

# *ZyWALL IDP 10*

*Intrusion Detection and Prevention Appliance*

## *User's Guide*

Version 2.0  
3/2005



# Copyright

Copyright © 2005 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

## **Disclaimer**

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

## **Trademarks**

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

# Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

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

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

If this equipment does cause harmful interference to radio/television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

## Notice 1

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

## Certifications

Go to [www.zyxel.com](http://www.zyxel.com)

- 1 Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.
- 2 Select the certification you wish to view from this page.

# Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel can service the device. Please contact your vendor for further information.
- Use ONLY the dedicated power supply for your device. Connect the power cord or power adaptor to the right supply voltage (110V AC in North America or 230V AC in Europe).
- Do NOT use the device if the power supply is damaged as it might cause electrocution.
- If the power supply is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power supply. Contact your local vendor to order a new power supply.
- Place connecting cables carefully so that no one will step on them or stumble over them. Do NOT allow anything to rest on the power cord and do NOT locate the product where anyone can walk on the power cord.
- Do NOT install nor use your device during a thunderstorm. There may be a remote risk of electric shock from lightning.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Make sure to connect the cables to the correct ports.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Do NOT store things on the device.
- Connect ONLY suitable accessories to the device.

# ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

## Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind of character to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

# Customer Support

Please have the following information ready when you contact customer support.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

METHOD	SUPPORT E-MAIL	TELEPHONE <sup>A</sup>	WEB SITE	REGULAR MAIL
LOCATION	SALES E-MAIL	FAX	FTP SITE	
CORPORATE HEADQUARTERS (WORLDWIDE)	support@zyxel.com.tw	+886-3-578-3942	www.zyxel.com www.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
	sales@zyxel.com.tw	+886-3-578-2439	ftp.zyxel.com ftp.europe.zyxel.com	
CZECH REPUBLIC	info@cz.zyxel.com	+420 241 091 350	www.zyxel.cz	ZyXEL Communications Czech s.r.o. Modranská 621 143 01 Praha 4 - Modrany Ceská Republika
	info@cz.zyxel.com	+420 241 091 359		
DENMARK	support@zyxel.dk	+45 39 55 07 00	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 5 2860 Soeborg Denmark
	sales@zyxel.dk	+45 39 55 07 07		
FINLAND	support@zyxel.fi	+358-9-4780-8411	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland
	sales@zyxel.fi	+358-9-4780 8448		
FRANCE	info@zyxel.fr	+33 (0)4 72 52 97 97	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
		+33 (0)4 72 52 19 20		
GERMANY	support@zyxel.de	+49-2405-6909-0	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
	sales@zyxel.de	+49-2405-6909-99		
NORTH AMERICA	support@zyxel.com	+1-800-255-4101 +1-714-632-0882	www.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
	sales@zyxel.com	+1-714-632-0858	ftp.us.zyxel.com	
NORWAY	support@zyxel.no	+47 22 80 61 80	www.zyxel.no	ZyXEL Communications A/S Nils Hansens vei 13 0667 Oslo Norway
	sales@zyxel.no	+47 22 80 61 81		
SPAIN	support@zyxel.es	+34 902 195 420	www.zyxel.es	ZyXEL Communications Alejandro Villegas 33 1º, 28043 Madrid Spain
	sales@zyxel.es	+34 913 005 345		
SWEDEN	support@zyxel.se	+46 31 744 7700	www.zyxel.se	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden
	sales@zyxel.se	+46 31 744 7701		

METHOD	SUPPORT E-MAIL	TELEPHONE <sup>A</sup>	WEB SITE	REGULAR MAIL
	SALES E-MAIL	FAX	FTP SITE	
UNITED KINGDOM	support@zyxel.co.uk	+44 (0) 1344 303044 08707 555779 (UK only)	www.zyxel.co.uk	ZyXEL Communications UK Ltd., 11, The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom (UK)
	sales@zyxel.co.uk	+44 (0) 1344 303034	ftp.zyxel.co.uk	

a. "+" is the (prefix) number you enter to make an international telephone call.

# Table of Contents

<b>Copyright .....</b>	<b>2</b>
<b>Federal Communications Commission (FCC) Interference Statement .....</b>	<b>3</b>
<b>Safety Warnings .....</b>	<b>4</b>
<b>ZyXEL Limited Warranty .....</b>	<b>5</b>
<b>Customer Support.....</b>	<b>6</b>
<b>Table of Contents .....</b>	<b>8</b>
<b>List of Figures .....</b>	<b>12</b>
<b>List of Tables .....</b>	<b>14</b>
<b>Preface .....</b>	<b>16</b>
<b>Chapter 1</b>	
<b>Introducing the ZyWALL IDP 10.....</b>	<b>18</b>
1.1 Introduction .....	18
1.2 Features .....	19
1.3 Application Examples .....	20
<b>Chapter 2</b>	
<b>Introducing the Web Configurator.....</b>	<b>24</b>
2.1 Web Configurator Overview .....	24
2.2 Accessing the ZyWALL Web Configurator .....	24
2.3 Navigating the ZyWALL Web Configurator .....	25
2.4 Example Configuration Settings .....	28
<b>Chapter 3</b>	
<b>General Settings.....</b>	<b>30</b>
3.1 Device .....	30
3.2 Introduction to VLANs .....	31
3.2.1 Tagged VLANs (IEEE 802.1Q) .....	31
3.3 Configuring VLAN on the ZyWALL .....	32
3.3.1 State .....	33



<b>Chapter 4</b>	
<b>Interface Screens .....</b>	<b>36</b>
4.1 10/100M Auto-Sensing Ethernet Ports .....	36
4.2 Configuring Link .....	36
4.3 Stealth .....	37
4.4 Policy Check .....	38
4.4.1 Policy Direction .....	39
<b>Chapter 5</b>	
<b>Remote Management .....</b>	<b>42</b>
5.1 Remote Management Overview .....	42
5.1.1 HTTPS .....	42
5.1.2 Remote Management and Stealth .....	43
5.2 Configuring WWW .....	43
5.3 SNMP .....	44
5.3.1 Supported MIBs .....	46
5.3.2 SNMP Traps .....	46
5.3.3 SNMP Configuration .....	46
5.4 SSH Overview .....	47
5.4.1 How SSH works .....	47
5.4.2 SSH Implementation on the ZyWALL .....	48
5.4.3 Requirements for Using SSH .....	48
5.5 SSH (Secure SHell) Configuration .....	48
5.5.1 Example Using SSH .....	49
<b>Chapter 6</b>	
<b>IDP Policies .....</b>	<b>52</b>
6.1 IDP Overview .....	52
6.2 mySecurity Zone .....	52
6.3 Signature Categories .....	53
6.3.1 P2P .....	53
6.3.2 IM .....	54
6.3.3 SPAM .....	55
6.3.4 DoS/DDoS .....	55
6.3.5 Scan .....	56
6.3.6 Buffer Overflow .....	57
6.3.7 Virus/Worm .....	58
6.3.8 Backdoor/Trojan .....	59
6.3.9 Access Control .....	60
6.3.10 Web Attack .....	61
6.3.11 Porn .....	62
6.3.12 Others .....	63
6.3.13 Policy Severity .....	64

6.3.14 Policy Actions .....	65
6.4 Configuring Pre-defined Policies .....	65
6.4.1 Search Example .....	68
6.4.2 Query Example .....	69
6.4.3 Modify Screen .....	70
6.5 Update .....	72
6.6 User-defined Policies .....	73
6.6.1 Configuring a User-defined IDP Policy .....	76
6.6.2 Packet Content Example .....	80
6.7 Registering your ZyWALL .....	81
<b>Chapter 7</b>	
<b>Log and Report.....</b>	<b>84</b>
7.1 Logs .....	84
7.2 Report .....	85
7.2.1 E-Mail .....	85
7.2.2 Syslog .....	87
7.3 Alarm Schedule .....	88
<b>Chapter 8</b>	
<b>Maintenance .....</b>	<b>90</b>
8.1 Maintenance Overview .....	90
8.2 Password .....	90
8.2.1 Forget Password .....	91
8.3 Time and Date .....	91
8.3.1 Pre-defined NTP Time Servers List .....	92
8.3.2 Time Server Synchronization .....	94
8.4 Firmware Upload .....	95
8.5 Configuration .....	98
8.5.1 Backup Configuration .....	99
8.5.2 Restore Configuration .....	99
8.5.3 Back to Factory Defaults .....	100
8.6 Restart .....	100
<b>Chapter 9</b>	
<b>Command Line Interface Overview .....</b>	<b>102</b>
9.1 Command Syntax Conventions .....	102
9.1.1 Help Facility .....	103
9.2 Login .....	103
9.3 Commands .....	103
<b>Appendix A</b>	
<b>Introduction to Intrusions .....</b>	<b>108</b>

Introduction to Ports .....	108
Introduction to Denial of Service .....	108
Scanning .....	111
Malicious Programs.....	112
Example Intrusions.....	113
<b>Appendix B</b>	
<b>Intrusion Protection .....</b>	<b>116</b>
Firewalls and Intrusions .....	116
Intrusion Detection and Prevention (IDP) .....	116
Detection Methods .....	117
<b>Index.....</b>	<b>120</b>

# List of Figures

Figure 1 ZyWALL .....	19
Figure 2 Installation Example 1 .....	21
Figure 3 Installation Example 2 .....	21
Figure 4 Installation Example 3 .....	22
Figure 5 Installation Example 4 .....	22
Figure 6 Default Web Configurator IP Address .....	24
Figure 7 Login Screen .....	25
Figure 8 Change Password Screen .....	25
Figure 9 Web Configurator HOME Screen .....	26
Figure 10 General: Device .....	30
Figure 11 General: VLAN .....	33
Figure 12 General: State .....	33
Figure 13 Interface: Link .....	37
Figure 14 Interface: Stealth .....	38
Figure 15 Policy Checking .....	39
Figure 16 Interface: Policy Check .....	40
Figure 17 Remote Management: WWW .....	43
Figure 18 SNMP Management Model .....	45
Figure 19 Remote Management: SNMP .....	46
Figure 20 SSH Communication Example .....	47
Figure 21 How SSH Works .....	48
Figure 22 Remote Management: SSH .....	49
Figure 23 PuTTY Settings .....	50
Figure 24 PuTTY Security Alert .....	50
Figure 25 ZyWALL Command Interface Login Screen .....	51
Figure 26 P2P Signatures .....	54
Figure 27 IM (Chat) Signatures .....	55
Figure 28 Spam Signatures .....	55
Figure 29 DoS/DDoS Signatures .....	56
Figure 30 Scan Signatures .....	57
Figure 31 Buffer Overflow Signatures .....	58
Figure 32 Worm/Virus Signatures .....	59
Figure 33 Backdoor/Trojan Signatures .....	60
Figure 34 Access Control Signatures .....	61
Figure 35 Web Attack Signatures .....	62
Figure 36 Porn Signatures .....	63
Figure 37 Others Signatures .....	64
Figure 38 Pre-defined IDP Policies Summary .....	66

