, denial of service and replay attacks.

**ISO (International Organization for Standardization)**
An organization responsible for a wide range of standards, like the OSI model and international relationship with ANSI on X.509.

**ISP (Internet service provider)**
A business that sells access to the Internet. A government organization or an educational institution may be the ISP for some organizations.

**ITU-T (International Telecommunication Union–Telecommunication)**
Formerly the CCITT (Consultative Committee for International Telegraph and Telephone), a worldwide telecommunications technology standards organization.

**IV**
See *initialization vector*.

**Java applet**
A program written in the Java programming language that can be included on an HTML page, much in the same way an image is included. When someone uses a Java technology–enabled browser to view a page that contains an applet, the applet's code is transferred to that user's system and carried out by the browser's Java virtual machine (JVM).

**Kerberos**
A trusted third-party authentication protocol developed at Massachusetts Institute of Technology.

**key**
A means of gaining or preventing access, possession, or control represented by any one of a large number of values.

**key exchange**
A scheme for two or more nodes to transfer a secret session key across an unsecured channel.

**key fingerprint**
A uniquely identifying string of numbers and characters used to authenticate public keys.

**key ID**
A code that uniquely identifies a key pair. Two key pairs can have the same user ID, but they have different key IDs.

**key length**
The number of bits representing the key size; the longer the key, the stronger it is.

**key management**
The process and procedure for safely storing and distributing accurate cryptographic keys; the overall process of generating and distributing cryptographic key to authorized recipients in a secure manner.

**key pair**
A public key and its complementary private key.

**keyring**
A set of keys. Each user has two types of keyrings: a private keyring and a public one.

**key splitting**
The process of dividing a private key into multiple pieces and sharing those pieces among several users. A designated number of users must bring their shares of the key together to use the key. Also called secret sharing.

**LAN (local area network)**
A computer network that spans a relatively small area generally confined to a single building or group of buildings.

**LDAP (Lightweight Directory Access Protocol)**
A protocol that supports access and search operations on directories containing information such as names, phone numbers, and addresses across otherwise incompatible systems over the Internet.

**LED (light-emitting diode)**
A small indicator light on a networking device that provides indication of status and other information about the device.

**link**
See *hyperlink*.

**Linux**
An open source version of the UNIX operating system.

**LiveSecurity Service**
See *WatchGuard LiveSecurity Service*.

**LogViewer**
A WatchGuard Firebox System application that displays a static view of a log file.

**loopback interface**
A pseudo interface that allows a host to use IP to talk to its own services. A host is generally configured to trust packets coming from addresses assigned to this interface. The Class A address group 127.0.0.0 has been reserved for these interfaces.

**mail server**
Refers to both the application and the physical machine tasked with routing incoming and outgoing electronic mail.

**management station**
The computer on which the WatchGuard Firebox System Manager and Policy Manager runs; sometimes referred to as the administration host.

**man-in-the-middle attack**
An attack that deceives two parties into thinking they are communicating with each other while, in fact, they are both communicating with a third party. This type of attack is often attempted when the attacker desires communication with a system under the identity of a particular user.

**name resolution**
The allocation of an IP address to a host name. See *Domain Name System*.

**NetBIOS (Network Basic Input / Output System)**
An extension of the DOS BIOS that enables a computer to connect to and communicate with a LAN (Local Area Network).

**NetBEUI (NetBIOS Extended User Interface)**
A non-routable networking protocol used by smaller, non-subnetted networks for internal communications. Because NetBEUI is not routable, network transmissions sent via NetBEUI cannot be transmitted over the Internet.

**network address translation (NAT)**
A method of hiding internal network addresses from hosts on an external network.

**MAC (Machine Authentication Code)**
A key-dependent, one-way hash function, requiring the use of the identical key to verify the hash.

**MAC address**
Media Access Control address that is unique to a computer, and is used to identify its hardware.

**masquerading**
A method of setting up addressing so that a firewall presents its IP address to the outside world in lieu of the IP addresses of the hosts protected by the firewall.

**Mazameter**
See *Bandwidth Meter*.

**MD2 (Message Digest 2)**
A 128-bit, one-way hash function that is dependent on a random permutation of bytes.

**MD4 (Message Digest 4)**
A 128-bit, one-way hash function that uses a simple set of bit manipulations on 32-bit operands.