Figure 39 Search Example .....	69
Figure 40 Query Example .....	70
Figure 41 Pre-defined Policies: Modify .....	71
Figure 42 Update Policies .....	72
Figure 43 User-defined Policies .....	74
Figure 44 Configuring a User-defined IDP Policy .....	77
Figure 45 Registering ZyWALL .....	82
Figure 46 View Log .....	84
Figure 47 Report: E-Mail .....	86
Figure 48 Report: syslog .....	87
Figure 49 Alarm .....	88
Figure 50 Maintenance: Password .....	90
Figure 51 Debug Mode Reset Example .....	91
Figure 52 Maintenance: Time Setting .....	93
Figure 53 Synchronization in Process .....	95
Figure 54 Synchronization is Successful .....	95
Figure 55 Synchronization Fail .....	95
Figure 56 Maintenance: F/W Upload .....	96
Figure 57 Firmware Upload in Progress .....	97
Figure 58 Network Temporarily Disconnected .....	98
Figure 59 Firmware Upload Error .....	98
Figure 60 Maintenance: Configuration .....	99
Figure 61 Maintenance: Restart .....	100
Figure 62 Three-Way Handshake .....	109
Figure 63 SYN Flood .....	110
Figure 64 Smurf Attack .....	111

# List of Tables

Table 1 Web Configurator HOME Screen .....	26
Table 2 Screens Summary .....	27
Table 3 Example Configuration Settings .....	28
Table 4 General: Device .....	31
Table 5 General: VLAN .....	33
Table 6 General: State .....	34
Table 7 Interface: Link .....	37
Table 8 Interface: Stealth .....	38
Table 9 Interface: Policy Check .....	40
Table 10 Remote Management: WWW .....	43
Table 11 SNMP Traps .....	46
Table 12 Remote Management: SNMP .....	47
Table 13 Remote Management: SSH .....	49
Table 14 Policy Severity .....	64
Table 15 Policy Actions .....	65
Table 16 Selecting Pre-defined Policies .....	66
Table 17 Pre-defined IDP Policies .....	71
Table 18 Update Policies .....	72
Table 19 User-defined Policies .....	74
Table 20 Configuring a User-defined IDP Policy .....	78
Table 21 Registering ZyWALL .....	82
Table 22 View Log .....	85
Table 23 Report: E-Mail .....	86
Table 24 Report: syslog .....	87
Table 25 Alarm .....	89
Table 26 Maintenance: Password .....	90
Table 27 Default Time Servers .....	92
Table 28 Time and Date .....	93
Table 29 Maintenance: F/W Upload .....	96
Table 30 Restore Configuration .....	99
Table 31 Commands Summary .....	103
Table 32 Common IP Ports .....	108
Table 33 Common Malicious Programs .....	112



# Preface

Congratulations on your purchase of the ZyWALL IDP 10.

## About This User's Guide

Congratulations on your purchase of the ZyWALL IDP 10 Intrusion Detection Prevention Appliance. This manual is designed to guide you through the configuration of your ZyWALL for its various applications.

## Related Documentation

- **Support Disk:** Refer to the included CD for support documents.
- **Quick Start Guide:** The Quick Start Guide is designed to help you get up and running right away. It contains hardware (connection) information, basic troubleshooting and shows you how to configure the device using the wizard.
- **Web Configurator Online Help:** Embedded web help for descriptions of individual screens and supplementary information.
- **Packing List Card:** The Packing List Card lists all items that should have come in the package.
- **Certifications:** Refer to the product page at [www.zyxel.com](http://www.zyxel.com) for information on product certifications.
- **ZyXEL Glossary and Web Site:** Please refer to [www.zyxel.com](http://www.zyxel.com) for an online glossary of networking terms and additional support documentation.

## User Guide Feedback










Help us help you. E-mail all User Guide-related comments, questions or suggestions for improvement to [techwriters@zyxel.com.tw](mailto:techwriters@zyxel.com.tw) or send regular mail to The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Thank you.

## Syntax Conventions

- This manual will refer to the ZyWALL IDP 10 Intrusion Detection Prevention Appliance simply as the ZyWALL.
- The version number on the title page is the latest firmware version that is documented in this User's Guide. Earlier versions may also be included.
- "Enter" means for you to type one or more characters and press the carriage return. "Select" or "Choose" means for you to use one of the predefined choices.
- The choices of a menu item are in Bold Arial font.
- Mouse action sequences are denoted using a comma. For example, "click the Apple icon, Control Panels and then Modem" means first click the Apple icon, then point your mouse pointer to Control Panels and then click Modem.
- For brevity's sake, we will use "e.g." as a shorthand for "for instance" and "i.e." for "that is" or "in other words" throughout this manual.



## Graphics Icons Key

<p>Prestige</p> 	<p>Computer</p> 	<p>Modem</p> 
<p>Switch</p> 	<p>Firewall</p> 	<p>Server</p> 
<p>Intrusion</p> 	<p>Block an intrusion</p> 	<p>Security Hole</p> 

# CHAPTER 1

## Introducing the ZyWALL IDP 10

This chapter introduces the main features and applications of the ZyWALL.

### 1.1 Introduction

An IDP system can detect malicious or suspicious packets and respond instantaneously. It can detect anomaly detections based on violations of protocol standards (RFCs – Requests for Comments) or traffic flows and abnormal flows such as port scans. The rules that define how to identify and respond to intrusions are called “signatures”.

**Note:** See *the appendices* for more detailed information on intrusions, intrusion examples and detection types.

The ZyWALL is an Intrusion Detection and Prevention (IDP) Appliance designed to protect against network-based intrusions. The ZyWALL functions as a transparent plug and play bridge designed to protect networks from intrusions while allowing safe Internet access.

The ZyWALL comes with a built-in signature set that can be regularly updated. Regular updates are vital as new intrusions evolve.

For people with knowledge of packet header types and OSI (Open System Interconnection), the IDP allows you to create your own rules.

You can configure the ZyWALL using the friendly, embedded web configurator or the command-line interface you access via the console port.

**Figure 1** ZyWALL

## 1.2 Features

### LAN, WAN and Management Ports

You can also manage the ZyWALL via the **LAN** or **WAN** port, but the **MGMT** port is dedicated for management. If you manage the ZyWALL via the LAN or WAN port then the ZyWALL itself may be susceptible to being compromised.

### Intrusion Detection & Prevention (IDP)

- Real-time detection & prevention system at structure
- Inline, Monitor, Bypass modes
- Automatic signature update
- Protect against:
  - DoS and DDoS attacks
  - Buffer overflow
  - Network and port scans
  - Trojan Horse attacks
  - Back Door attacks
  - Worms
- Detection Methods:
  - Heuristic Analysis based on exceeding statistical thresholds such as abnormal port scan probes.
  - Pattern Matching where a signature database identifies malicious code strings in packets.
  - Protocol Anomaly Detection based on RFC protocol violations.

- Traffic flow anomalies where certain applications such as peer-to-peer applications for example are defined as “abnormal” and therefore an “intrusion”.
- Stateful pattern matching based on reassembling TCP streams to make the complete string available to the detection engine.
- User-defined rules allow:
  - Multiple Attack Pattern Detection
  - Multiple string match
  - IP/TCP/UDP/ICMP and IGMP packets filters that block suspect attack sources.

### **Firmware Upgrade**

- Automatically schedule download and upgrade

### **Logs & Reports**

- Automatically schedule reports sent by E-mail.
- Alarms are urgent notification of attacks.

### **System Management**

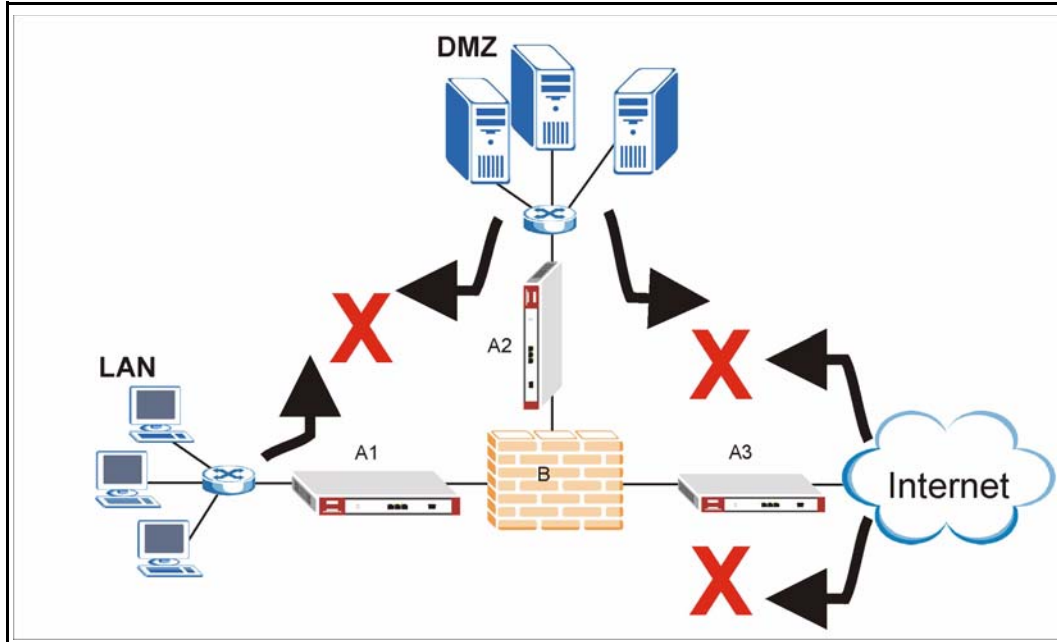
- Console (RS-232)
- Web-based GUI (HTTP and HTTPS)
- Command line interface
- SNMP v2c

## **1.3 Application Examples**

You can install a ZyWALL either between the firewall (or switch) and Internet (see [Figure 2 on page 21](#)) to protect your local networks and firewall (or switch) from intrusions from the Internet, behind the firewall (or switch) to protect the DMZ servers from intrusions from the local network (due to an infected LAN computer, for example), or ideally, install one in front of the firewall and two others behind the firewall.