**MD5 (Message Digest 5)**
An improved, more complex version of MD4, but still a 128-bit, one-way hash function.

**message digest**
A number that is derived from a message. A change to a single character in the message will cause it to have a different message digest.

**MIME (Multipurpose Internet Mail Extensions)**
Extensions to the SMTP format that allow binary data, such as that found in graphic files or documents, to be published and read on the Internet.

**modem**
A communications device that sends computer transmissions over a standard telephone line.

**motherboard**
The main printed circuit board in a computer, which contains sockets that accept additional boards (daughterboards).

**MSDUN**
Microsoft Dial-Up Networking is an executable program required for remote user VPN.

**multiple network configuration**
A configuration used in situations in which a Firebox is placed with separate logical networks on its interface.

**National Institute for Standards and Technology**
A division of the U.S. Department of Commerce that publishes open interoperability standards called Federal Information Processing Standards (FIPSs).

**network address**
The network portion of an IP address. For a class A network, the network address is the first byte of the IP address. For a class B network, the network address is the first two bytes of the IP address. For a class C network, the network address is the first three bytes of the IP address. In each case, the remainder is the host address. In the Internet, assigned network addresses are globally unique.

**network address translation (NAT)**
A method of hiding or masquerading network addresses from hosts on another network, protecting the confidentiality and architecture of the network.

**netmask**
An inverse mask of the significant bits of a network address. On a local net, the range of addresses one can expect to be found directly connected to the network. Because netmasks generally occur with a Class C license address space of 8 bits, the netmask is 255.255.255.0. It can be a smaller number of bits if

subnetting is in effect. Some systems require the netmask to be an even number of bits.

**network adaptor, network interface card**
A device that sends and receives data between the computer and the network cabling. It may work either internally, such as a PCI, or externally, such as a SCSI adaptor which connects to a computer's SCSI port.

**network number**
The portion of an IP address that is common to all hosts on a single network and is normally defined by the set portion of the corresponding netmask.

**network range**
The portion of an IP address that is allocated to individual hosts on a single network and is normally defined by the cleared portion of the corresponding netmask.

**NFS (Network File System)**
A popular TCP/IP service for providing shared file systems over a network.

**NIST**
See *National Institute for Standards and Technology.*

**node**
A computer or CPU on a network.

**non-seed router**
A router that waits to receive routing information (the routing maintenance table) from other routers on the network before it begins routing packets.

**NTP (Network Time Protocol)**
An Internet service used to synchronize clocks between Internet hosts. Properly configured, NTP can usually keep the clocks of participating hosts within a few milliseconds of each other.

**Oakley**
The Oakley Session Key Exchange provides a hybrid Diffie-Hellman session key exchange for use within the ISA/KMP framework. Oakley provides the important property of Perfect Forward Secrecy.

**octet**
A byte. Used instead of "byte" in most IP documents because historically many hosts did not use 8-bit bytes.

**one-time pad**
A large, non-repeating set of truly random key letters used for encryption, considered the only perfect encryption scheme.

**one-way hash function**
A function that produces a message digest that cannot be reversed to produce the original.

**optional interface**
An interface that connects to a second secured network, typically any network of servers provided for public access.

**optional network**
A network protected by the firewall but still accessible from the trusted and external networks. Typically, any network of servers provided for public access.

**OSI (Open Systems Interconnection)**
A standard description or reference model for how messages should be transmitted between any two points in a telecommunication network. Its purpose is to guide product implementors so that their products will consistently work with other products.

**out-of-band (OOB)**
A management feature that enables the management station to communicate with the Firebox using a telephone line and a modem. OOB is very useful for remotely configuring a Firebox when Ethernet access is unavailable.

**packet**
A unit of information containing specific protocols and codes that allow precise transmittal from one node in a network to another.

**packet filtering**
A way of controlling access to a network by analyzing the incoming and outgoing packets and letting them pass or halting them based on the IP addresses of the source and destination. Packet filtering is one technique, among many, for implementing security firewalls.

**passive mode FTP**
See *active mode FTP*.

**passphrase**
An easy-to-remember phrase used for better security than a single password; key crunching converts it into a random key.

**password**
A sequence of characters or a word that a user submits to a system for purposes of authentication, validation, or verification.

**password caching**
The storage of a user's username and password in a network administrator database or encrypted file on a computer.

**Password Authentication Protocol (PAP)**
An authentication protocol that allows PPP peers to authenticate one another. It does not prevent unauthorized access, but identifies the remote end.

**PCI (peripheral component interconnect)**
A unique network interface card slot on the motherboard of a computer.

**PCMCIA (Personal Computer Memory Code International Association) card**
A standard compact physical interface used in personal computers. The most common application of PCMCIA cards is for modems and storage.

**perfect forward secrecy (PFS)**
A cryptosystem in which the cipher text yields no possible information about the plain text, except possibly the length.

**PEM**
See *Privacy Enhanced Mail*.

**peer-to-peer**
A network computing system in which all computers are treated as equals on the network.

**peripherals**
Equipment such as disk drives, CD-ROM drives, modems, and printers that are connected to a computer.

**permission**
Authorization to perform an action.

**PGP**
See *Pretty Good Privacy*.

**PGP/MIME**
An IETF standard (RFC 2015) that provides privacy and authentication using the Multipurpose Internet Mail Extensions (MIME) security content types described in RFC1847, currently deployed in PGP 5.0 and later versions.

**Phase 1, Phase 2**
Stages in the IKE negotiation. Phase 1 authenticates the two parties and sets up a key management security association for protecting the data. Phase 2 negotiates data management security association, which uses the data management policy to set up IPSec tunnels in the kernel for encapsulating and decapsulating data packets.

**ping (packet Internet groper)**
A utility for determining whether a specific IP address is accessible. It works by sending a packet to the specified address and waiting for a reply.

**PKCS**
See *Public Key Crypto Standards*.

**PKI**
See *Public Key Infrastructure*.

**plain text**
Characters in a human-readable form prior to or after encryption. Also called *clear text*.

**PLIP (Parallel Line Internet Protocol)**
A protocol for exchanging IP packets over a parallel cable.

**Plug and Play**
A standard in the personal computer market that assures the user that the product is as simple to install as possible.

**Policy Manager**
One component in the WatchGuard Firebox System that provides a user interface for modifying and uploading a Firebox configuration file.

**pop-up window**
A window that suddenly appears (pops up) when an option is selected with a mouse or a function key is pressed.

**port**
A channel for transferring electronic information between a computer and a network, peripherals, or another computer.

**port address translation**
*See dynamic NAT.*

**portal**
A Web site that serves as a gateway to the World Wide Web and typically offers a search engine or links to other pages.

**port forwarding**
In the WatchGuard Firebox System, an option in which the Firebox redirects IP packets to a specific masqueraded host behind the firewall based on the original destination port number. Also called static NAT.

**port space probe**
An intrusion measure in which a hacker sequentially attacks port numbers. These probes are usually attempts to map port space to look for security holes which the sender might exploit.

**port, TCP or UDP**
A TCP or UDP service endpoint. Together with the hosts' IP addresses, ports uniquely identify the two peers of a TCP connection.

**PPP (Point-to-Point Protocol)**
A link-layer protocol used to exchange IP packets across a point-to-point connection, usually a serial line.

**PPPoE (Point-to-Point Protocol over Ethernet)**
A specification for connecting the users on an Ethernet to the Internet through a common broadband medium.

**PPTP (Point-to-Point Tunneling Protocol)**
A VPN tunnelling protocol with encryption. It uses one TCP port (for negotiation and authentication of a VPN connection) and one IP protocol (for data transfer) to connect the two peers in a VPN.

**Pretty Good Privacy (PGP)**
An application and protocol (RFC 1991) for secure email and file encryption. PGP uses a variety of algorithms, like IDEA, RSA, DSA, MD5, SHA-1, for providing encryption, authentication, message integrity, and key management.

**primary key (IPSec)**
An IPSec key responsible for creating a security association. Values can be set in time or data size.

**principle of precedence**
Rules that determine which permissions and prohibitions override which others when creating a combination of security policies.