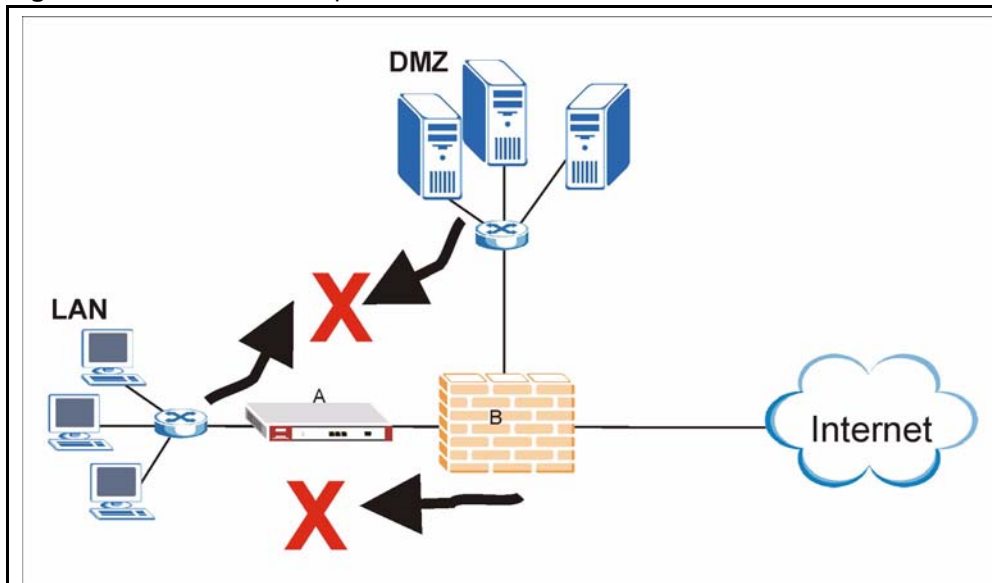
In installation example 1 ([Figure 2 on page 21](#)) the ZyWALL (A) protects the firewall/router (B), DMZ servers and LAN computers from network intrusions from the Internet. However, it does not protect the DMZ servers from intrusions from the LAN (and vice versa), and the ZyWALL itself is vulnerable, as it does not receive firewall protection.

**Figure 2** Installation Example 1

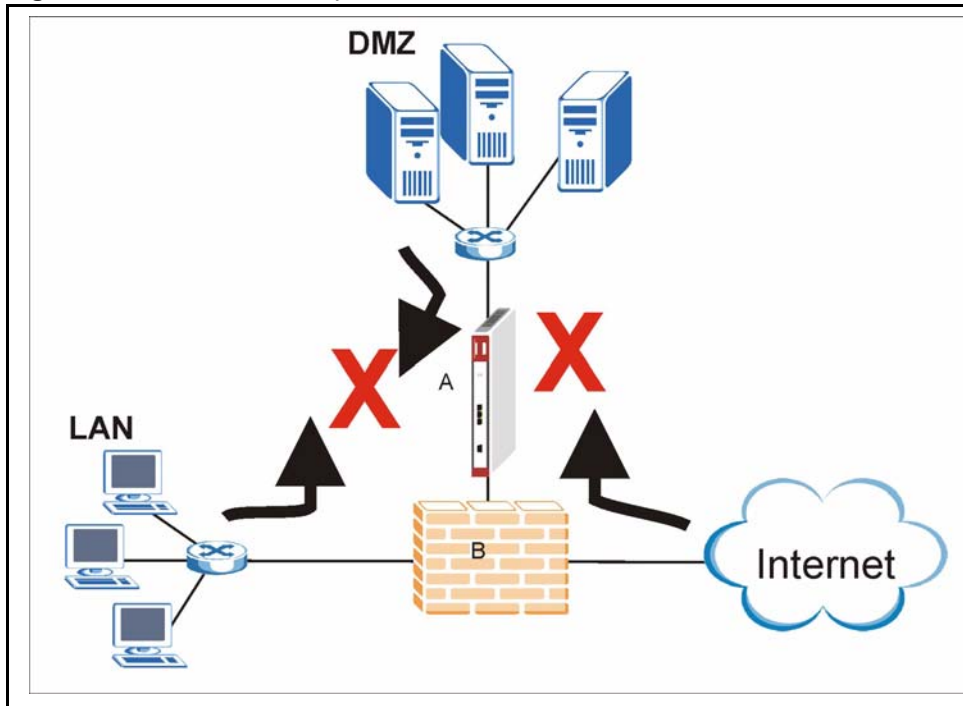


In installation example 2 (see [Figure 3 on page 21](#)) the ZyWALL (A) protects the LAN from intrusions from the Internet and the DMZ servers from intrusions from the LAN (and vice versa). The ZyWALL itself receives firewall protection too. However, it does not protect the firewall (B) nor the DMZ servers from intrusions from the Internet.

**Figure 3** Installation Example 2

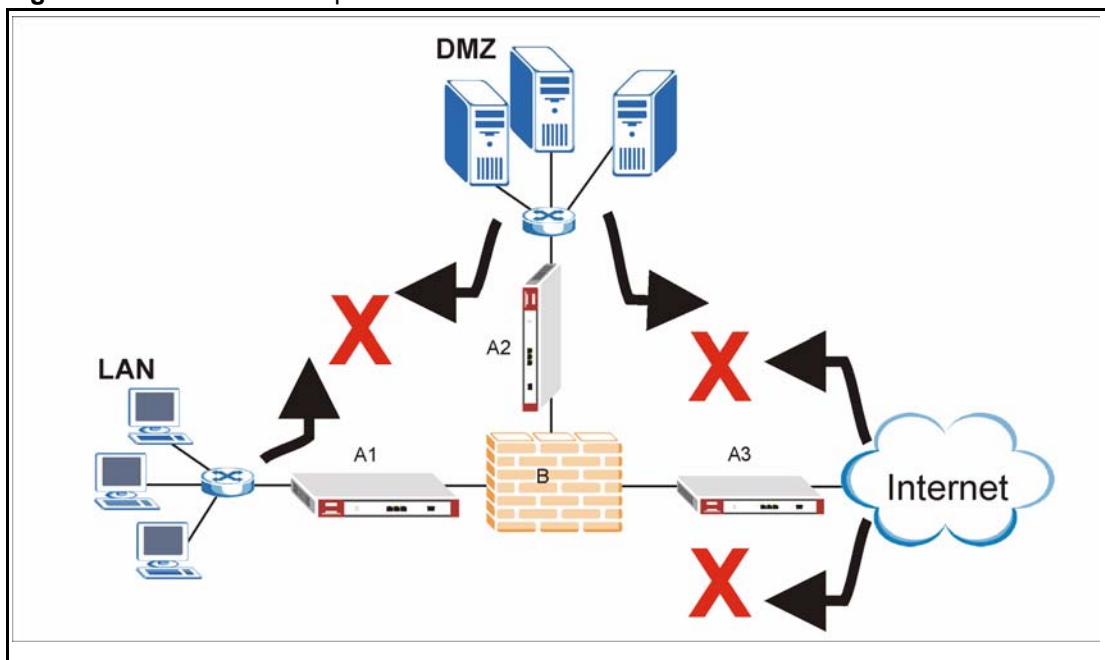


In installation example 3 (see [Figure 4 on page 22](#)) the ZyWALL (A) protects the DMZ servers from intrusions from the Internet and also from intrusions from the LAN (and vice versa). The ZyWALL itself receives firewall protection too. However, it does not protect the LAN computers nor the firewall (B) from intrusions from the Internet.

**Figure 4** Installation Example 3

In installation example 4 (see [Figure 5 on page 22](#)) ZyWALLs (A1 and A3) protect the LAN and DMZ from intrusions from the Internet and from each other. ZyWALLs (A1 and A3) also receive firewall protection.

ZyWALL (A2) protects the firewall (B), DMZ servers (and LAN). However, ZyWALL (A2) does not receive firewall protection.

**Figure 5** Installation Example 4



# CHAPTER 2

## Introducing the Web Configurator

This chapter describes how to access the ZyWALL web configurator and provides an overview of its screens.

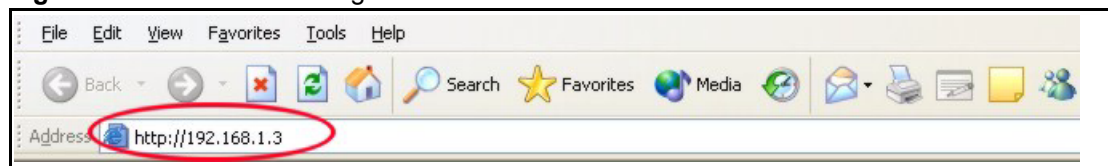
### 2.1 Web Configurator Overview

The embedded web configurator (eWC) allows you to manage the ZyWALL from anywhere through a browser such as Microsoft Internet Explorer or Netscape Navigator. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions with JavaScript enabled. It is recommended that you set your screen resolution to 1024 by 768 pixels. The screens you see in the web configurator may vary somewhat from the ones shown in this document due to differences between individual firmware versions.

### 2.2 Accessing the ZyWALL Web Configurator

- 1 Make sure your ZyWALL hardware is properly connected and prepare your computer/ computer network to connect to the ZyWALL (refer to the *Quick Start Guide*).
- 2 Launch your web browser and type "192.168.1.3" as the URL.

**Figure 6** Default Web Configurator IP Address



- 3 Type "1234" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.

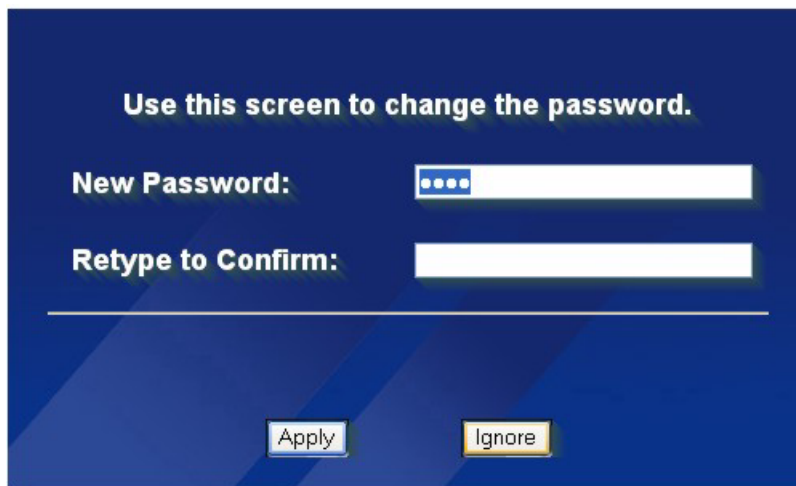


**Figure 7** Login Screen



- 4 You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) and click **Apply** or click **Ignore**.