**Privacy Enhanced Mail (PEM)**
A protocol to provide secure Internet mail (RFC 1421-1424), including services for encryption, authentication, message integrity, and key management. PEM uses ANSI X.509 certificates.

**private key**
The privately held "secret" component of an integrated asymmetric key pair, often referred to as the decryption key.

**probe**
A type of hacking attempt characterized by repetitious, sequential access attempts. For example, a hacker might try to probe a series of ports for one that is more open and less secure.

**protocol**
A set of formal rules describing how to transmit data, especially across a network. Low-level protocols define the electrical and physical standards to be observed, bit- and byte-ordering, and the transmission and error detection and correction of the bit stream. High-level protocols deal with the data formatting, including the syntax of messages, the terminal-to-computer dialog, character sets, and sequencing of messages.

**provisioning**
The process of setting the parameters of the Firebox or SOHO before it is sent to a customer. With respect to the Firebox, the minimum Policy Manager configuration is set with the most basic services on the box, Ping and WatchGuard. Provisioning also sets the IP addresses on the Firebox.

**proxy ARP**
The technique in which one host, usually a router, answers Address Resolution Protocol (ARP) requests intended for another machine. By "faking" its identity, the router accepts responsibility for routing packets to the "real" destination.

**proxy server**
A server that stands in place of another server. In firewalling, a proxy server poses as a specific service but has more rigid access and routing rules.

**pseudo-random number**
A number that results from applying randomizing algorithms to input derived from the computing environment, such as mouse coordinates. See also *random number*.

**public key**
The publicly available component of an integrated asymmetric key pair, often referred to as the encryption key.

**public key cryptography**
Cryptography in which a public and private key pair is used, and no security is needed in the channel itself.

***Public Key Crypto Standards***
A set of standards for public key cryptography developed in cooperation with an informal consortium (Apple, DEC, Lotus, Microsoft, MIT, RSA, and Sun) that includes algorithm-specific and algorithm-independent implementation standards.

**Public Key Infrastructure**
A widely available and accessible certificate system for obtaining an entity's public key.

**QuickSetup Wizard**
A wizard that creates a basic Firebox configuration. It consists of a series of windows that prompt for essential configuration information for drop-in or advanced network installations.

**RADIUS (Remote Authentication Dial-In User Service)**
A protocol for distributed security that secures remote access to networks and network services against unauthorized access. RADIUS consists of two pieces—authentication server code and client protocols.

**random number**
A necessary element in generating unique keys that are unpredictable to an adversary. True random numbers are typically derived from analog sources, and usually involve the use of special hardware.

**RC4 (Rivest Cipher 4)**
A variable key size stream cipher, once a proprietary algorithm of RSA Data Security, Inc.

**RC5 (Rivest Cipher 5)**
A block cipher with a variety of arguments, block size, key size, and number of rounds.

**related hosts**
A method to place hosts on the optional or external interface when using a simple or drop-in network configuration. Examples include placing a router on the external interface or an HTTP server on the optional interface.

**related networks**
Networks on the same physical wire as the Firebox interfaces but with network addresses that belong to an entirely different network.

**repeater**
A network device that regenerates signals so that they can extend the cable length.

**report**
A formatted collection of information that is organized to provide project data on a specific subject.

**revocation**
Retraction of certification or authorization.

**RFC (Request for Comments)**
RFC documents describe standards used or proposed for the Internet. Each RFC is identified by a number, such as RFC 1700. RFCs can be retrieved either by email or FTP.

**ring topology**
A basic networking topology in which all nodes are connected in a circle with no terminated ends on the cable.

**route**
The sequence of hosts through which information travels to reach its destination host.

**routed configuration or network**
A configuration with separate network addresses assigned to at least two of the three Firebox interfaces. This type of configuration is intended for situations in which the Firebox is put in place with separate logical networks on its interfaces.

**router**
A device, connected to at least two networks, that receives and sends packets between those networks. Routers use headers and a forwarding table to forward packets to their destination. Most rely on ICMP to communicate with one another and configure the best route between any two hosts.

**RUVPN (Remote User VPN)**
Remote User Virtual Private Networking establishes a secure connection between an unsecured remote host and a protected network over an unsecured network.