**Figure 8** Change Password Screen

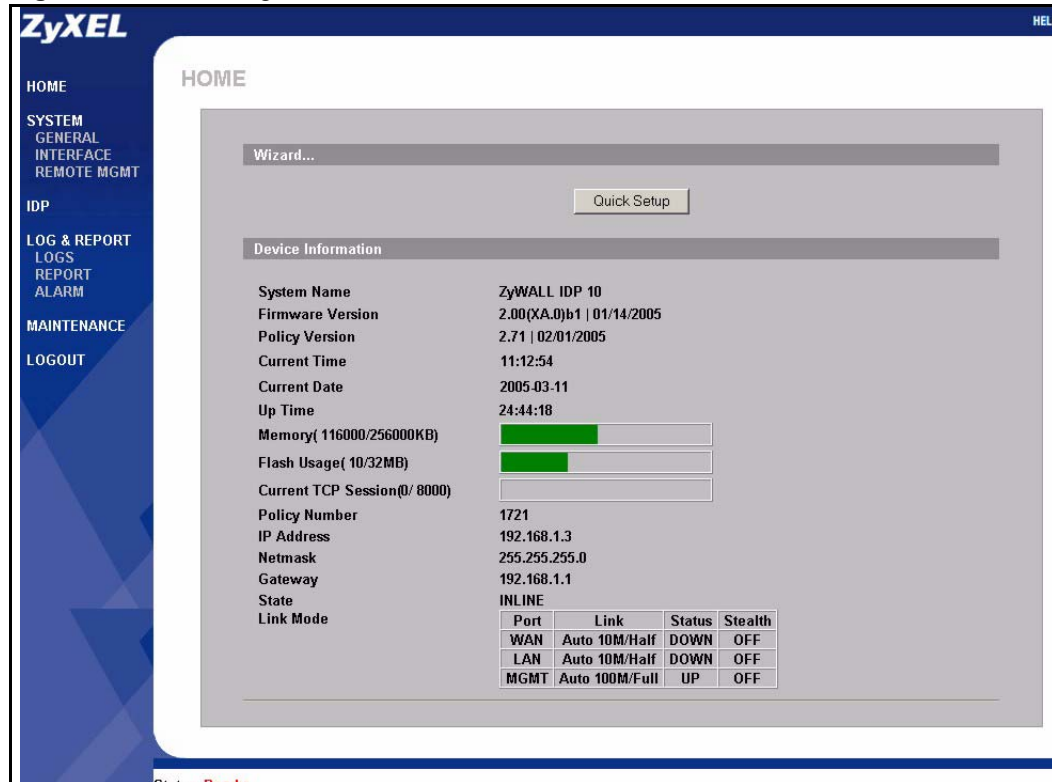


- 5 You should now see the **HOME** screen (see [Figure 9 on page 26](#)).

## 2.3 Navigating the ZyWALL Web Configurator

The following summarizes how to navigate the web configurator from the **HOME** screen.

You can configure the ZyWALL's IP address in order to access it for management. All LAN, WAN, DNZ and WLAN ports act as a hub and share the same IP address.

**Figure 9** Web Configurator HOME Screen

Use submenus to configure ZyWALL features.

Click **MAINTENANCE** to view information about your ZyWALL or upgrade configuration/firmware files. Maintenance includes **Password**, **Time Setting**, **F/W (firmware) Upload**, **Configuration** (Backup, Restore, Default), and **Restart**.

Click **LOGOUT** at any time to exit the web configurator.

The following table describes the labels in this screen.

**Table 1** Web Configurator HOME Screen

LABEL	DESCRIPTION
Wizard...	
Quick Setup	Click <b>Quick Setup</b> to start the ZyWALL setup wizard.
Device Information	
System Name	The system name identifies your device type. The system name should also be on a sticker on your device. If you are uploading firmware, be sure to upload firmware for this exact system name.
Firmware Version	This is the firmware version number and the date created.
Policy Version	This field displays the intrusion signature set version number and the date updated
Current Time	This field displays the present time as configured on the device.
Current Date	This field displays the present date as configured on the device.

**Table 1** Web Configurator HOME Screen (continued)

LABEL	DESCRIPTION
Up Time	This field displays the total time in seconds since the ZyWALL was last turned on.
Memory	The first number shows how many kilobytes of the heap memory the ZyWALL is using. Heap memory refers to the memory that is used by the ZYWALL operating system. The second number shows the ZyWALL's total heap memory (in kilobytes). The bar displays what percent of the ZyWALL's heap memory is in use. The bar is green when less than 70% is in use and red when more than 70% is in use.
Flash Usage	The first number shows the amount of flash (non-volatile) memory used by the ZyWALL. The bar displays what percentage of disk space is in use. The bar is green when less than 70% is in use and red when more than 70% is in use. The second number shows the total available disk space (in megabytes).
Current TCP Session	This field displays number of TCP sessions currently established.
Policy Number	This field displays the number of signature "rules" for the displayed policy version.
IP Address	This shows the ZyWALL's IP address. The LAN, WAN and MGMT ports all use the same IP address.
Netmask	This shows the ZyWALL's subnet mask.
Gateway	This field displays the IP address of the gateway. The gateway is an immediate neighbor of your ZyWALL that will forward the packet to the destination. The gateway must be on the same segment as your ZyWALL. The gateway and DNS settings are only relevant to the internal functions (SNMP, e-mail, syslog) of the ZyWALL.
State	This field displays whether the ZyWALL is <b>Inline</b> (configure an action for suspicious packets), <b>Monitor</b> (send out alerts only for suspicious packets) or <b>Bypass</b> (all traffic can pass through the ZyWALL without inspection).
Link Mode	This field displays whether each port is up or down, the speed (10M or 100M), the duplex mode (full or half) and whether stealth is enabled.

### 2.1.1 Navigation Panel

After you enter the password, use the sub-menus on the navigation panel to configure ZyWALL features.

The following table describes the sub-menus.

**Table 2** Screens Summary

LINK	TAB	FUNCTION
Home		This screen shows the ZyWALL's general device information. Use this screen to access the setup wizard.
SYSTEM		Access the <b>GENERAL</b> , <b>INTERFACE</b> and <b>REMOTE MGMT</b> links from here.
GENERAL	Device	Use this screen to configure device TCP/IP settings and TCP idle timeout.
	VLAN	Use this screen to configure the VLAN tag and VLAN ID.
	State	Use this screen to set the intrusion operating state ( <b>Inline</b> , <b>Monitor</b> or <b>Bypass</b> ).
INTERFACE	Link	Use this screen to set each port's speed and duplex mode.
	Stealth	Use this screen to enable/disable stealth on the LAN or WAN ports.

**Table 2** Screens Summary (continued)

LINK	TAB	FUNCTION
	Policy Check	Policy check determines the interface on which traffic will be checked against the ZyWALL policy rules (both pre-defined and user-defined). By selecting <b>LAN port</b> , then only traffic coming into the LAN and out through the WAN will be checked. Similarly, by selecting <b>WAN port</b> , then only traffic coming into the WAN and out through the LAN will be checked.
REMOTE MGMT	WWW	Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTP to manage the ZyWALL.
	SNMP	Use this screen to configure Simple Network Management Protocol (SNMP) ZyWALL management.
	SSH	Use this screen to configure through which interface(s) and from which IP address(es) users can use Secure Shell to manage the ZyWALL.
IDP	Pre-defined	All pre-defined IDP policies are already stored in the ZyWALL by default. Use this screen to see all pre-defined policies or search for specific ones.
	Update	Use this screen to set the IP address of the update server and to schedule automatic downloading.
	User-defined	Use screen to create your own intrusion protection policies.
	Registration	Use this screen to register for IDP update server downloads.
LOG & REPORT		Access the <b>LOGS</b> , <b>REPORT</b> and <b>ALARM</b> links from here.
LOGS	View Log	Use this screen to view the logs for the categories that you selected.
REPORT	E-Mail	Use this screen to configure and schedule e-mailed log reports.
	syslog	A syslog server is an external logging server used to store and parse logs.
ALARM	ALARM	Use this screen to configure and set the frequency of (e-mailed) alarms.
MAINTENANCE	Password	Use this screen to change your password.
	Time Setting	Use this screen to set your ZyWALL's time and date.
	F/W Upload	Use this screen to configure and schedule firmware uploads to your ZyWALL.
	Configuration	Use this screen to back up, restore ZyWALL configuration settings or reset them to the factory defaults.
	Restart	This screen allows you to reboot the ZyWALL without turning the power off.
LOGOUT		Click this link to log out of and exit the web configurator. For security reasons, you should do this after each management session.

## 2.4 Example Configuration Settings

The following table shows an example setup for your ZyWALL. In this setup, the ZyWALL is behind a NAT router (or firewall) and is given a private IP address. The gateway is also in a private network. The **LAN** and **WAN** ports are both in stealth mode and remote management is only allowed from the **MGMT** port.

**Table 3** Example Configuration Settings

FIELD	EXAMPLE CONFIGURATION		
IP Address		10. 10. 1.1 (private IP address)	
Subnet Mask		255.255.255. 0	

**Table 3** Example Configuration Settings

<b>FIELD</b>	<b>EXAMPLE CONFIGURATION</b>		
Gateway		10. 10. 1.254 (switch or router on LAN or DMZ)	
State		INLINE	
Ports Settings			
Port	Link	Status	Stealth
WAN	Auto 10M/Half	UP	ON
LAN	Auto 100M/Full	UP	ON
MGMT	Auto 100M/Full	UP	OFF
Remote Management:			
WWW Server Access		MGMT only	
SNMP Server Access		MGMT only	
SSH Server Access		MGMT only	

# CHAPTER 3

## General Settings

This chapter describes how to configure the ZyWALL's TCP, VLAN and State settings.

### 3.1 Device

Enter the ZyWALL IP address, subnet mask, gateway IP address and DNS server IP address in the next screen. The gateway and DNS entries relate to the e-mail, syslog and SNMP functions of the ZyWALL.

The DNS server maps a domain name to its corresponding IP address and vice versa. If you configure a DNS server, you can enter an IP address or domain name for e-mail, syslog, etc. servers.

If you change the ZyWALL IP address, you will need to access it again using the new IP address. To change your ZyWALL's network settings click **GENERAL**, then the **Device** tab.

**Figure 10** General: Device

The screenshot shows the 'GENERAL' configuration page with the 'Device' tab selected. The 'General Setup' section contains a text field for 'System Name' with the value 'IDP10' and a numeric field for 'Administrator Inactivity Timer' set to '30' with a note '(minutes, 0 means no timeout)'. The 'Device Setup' section contains four rows of IP address fields: 'IP Address' (192.168.1.3), 'Subnet Mask' (255.255.255.0), 'Gateway' (0.0.0.0), and 'DNS Server' (0.0.0.0). At the bottom of the form are 'Apply' and 'Reset' buttons.

The following table describes the fields in this screen.

**Table 4 General: Device**

<b>LABEL</b>	<b>DESCRIPTION</b>
System Name	Enter a descriptive name of up to 128 single-Byte or double-Byte characters for identification purposes.
Administrator Inactivity Timer	Type how many minutes a management session (either via the web configurator or SSH) can be left idle before the session times out. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Device Setup	
IP Address	Type the IP address of your ZyWALL. If you change the ZyWALL IP address, you will need to access it again using the new IP address.
Subnet Mask	Type the IP subnet mask of your ZyWALL.
Gateway	Type the IP address of the gateway. The gateway and DNS entries relate to the e-mail, syslog and SNMP functions of the ZyWALL.
DNS Server	The DNS server maps a domain name to its corresponding IP address and vice versa. If you configure a DNS server, you can enter an IP address or domain name for e-mail, syslog, etc. servers.
Apply	Click this button to save your changes back to the ZyWALL.
Reset	Click this button to begin configuring this screen afresh.

## 3.2 Introduction to VLANs

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

VLAN increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain.

### 3.2.1 Tagged VLANs (IEEE 802.1Q)

This section gives some technical background information on tagged VLANs. Skip to *section Configuring VLAN on the ZyWALL* to see how to configure VLAN tagging on the ZyWALL. When a device receives a frame from a workstation, the VLAN from whence it came must be known so the device may respond, if necessary, to the source of the frame. This is accomplished by tagging.

IEEE 802.1Q tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across devices - tagged VLANs are not confined to the device on which they were created.

The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier, residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information, a tagged header starts after the source address field of the Ethernet frame).

- TPID: 2 Bytes
- User Priority: 3 Bits
- CFI: 1 Bit
- VLAN ID: 12 bits

TPID has a defined value of 8100 (hex). The first three bits of the TCI define user priority (giving eight priority levels). The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are from 1 to 4,094.

### 3.3 Configuring VLAN on the ZyWALL

The ZyWALL is capable of receiving tagged or untagged frames. The ZyWALL does not alter the VLAN ID of a frame if it is already tagged; however, when an untagged frame enters the ZyWALL, it can.

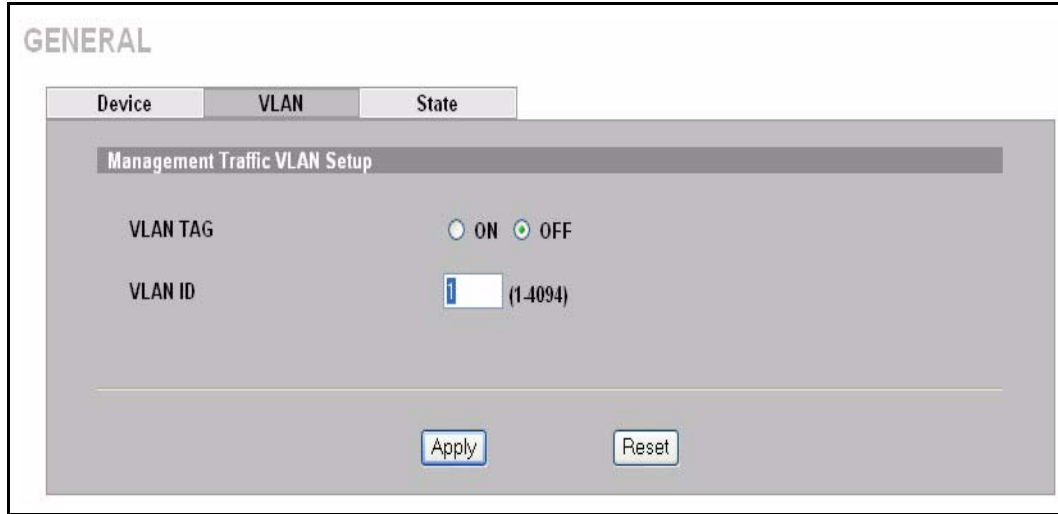
If VLAN tagging is enabled, then the frame is transmitted as a tagged frame with the VLAN ID you assign here; otherwise, it is transmitted as an untagged frame.

VLAN on the ZyWALL is for management functions of the ZyWALL. If your management computer, mail or syslog server (from whatever port) are in a VLAN group then enter that group VLAN ID in order for the ZyWALL to be able to communicate with them. There can only be one VLAN group. You cannot have the management computer, mail or syslog server in a different VLAN groups.

To change your ZyWALL's VLAN settings, click **GENERAL**, then the **VLAN** tab.



**Figure 11** General: VLAN



The following table describes the fields in this screen.

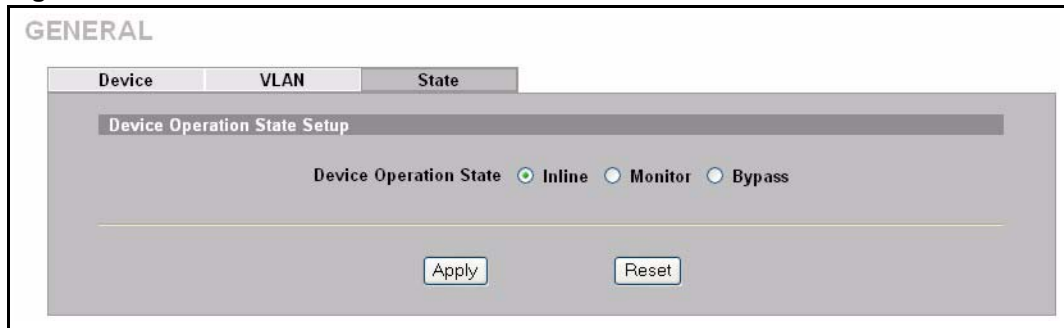
**Table 5** General: VLAN

LABEL	DESCRIPTION
Management Traffic VLAN Setup	
VLAN Tag	Select <b>ON</b> to have the ZyWALL tag outgoing frames with the VLAN ID specified in the next field.
VLAN ID	If you enabled VLAN tagging, enter the tag for outgoing frames here; the valid range is between 1 and 4094.
Apply	Click this button to save your changes back to the ZyWALL.
Reset	Click this button to begin configuring this screen afresh.

### 3.3.1 State

To change your ZyWALL's **State** settings, click **GENERAL**, then the **State** tab.

**Figure 12** General: State



The following table describes the fields in this screen.

**Table 6** General: State

LABEL	DESCRIPTION
Device Operation State Setup	
Device Operation State:	<p><b>Inline:</b> The ZyWALL will both identify suspicious or malicious packets and perform the action dictated by the rule for that type of intrusion (block, log, drop, send an alarm).</p> <p><b>Monitor:</b> <b>Monitor</b> means the ZyWALL will function as a traditional IDS (Intrusion Detection System) by identifying suspicious or malicious packets and then sending alerts (only). <b>Monitor</b> state may be advisable when you first deploy the ZyWALL in your network so valid traffic is not blocked ("false positives") nor invalid traffic wrongly allowed ("false negatives"). When "false positives" and "false negatives" have been identified and corrected, you should then change to <b>Inline</b>.</p> <p><b>Bypass:</b> All LAN and WAN traffic is allowed to pass through the ZyWALL without inspection.</p>
Apply	Click this button to save your changes back to the ZyWALL.
Reset	Click this button to begin configuring this screen afresh.



# CHAPTER 4

## Interface Screens

This chapter shows you how to configure the ZyWALL ports.

### 4.1 10/100M Auto-Sensing Ethernet Ports

The ZyWALL supports 10/100Mbps auto-negotiating Ethernet. There are two factors related to the connection of two Ethernet ports: speed and duplex mode. In a 10/100Mbps fast Ethernet, the speed can be 10Mbps or 100Mbps and the duplex mode can be half duplex or full duplex. The auto-negotiation capability makes one Ethernet port able to negotiate with a peer automatically to obtain the optimal connection speed and duplex mode.

When auto-negotiation is turned on, the Ethernet port of the ZyWALL negotiates with the peer Ethernet port on the Ethernet cable automatically to determine the optimal connection speed and duplex mode. If the peer Ethernet port does not support auto-negotiation or turns off this feature, the ZyWALL determines the connection speed by detecting the signal on the cable and using half duplex mode. When the ZyWALL's auto-negotiation is turned off, the Ethernet port uses the pre-configured speed and duplex mode settings when making a connection, thus requiring you to check the settings of the peer Ethernet port in order to connect.

### 4.2 Configuring Link

To change your ZyWALL's link settings, click **INTERFACE**, then the **Link** tab.

**Figure 13** Interface: Link

The screenshot shows the 'Interface Link Setup' configuration page. It features three tabs: 'Link', 'Stealth', and 'Policy Check'. The 'Link' tab is selected. The page title is 'Interface Link Setup'. There are three sections for configuration: 'WAN:', 'LAN:', and 'Management:'. Each section has radio buttons for speed (10, 100) and duplex mode (Full, Half, Auto). At the bottom, there are 'Apply' and 'Reset' buttons.

The following table describes the fields in this screen.

**Table 7** Interface: Link

LABEL	DESCRIPTION
WAN	Select the speed ( <b>10</b> or <b>100</b> Mbps) and duplex mode ( <b>Full</b> , <b>Half</b> , <b>Auto</b> ) for this port.
LAN	Select the speed ( <b>10</b> or <b>100</b> Mbps) and duplex mode ( <b>Full</b> , <b>Half</b> , <b>Auto</b> ) for this port.
Management	Select the speed ( <b>10</b> or <b>100</b> Mbps) and duplex mode ( <b>Full</b> , <b>Half</b> , <b>Auto</b> ) for this port.
Apply	Click this button to save your changes back to the ZyWALL.
Reset	Click this button to begin configuring this screen afresh.

## 4.3 Stealth

Stealth enabled on a port means that the ZyWALL drops all incoming packets destined for the ZyWALL received on that port with no response to the sender. The ZyWALL doesn't respond to ICMP requests such as Ping, that is, it doesn't send ICMP\_ECHO\_REPLY packets. It doesn't send TCP\_RST packets if a TCP connection is blocked nor does it send ICMP\_PORT\_UNREACHABLE packets for UDP requests or forwarded traffic.

Replies to outgoing traffic from the ZyWALL are also not allowed.

You will have to disable stealth on the LAN port or WAN port (via the MGMT port or console port) before being allowed to manage the ZyWALL from that port. The MGMT port has no stealth function.

To change your ZyWALL's stealth settings, click **INTERFACE**, then the **Stealth** tab.

**Figure 14** Interface: Stealth

The screenshot shows a web-based configuration interface for a ZyWALL. At the top, there are three tabs: 'Link', 'Stealth', and 'Policy Check'. The 'Stealth' tab is selected. Below the tabs is a section titled 'Interface Stealth Setup'. This section contains two rows of radio button controls. The first row is for 'WAN Port' with 'ON' and 'OFF' options. The second row is for 'LAN Port' with 'ON' and 'OFF' options. At the bottom of the configuration area, there are two buttons: 'Apply' and 'Reset'.

The following table describes the fields in this screen.