**salt**
A random string that is concatenated with passwords (or random numbers) before being operated on by a one-way function. This concatenation effectively lengthens and obscures the password, making the cipher text less susceptible to dictionary attacks.

**scalable architecture**
Software and/or hardware constructed so that, after configuring a single machine, the same configuration can be propagated to a group of connected machines.

**screening router**
A machine that performs packet filtering.

**SCSI (Small Computer System Interface)**
A processor-independent standard for system-level interfacing between a computer and intelligent devices including hard disks, floppy disks, CD-ROM, printers, and scanners.

**secondary network**
A network on the same physical wire as a Firebox interface that has an address belonging to an entirely different network.

**secret key**
Either the private key in public key (asymmetric) algorithms or the session key in symmetric algorithms.

**secret sharing**
See *key splitting*.

**secure channel**
A means of conveying information from one entity to another such that an intruder does not have the ability to reorder, delete, insert, or read.

**Secure Sockets Layer (SSL)**
A protocol for transmitting private documents over the Internet. SSL works by using a private key to encrypt data transferred over an SSL connection.

**SecurID server**
Each time an end user connects to the specialized-HTTP server running on the Firebox on port 4100, a Java-enabled applet opens and prompts for the username, password, and whether or not to use SecurID (PAP) Authentication. The username and password are DES-encrypted using a secret key shared between the Java client and the Firebox. The Firebox then decrypts the name and password to create a RADIUS PAP Access-Request packet, and then sends it to the configured RADIUS server.

**security traffic display**
An LED indicator on the front of a Firebox that indicates the directions of traffic between the Firebox interfaces. The display can either be a triangle display, for Fireboxes with three interfaces, or a star display, for Fireboxes with six interfaces.

**seed router**
A router that supplies routing information (such as network numbers and ranges) to the network.

**segment**
One or more nodes in a network. Segments are connected to subnets by hubs and repeaters.

**self-extracting file**
A compressed file that automatically decompresses when double-clicked.

**server**
A computer that provides shared resources to network users.

**server-based network**
A network in which all client computers use a dedicated central server computer for network functions such as storage, security, and other resources.

**Server Message Block (SMB)**
A message format used by DOS and Windows to share files, directories, and devices. NetBIOS is based on the SMB format, and many network products use SMB. These SMB-based networks include LAN Manager, Windows for Workgroups, Windows NT, and LAN Server.

**Services Arena**
An area in Policy Manager that displays the icons that represent the services (proxied and filtered) configured for a Firebox.

**ServiceWatch**
A graphical monitor that provides a real-time display that graphs how many connections exist, by service.

**session key**
The secret (symmetric) key used to encrypt each set of data on a transaction basis. A different session key is used for each communication session.

**session stealing**
An intrusion maneuver whereby a hacker sends a command to an already existing connection in order to have that command provide the information needed to stage a separate attack.

**setup keys (IKE)**
IKE keys responsible for creating a security association.

**SHA-1 (Secure Hash Algorithm)**
The 1994 revision to SHA, developed by NIST, (FIPS 180-1). When used with DSS, it produces a 160-bit hash, similar to MD4.

**shared secret**
A passphrase or password that is the same on the host and the client computer. It is used for authentication.

**SHTTP**
See *HTTPS*.

**sign**
To apply a signature.

**signature**
A digital code created with a private key.

**single sign-on**
A sign-on in which one logon provides access to all resources on the network.

**slash notation**
A format for writing IP addresses in which the number of bits in the IP number is specified at the end of the IP address. For example: 192.168.44.0/24.

**SLIP (Serial Line Internet Protocol)**
A protocol for exchanging IP packets over a serial line.

**S/MIME (Secure Multipurpose Mail Extension)**
A proposed standard for encrypting and authenticating MIME data. S/MIME defines a format for the MIME data, the algorithms that must be used for interoperability (RSA, RC2, SHA-1) and the additional operational concerns such as ANSI X.509 certificates and transport over the Internet.

**SMS (Security Management System)**
The former name of the GUI used to configure a Firebox. Now known as WatchGuard Policy Manager.