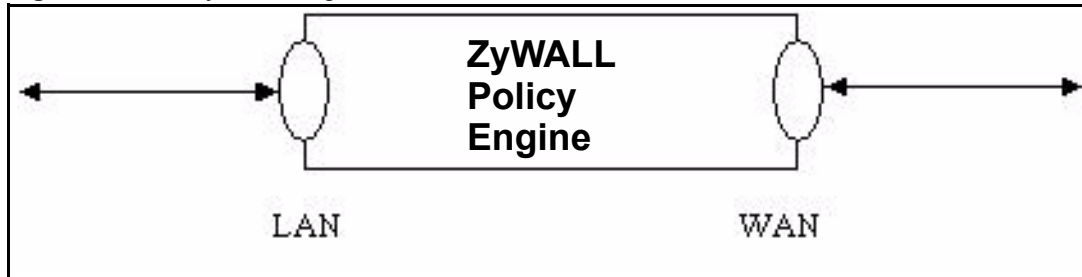
**Table 8** Interface: Stealth

LABEL	DESCRIPTION
Interface Stealth Setup	
WAN Port	Select <b>ON</b> to enable stealth on the WAN port.
LAN Port	Select <b>ON</b> to enable stealth on the LAN port.
Apply	Click this button to save your changes back to the ZyWALL.
Reset	Click this button to begin configuring this screen afresh.

## 4.4 Policy Check

Policy check determines the interface on which traffic will be checked against the ZyWALL policy rules (both pre-defined and user-defined). By selecting LAN only, then only traffic coming into the LAN and out through the WAN will be checked. Similarly, by selecting WAN only, then only traffic coming into the WAN and out through the LAN will be checked.

The interface you choose depends on the deployment of your ZyWALL. ([Section 1.3 on page 20](#)) For example for ZyWALL A1 in *installation example 4*, you might apply policy checking on the LAN only. By selecting one interface instead of both (the default) ZyWALL throughput will increase.

**Figure 15** Policy Checking

#### 4.4.1 Policy Direction

Do not confuse policy check with a policy rule direction (see the IDP pre-defined and user-defined policy screens) that refers to the intent of the policy rules (both pre-defined and user-defined).

**Incoming** means the policy applies to traffic coming from the WAN to the LAN.

**Outgoing** means the policy applies to traffic coming from the LAN to the WAN.

**Bi-directional** means the policy applies to traffic coming from the LAN or WAN.

Some rules such as blocking MSN Login would only apply to outgoing traffic as the intent is to block outgoing attempts to log into MSN Messenger. Similarly other rules would only apply to incoming traffic where the intent is to take an action on traffic initiated from somewhere on the WAN side.

Pre-defined policies have the direction pre-determined.

To configure **Policy Check**, click **INTERFACE**, then the **Policy Check** tab.

**Figure 16** Interface: Policy Check

The screenshot shows the 'Policy Check' configuration screen. It features a header with three tabs: 'Link', 'Stealth', and 'Policy Check'. The 'Policy Check' tab is selected. Below the tabs is a section titled 'Policy Check Setup'. This section contains two rows of radio button controls. The first row is labeled 'WAN Port:' and has two radio buttons: 'ON' (which is selected) and 'OFF'. The second row is labeled 'LAN Port:' and also has two radio buttons: 'ON' (selected) and 'OFF'. At the bottom of the screen, there are two buttons: 'Apply' and 'Reset'.

The following table describes the fields in this screen.

**Table 9** Interface: Policy Check

LABEL	DESCRIPTION
Policy Check Setup	
WAN Port	Select <b>ON</b> to have the ZyWALL check traffic coming into the WAN and out through the LAN against the ZyWALL policy rules (both pre-defined and user-defined).
LAN Port	Select <b>ON</b> to have the ZyWALL check traffic coming into the LAN and out through the WAN against the ZyWALL policy rules (both pre-defined and user-defined).
Apply	Click this button to save your changes back to the ZyWALL.
Reset	Click this button to begin configuring this screen afresh.





# CHAPTER 5

## Remote Management

The remote management screens allow you to which ports are allowed web and SSH access and configure SNMP

### 5.1 Remote Management Overview

Remote management allows you to determine which services can access which ZyWALL interface (if any) from which computers.

You may access your ZyWALL using web or SSH via:

- LAN + MGMT
- WAN + MGMT
- MGMT
- ALL
- Disable

To disable remote management, select **Disable** in the **Server Access** field of the corresponding screen (**WWW** or **SSH**).

Remote management over LAN or WAN will not work when there is already another remote management session of the same type (web or SSH) running. You may only have one remote management session of the same type running at one time.

The Remote Management - WWW screen allows you to manage the ZyWALL using the web configurator. The default (at the time of writing) is **MGMT** only. If you want to begin managing the ZyWALL from another port, you will first have to start a local console port session to change this default using the commands.

#### 5.1.1 HTTPS

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

It relies upon certificates, public keys, and private keys. HTTPS on the ZyWALL is used so that you may securely access the ZyWALL using the web configurator.

HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the ZyWALL.  
 HTTP connection requests from a web browser go to port 80 (by default) on the ZyWALL.

### 5.1.2 Remote Management and Stealth

If you enable **Stealth** on a port, you cannot perform remote management via that port.

## 5.2 Configuring WWW

Click **Remote Management** to open the following screen (**WWW** is the first tab) to choose a port(s) through which you can manage the ZyWALL using the web configurator.

**Figure 17** Remote Management: WWW

The screenshot shows the 'REMOTE MANAGEMENT' configuration page. At the top, there are three tabs: 'WWW', 'SNMP', and 'SSH'. The 'WWW' tab is selected. Below the tabs, there are two main sections: 'HTTPS' and 'HTTP'.  
 In the 'HTTPS' section:  
 - 'Server Port' is a text box containing '443'.  
 - 'Server Access' is a dropdown menu with 'MGMT' selected.  
 - 'Secure Client IP Address' has radio buttons for 'All' (selected) and 'Selected', followed by four IP address input boxes, each containing '0'.  
 In the 'HTTP' section:  
 - 'Server Port' is a text box containing '80'.  
 - 'Server Access' is a dropdown menu with 'ALL' selected.  
 - 'Secure Client IP Address' has radio buttons for 'All' (selected) and 'Selected', followed by four IP address input boxes, each containing '0'.  
 At the bottom of the form are two buttons: 'Apply' and 'Reset'.

The following table describes the fields in this screen.

**Table 10** Remote Management: WWW

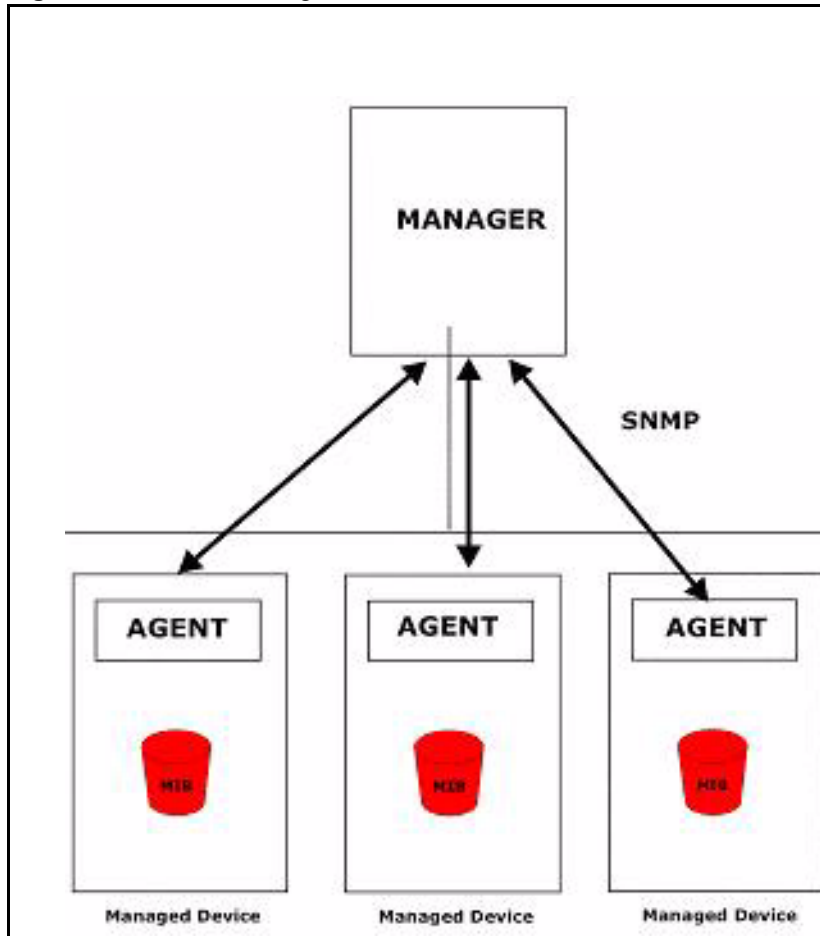
LABEL	DESCRIPTION
HTTPS	
Server Certificate	Select the Server Certificate that the ZyWALL will use to identify itself. The ZyWALL is the SSL server and must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the ZyWALL). Select a ZyWALL interface from Server Access on which incoming HTTPS access is allowed.
Server Port	The HTTPS proxy server listens on port 443 by default. If you change the HTTPS proxy server port to a different number on the ZyWALL, for example 8443, then you must notify people who need to access the ZyWALL web configurator to use "https://ZyWALL IP Address:8443" as the URL.

**Table 10** Remote Management: WWW (continued)

LABEL	DESCRIPTION
Server Access	You can allow only secure web configurator access by setting the HTTP <b>Server Access</b> field to <b>Disable</b> and setting the HTTPS <b>Server Access</b> field to an interface(s). Options are <b>LAN + MGMT</b> , <b>WAN + MGMT</b> , <b>MGMT</b> , <b>ALL</b> and <b>Disable</b> .
Secure Client IP Address	A secure client is a "trusted" computer that is allowed to communicate with the ZyWALL using this service. Select <b>All</b> to allow any computer to access the ZyWALL using this service. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the ZyWALL using this service.
HTTP	
Server Access	Select the interface(s) through which a computer may access the ZyWALL using this service. Define the rule for server access by selecting from the drop-down menu. Options are <b>LAN + MGMT</b> , <b>WAN + MGMT</b> , <b>MGMT</b> , <b>ALL</b> and <b>Disable</b> . Select <b>Disable</b> to prevent remote management of a service.
Secure Client IP Address	A secure client is a "trusted" computer that is allowed to communicate with the ZyWALL using this service. Select <b>All</b> to allow any computer to access the ZyWALL using this service. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the ZyWALL using this service.
Apply	Click this button to save your changes back to the ZyWALL.
Reset	Click this button to begin configuring this screen afresh.

## 5.3 SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your ZyWALL supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyWALL through the network. The ZyWALL supports SNMP version 2c (SNMPv2c). The next figure illustrates an SNMP management operation.

**Figure 18** SNMP Management Model

An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the ZyWALL). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.

- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

### 5.3.1 Supported MIBs

The ZyWALL supports MIB II that is defined in RFC-1213 and RFC-1215. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.

### 5.3.2 SNMP Traps

The ZyWALL will send traps to the SNMP manager when any one of the following events occurs<sup>1</sup>

**Table 11** SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
0	coldStart (defined in <i>RFC-1215</i> )	A trap is sent after booting (power on).
1	warmStart (defined in <i>RFC-1215</i> )	A trap is sent after booting (software reboot).

### 5.3.3 SNMP Configuration

To change your ZyWALL's SNMP settings, click **REMOTE MGNT**, then the **SNMP** tab. The screen appears as shown.

**Figure 19** Remote Management: SNMP

The screenshot shows the 'REMOTE MANAGEMENT' interface with the 'SNMP' tab selected. The 'SNMP Configuration' section contains the following settings:

- Get Community:** public
- Set Community:** private
- Trap Community:** SNMP\_trap
- Destination:** 0 . 0 . 0 . 0
- Server Access:** Disable (dropdown menu)
- Secure Client IP Address:**  All  Selected 0 . 0 . 0 . 0

Buttons for 'Apply' and 'Reset' are located at the bottom of the configuration area.

1. These are the traps supported at the time of writing.

The following table describes the fields in this screen.

**Table 12** Remote Management: SNMP

LABEL	DESCRIPTION
SNMP Configuration	
Get Community	This is the “password” for the incoming Get and GetNext requests from the management station.
Set Community	This is the “password” for incoming Set requests from the management station.
Trap Community	Type the trap community, which is the password sent with each trap to the SNMP manager.
Destination	Type the IP address of the station to which SNMP traps are sent.
Server Access	Select the interface(s) through which a computer may access the ZyWALL using this service. Define the rule for server access by selecting from the drop-down menu. Options are <b>LAN + MGMT</b> , <b>WAN + MGMT</b> , <b>MGMT</b> , <b>ALL</b> and <b>Disable</b> .
Secure Client IP Address	A secure client is a “trusted” computer that is allowed to communicate with the ZyWALL using this service. Select <b>All</b> to allow any computer to access the ZyWALL using this service. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the ZyWALL using this service.
Apply	Click this button to save your changes back to the ZyWALL.
Reset	Click this button to begin configuring this screen afresh.

## 5.4 SSH Overview

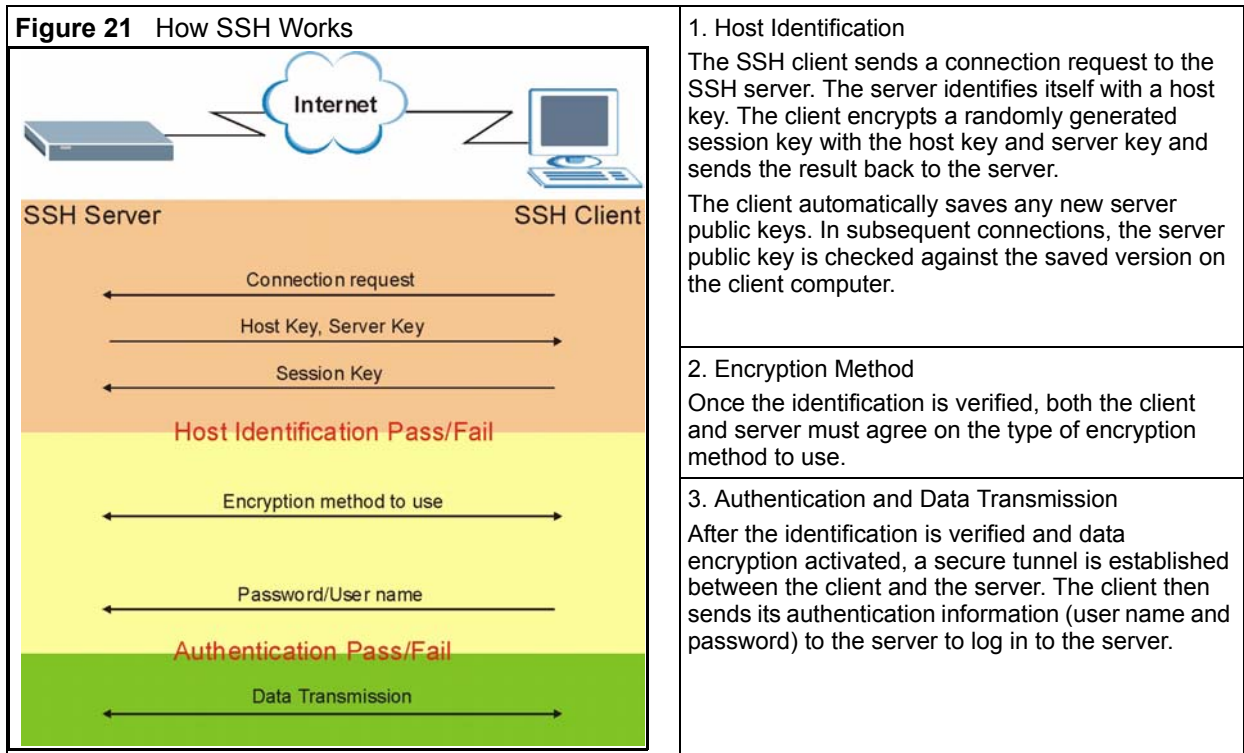
Unlike Telnet or FTP, which transmit data in clear text, SSH (Secure Shell) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

**Figure 20** SSH Communication Example



### 5.4.1 How SSH works

The following table summarizes how a secure connection is established between two remote hosts.



## 5.4.2 SSH Implementation on the ZyWALL

Your ZyWALL supports SSH version 1.5 using RSA authentication and three encryption methods (DES, 3DES and Blowfish). The SSH server is implemented on the ZyWALL for remote management and file transfer on port 22. Only one SSH connection is allowed at a time.

## 5.4.3 Requirements for Using SSH

You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the ZyWALL over SSH.

## 5.5 SSH (Secure Shell) Configuration

To change your ZyWALL's Secure Shell settings, click **REMOTE MGNT**, then the **SSH** tab.



**Figure 22** Remote Management: SSH

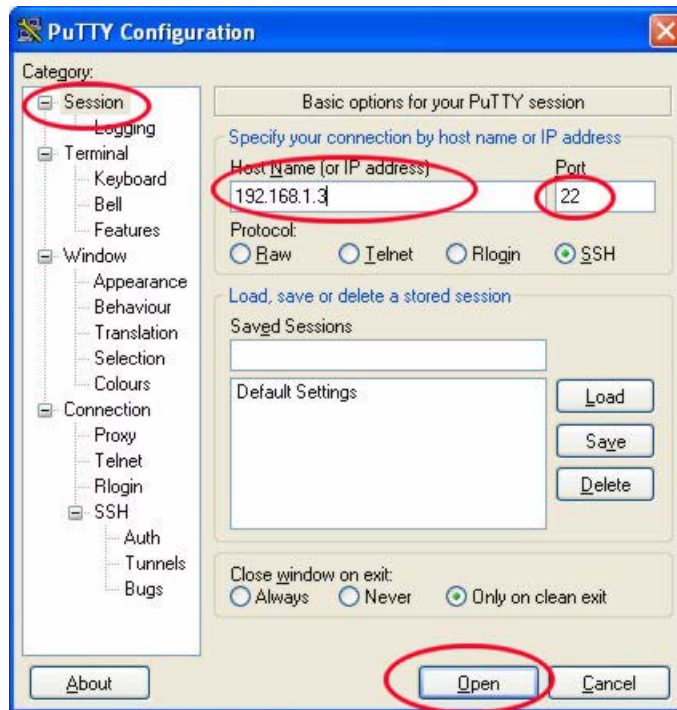
The following table describes the fields in this screen.

**Table 13** Remote Management: SSH

LABEL	DESCRIPTION
Server Access	Select the interface(s) through which a computer may access the ZyWALL using this service. The default is <b>Disable</b> . You need to select a port in order to access the ZyWALL using SSH. Options are <b>LAN + MGMT</b> , <b>WAN + MGMT</b> , <b>MGMT</b> (only), <b>ALL</b> (WAN + LAN + MGMT) and <b>Disable</b> . Select <b>Disable</b> to totally prevent SSH access to the ZyWALL.
Secure Client IP Address	A secure client is a "trusted" computer that is allowed to communicate with the ZyWALL using SSH. Select <b>Selected</b> or <b>All</b> . If you choose <b>Selected</b> you must enter an IP address in the field provided. The ZyWALL will check if the client IP address matches the value here when an SSH session is up. If it does not match, the ZyWALL will disconnect the session immediately. Select <b>All</b> if you want to allow computers with any IP address to access the ZyWALL via SSH.
Apply	Click this button to save your changes back to the ZyWALL.
Reset	Click this button to begin configuring this screen afresh.

### 5.5.1 Example Using SSH

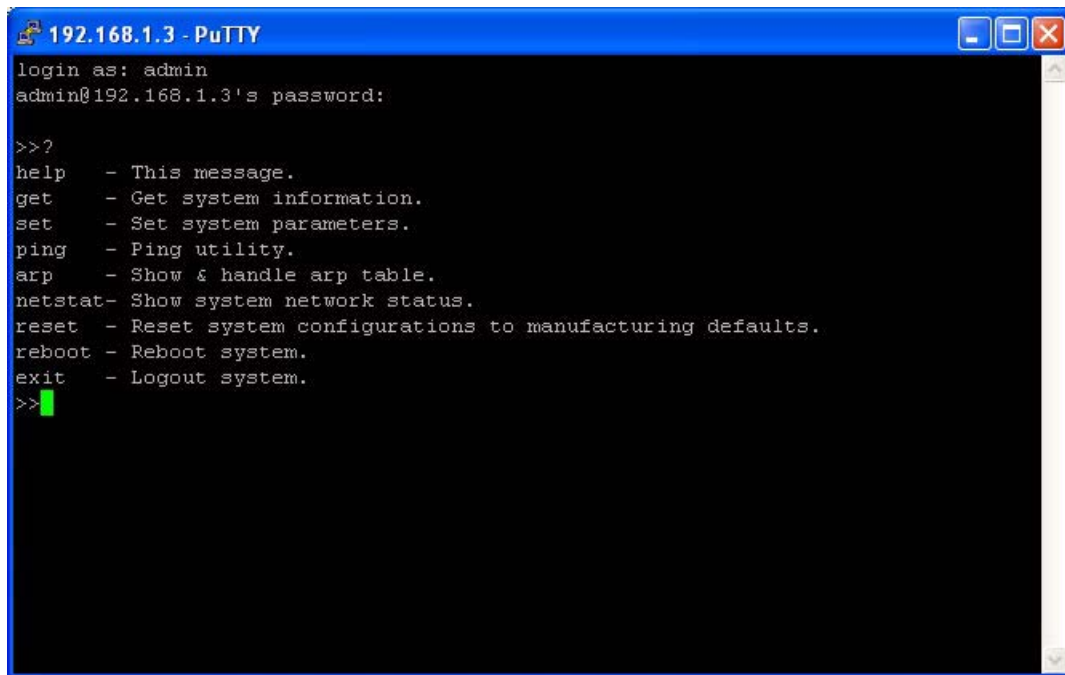
- 1 Enable SSH access on a port as shown in [Section 5.5 on page 48](#).
- 2 Run an SSH client program. PuTTY is used in this example. PuTTY is freeware that can be downloaded from the Internet.
- 3 Configure PuTTY as shown in the following screen.