**SMTP (Simple Mail Transfer Protocol)**
A protocol for sending electronic messages between servers.

**social engineering attack**
An attack in which an individual is persuaded or tricked into divulging privileged information to an attacker.

**SOCKS**
A protocol for handling TCP traffic through a proxy server. It can be used with virtually any TCP application, including Web browsers and FTP clients. It provides a simple firewall because it checks incoming and outgoing packets and hides the IP addresses of client applications.

**SOHO**
Small Office–Home Office. Also the name of the WatchGuard firewall devices designed for this segment of the market.

**spam**
Unsolicited email sent to many recipients, much like an electronic version of junk mail.

**spoofing**
Altering packets to falsely identify the originating computer to confuse or attack another computer. The originating computer is usually misidentified as a trusted computer within an organization.

**SSL**
See *Secure Sockets Layer.*

**stance**
The policy of a firewall regarding the default handling of IP packets. Stance dictates what the firewall will do with any given packet in the absence of explicit instructions. The WatchGuard default stance is to discard all packets that are not explicitly allowed, often stated as "That which is not explicitly allowed is denied."

**star topology**
A networking setup used with 10BASE-T cabling and a hub in which each node on the network is connected to the hub like points of a star.

**static NAT**
Network address translation in which incoming packets destined for a public address on an external network are remapped to an address behind the firewall.

**stream cypher**
A class of symmetric key encryption where transformation can be changed for each symbol of plain text being encrypted; useful for equipment with little memory to buffer data.

**subnet**
A network segment connected by hubs or repeaters. For example, one could take a class C network with 256 available addresses and create two additional netmasks under it that separate the first 128 and last 128 addresses into separate identifiable networks. Subnetting enables a client with a single network to create multiple networks; the advanced or multiple network configurations can then be used when setting up the Firebox.

**subnet mask**
A 32-bit number used to identify which port of an IP address is masked.

**substitution cypher**
A method in which the characters of the plain text are substituted with other characters to form the cipher text.

**switch**
A device that filters and forwards packets between LAN segments.

**symmetric algorithm**
Also called conventional, secret key, and single key algorithms; the encryption and decryption key are either the same or can be calculated from one another.

**SYN flood attack**
A method of denying service to legitimate users by overloading a network with illegitimate TCP connection attempts.

**syslog**
An industry-standard protocol used for capturing log information for devices on a network. Syslog support is included in Unix-based and Linux-based systems.

**System Manager**
A WatchGuard toolkit of applications run from a single location, enabling configuration, management, and monitoring of a network security policy. Formerly called *Control Center*.

**TCP (Transmission Control Protocol)**
A reliable byte-streaming protocol that implements a virtual connection. Most long-haul traffic on the Internet uses TCP.

**TCP/IP (Transmission Control Protocol/Internet Protocol)**
A common networking protocol with the ability to connect different elements.

**TCP session hijacking**
An intrusion in which an individual takes over a TCP session between two machines. A hacker can gain access to a machine because most authentication occurs only at the start of the TCP session.

**Telnet**
A terminal emulation program for TCP/IP networks. It runs on a computer and connects a workstation to a server on a network.

**terminator**
A resistor at the end of an Ethernet cable that absorbs energy to prevent reflected energy back along the cable (signal bounce). It is usually attached to an electrical ground at one end.

**Thick Ethernet cable**
Industry-standard Ethernet cable or any other cable that uses the IEEE 802.3 Media Access Unit interface. Also called 10-BASE-5.

**Thin Ethernet cable**
IEEE 802.3, 10BASE2 cable that connects to the Ethernet cable system with a cylindrical BNC connector. Usually, quarter-inch black coaxial cable.

**timestamping**
Recording the time of creation or existence of information.

**TLS**
See *Transport Layer Security.*

**TLSP**
See *Transport Layer Security Protocol*.

**token**
An abstract concept passed between cooperating agents to ensure synchronized access to a shared resource. Whoever has the token has exclusive access to the resource it controls.

**tooltip**
A name or phrase that appears when the mouse pointer pauses over a button or icon.

**topology**
A wiring configuration used for a network.

**Transport Layer Security (TLS)**
Based on the Secure Sockets Layer (SSL) version 3.0 protocol, TLS provides communications privacy over the Internet.

**Transport Layer Security Protocol (TLSP)**
ISO 10736, draft international standard.

**transposition cipher**
A cipher in which the plain text remains the same but the order of the characters is transposed.

**triple-DES**
An advanced form of encryption using three keys rather than one or two. It is roughly as secure as single DES would be if it had a 112-bit key.

**trust**
Confidence in the honesty, integrity, or reliability of a person, company, or other entity.

**Trusted interface**
The interface on the Firebox that connects to the internal network, which should be protected to the maximum practical amount.

**Trusted network**
The network behind the firewall that must be protected from the security challenge—usually, the Internet.

**tunnel**
An entity through which one network sends its data by way of another network's connections. Tunneling works by encapsulating a network protocol within packets carried by the second network. For example, Microsoft's PPTP technology enables organizations to use the Internet to transmit data across a virtual private network (VPN). It does this by embedding its own network protocol within the TCP/IP packets carried by the Internet.

**twisted-pair cable**
A cable used for both network and telephone communications. Also known as UTP (unshielded twisted pair) and 10BASE-T/100BASE-T cable.

**UDP (User Datagram Protocol)**
A connectionless protocol. Used less frequently for long-distance connections, largely because it lacks TCP's congestion control features. Used quite heavily in local area networks for NFS.

**URL (Universal Resource Locator)**
The user-friendly address that identifies the location of a Web site such as http://www.watchguard.com.

**validation**
A means to provide timeliness of authorization to use or manipulate information or resources.

**verification**
The act of comparing a signature created with a private key to its public key. Verification proves that the information was actually sent by the signer and that the message has not been subsequently altered by anyone else.

**VPN (virtual private network)**
A virtual, secured network over a public or unsecure network (such as the Internet) where the alternative—a dedicated physical network—is either prohibitively expensive or impossible to create. Companies with branch offices commonly use VPNs to connect multiple locations.

**WAN (wide area network)**
A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local area networks (LANs).

**WatchGuard installation directory**
The directory into which the WatchGuard Firebox System software is installed by default.

**WatchGuard LiveSecurity Service**
Part of the WatchGuard Firebox System offering, separate from the software and the Firebox, which keeps network defenses current. It includes the broadcast network that transmits alerts, editorials, threat responses, and software updates via email; a technical support contract; and a Web site containing information, archives, online training, and the latest software.

**WatchGuard Security Event Processor (WSEP)**
A program that controls notification and logging on the log hosts. It provides critical timing services for the Firebox and includes its own GUI.

**Web browser**
Software that interprets and displays documents formatted for the Internet or an intranet.

**Web of Trust**
A distributed trust model used by PGP to validate the ownership of a public key.

**Web page**
A single HTML-formatted file.

**Web site**
A collection of Web pages located in the directory tree under a single home page.

**WebBlocker**
An optional WatchGuard software module that blocks users behind the Firebox from accessing undesirable Web sites based on content type, time of day, and/or specific URL.

**WINS (Windows Internet Name Service)**
WINS provides name resolution for clients running Windows NT and earlier versions of Microsoft operating systems. With name resolution, users access servers by name rather than needing to use an IP address.

**wizard**
A tool that guides a user through a complex task by asking questions and then performing the task based on responses.

**World Wide Web (WWW)**
The collection of available information on the Internet viewable using a Web browser.

**World Wide Web Consortium (W3C)**
An international industry consortium founded in 1994 to develop common protocols for the evolution of the World Wide Web.

**worm**
A program that seeks access into other computers. After a worm penetrates another computer, it continues seeking access to other areas. Worms often steal or vandalize computer data. Many viruses are actually worms that use email or database systems to propagate themselves to other victims.

**XOR**
Exclusive-or operation; a mathematical way to represent differences.

**X.509v3**
An ITU-T digital certificate that is an internationally recognized electronic document used to prove identity and public key ownership over a communication network. It contains the issuer's name, the user's identifying information, and the issuer's digital signature, as well as other possible extensions in version 3.

# Index

# E



# F

# H



# I



# L



# M

# N



# O



# P

# R



# S

# T



# U



# V

# W



# Z