**Figure 23** PuTTY Settings

4 You may see a PuTTY security alert next. Click **Yes** to continue.

**Figure 24** PuTTY Security Alert

5 You see the login screen of the ZyWALL next. Enter the username (default is "admin") and password (default is '1234') to log in.

**Figure 25** ZyWALL Command Interface Login Screen

```
192.168.1.3 - PuTTY
login as: admin
admin@192.168.1.3's password:

>>?
help  - This message.
get   - Get system information.
set   - Set system parameters.
ping  - Ping utility.
arp   - Show & handle arp table.
netstat- Show system network status.
reset - Reset system configurations to manufacturing defaults.
reboot - Reboot system.
exit  - Logout system.
>> █
```

# CHAPTER 6

## IDP Policies

This chapter describes how to configure your ZyWALL's IDP settings.

### 6.1 IDP Overview

An IDP system can detect malicious or suspicious packets and respond instantaneously. It can detect “misuse” detections based on pre-defined attack patterns and “anomaly” detections based on violations of protocol standards (RFCs – Requests for Comments) or abnormal flows such as port scans. The rules that define “misuse” or “anomaly” detections and how to respond to them are called “IDP policies”.

The ZyWALL ships with a built-in “pre-defined” policy set. This policy set can be regularly updated (see **Update**). Regular updates are vital as new attack types evolve.

For people with knowledge of packet header types and OSI (Open System Interconnection), the IDP allows you to create your own (“user-defined”) rules.

See *the appendices* for more information on IDP systems.

Rule ordering is important as rules are applied in turn. Pre-defined rules have already been ordered for you and cannot be re-ordered.

The total number of pre-defined and user-defined rules (maximum 128 rules permitted) allowed on the ZyWALL is 3,000.

### 6.2 mySecurity Zone

mySecurity Zone is a web portal that provides all "security" related information for ZyXEL security products.

You can find the policy description here that gives a detailed description about the intrusion for which the policy was written. Copy the policy ID from the **Policy ID** column in the **Pre-defined** screen or **View Log** screen and paste it in a mySecurity zone search field to find detailed information about the specific intrusion.

You can also find an advisory that tells you how to respond to new attacks.

If you have already registered your ZyWALL on myZyXEL.com, then you can use your myzyXEL.com username and password to log into mySecurity Zone without having to register again.

For more information on mySecurity zone, please visit <http://www.mysecurity.zyxel.com>.

## 6.3 Signature Categories

This section defines some IDP terms used in the ZyWALL. See *the appendices* for more detailed information on IDP term definitions. The following are both the pre-defined (not editable) and user-defined signature categories (you may refer to these policy categories when categorizing your own user-defined rules).

### 6.3.1 P2P

Peer-to-peer (P2P) is where computing devices link directly to each other and can directly initiate communication with each other; they do not need an intermediary. A device can be both the client and the server. In the ZyWALL, P2P refers to peer-to-peer applications such as e-Mule, e-Donkey, BitTorrent, iMesh etc. To find a list of all peer-to-peer signatures supported by the ZyWALL, do a policy search by name (P2P) or policy query by type (**P2P**). The following screen shows some P2P signatures supported by the ZyWALL at the time of writing.

**Figure 26** P2P Signatures

#	<input type="checkbox"/> Enable	<input type="checkbox"/> Alarm	Type	Name	Direction	Action	Policy ID
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	P2P	VNN Client Login	Outgoing	Log	1051701
2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	P2P	P2P ezPeer client login	Bidirectional	Log	1050408
3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	P2P	P2P Kuro client login	Bidirectional	Log	1050409
4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	P2P	P2P eMule0.30e Login	Outgoing	Log	1051685
5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	P2P	P2P eDonkey UDP Server status request	Bidirectional	Log	1051141
6	<input checked="" type="checkbox"/>	<input type="checkbox"/>	P2P	P2P Overnet UDP connect	Bidirectional	Log	1051145
7	<input checked="" type="checkbox"/>	<input type="checkbox"/>	P2P	P2P eDonkey GET server list	Bidirectional	Log	1051159
8	<input checked="" type="checkbox"/>	<input type="checkbox"/>	P2P	P2P eDonkey Server status requests and reports 4665/UDP	Bidirectional	Log	1051151
9	<input checked="" type="checkbox"/>	<input type="checkbox"/>	P2P	P2P eDonkey detection 4242/TCP	Bidirectional	Log	1050410
10	<input checked="" type="checkbox"/>	<input type="checkbox"/>	P2P	P2P eDonkey detection 4661-4665/TCP	Bidirectional	Log	1050411
11	<input checked="" type="checkbox"/>	<input type="checkbox"/>	P2P	P2P eDonkey connection	Outgoing	Log	1050423
12	<input checked="" type="checkbox"/>	<input type="checkbox"/>	P2P	P2P eMule detection	Bidirectional	Log	1050412
13	<input checked="" type="checkbox"/>	<input type="checkbox"/>	P2P	P2P ML donkey www	Bidirectional	Log	1050413

### 6.3.2 IM

IM (Instant Messaging) refers to chat applications. Chat is real-time, text-based communication between two or more users via networks-connected computers. After you enter a chat (or chat room), any room member can type a message that will appear on the monitors of all the other participants. To find a list of all IM signatures supported by the ZyWALL, do a policy search by name (IM or chat) or policy query by type (IM). The following screen shows some IM signatures supported by the ZyWALL at the time of writing.

Figure 27 IM (Chat) Signatures

#	Enable	Alarm	Type	Name	Direction	Action	Policy ID
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Instant Messenger	CHAT MSN 6.x->4.x file transfer request	Bidirectional	Log	1050935
2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Instant Messenger	CHAT MSN file transfer request	Bidirectional	Log	1050364
3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Instant Messenger	CHAT MSN message	Bidirectional	Log	1050363
4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Instant Messenger	CHAT MSN login attempt	Outgoing	Log	1050362
5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Instant Messenger	CHAT MSN user search	Outgoing	Log	1050367
6	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Instant Messenger	CHAT MSN 6.x login attempt <1024	Outgoing	Log	1051207
7	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Instant Messenger	CHAT MSN 7.x login attempt <1024	Outgoing	Log	1051770

### 6.3.3 SPAM

Spam is unsolicited "junk" e-mail sent to large numbers of people to promote products or services. To find a list of all spam signatures supported by the ZyWALL, do a policy search by name (spam) or policy query by type (**SPAM**). The following screen shows some spam signatures supported by the ZyWALL at the time of writing.

Figure 28 Spam Signatures

#	Enable	Alarm	Type	Name	Direction	Action	Policy ID
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	SPAM	SPAM Dynamailer	Incoming	Log + Drop Packet + Block Connection	1050345
2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	SPAM	SPAM www-mailserver.com	Incoming	Log + Drop Packet + Block Connection	1050347
3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	SPAM	SPAM mailserver.idv.tw	Incoming	Log + Drop Packet + Block Connection	1050348
4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	SPAM	SPAM The Bat!	Incoming	Log + Drop Packet + Block Connection	1050354
5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	SPAM	SPAM Drug	Incoming	Log + Drop Packet + Block Connection	1051222

### 6.3.4 DoS/DDoS

The goal of Denial of Service (DoS) attacks is not to steal information, but to disable a device or network on the Internet. A distributed denial-of-service (DDoS) attack is one in which multiple compromised systems attack a single target, thereby causing denial of service for users of the targeted system. To find a list of all Denial of Service or Distributed Denial of Service signatures supported by the ZyWALL, do a policy search by name (DoS) or policy query by type (**DoS/DDoS**). The following screen shows some of the DoS/DDoS signatures supported by the ZyWALL at the time of writing.

Figure 29 DoS/DDoS Signatures

#	Enable	Alarm	Type	Name	Direction	Action	Policy
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DDoS	TCP FLOOD	Bidirectional	Log + Drop Packet	40265311
2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DDoS	UDP FLOOD	Bidirectional	Log + Drop Packet	40265311
3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DDoS	ICMP FLOOD	Bidirectional	Log + Drop Packet	40265311
4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DDoS	IGMP FLOOD	Bidirectional	Log + Drop Packet	40265311
5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DDoS	IP FLOOD	Bidirectional	Log + Drop Packet	40265311
6	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DDoS	TCP SYN	Bidirectional	Log + Drop Packet	40265311
7	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DDoS	UDP SMURF	Bidirectional	Log + Drop Packet	40433090
8	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DDoS	ICMP SMURF	Bidirectional	Log + Drop Packet	40433090
9	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DDoS	DoS HGOD & SynKiller Flooding	Bidirectional	Log + Drop Packet	105177
10	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DDoS	DoS UDP echo+chargen bomb	Bidirectional	Log + Drop Packet	104876
11	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DDoS	ICMP Large ICMP Packet	Bidirectional	Log	104900
12	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DDoS	MISC UPNP malformed advertisement	Bidirectional	Log	104902
13	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DDoS	NETBIOS DoS RFPoison	Bidirectional	Log + Drop Packet	104903
14	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DDoS	SMTP exchange mime DoS	Bidirectional	Log + Drop Packet	104920
15	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DDoS	TELNET livingston DoS	Bidirectional	Log	104925
16	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DDoS	MS Terminal server request (RDP)	Bidirectional	Log	104990
17	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DDoS	BACKDOOR trinity connection attempt	Incoming	Log	104995
18	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DDoS	BACKDOOR win-trin00 connection attempt	Incoming	Log + Drop Packet	104995
19	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DDoS	ATTACK-RESPONSES successful gobbles ssh exploit uname	Outgoing	Log + Drop Packet	105005

### 6.3.5 Scan

Scan refers to all port, IP or vulnerability scans. Hackers scan ports to find targets. They may use a TCP connect() call, SYN scanning (half-open scanning), Nmap etc. After a target has been found, a layer-7 scanner can be used to exploit vulnerabilities. To find a list of all scan-related signatures supported by the ZyWALL, do a policy search by name (scan) or policy query by type (**Scan**). The following screen shows some of the scan-related signatures supported by the ZyWALL at the time of writing.



**Figure 30** Scan Signatures

#	Enable	Alarm	Type	Name	Direction	Action	Policy ID
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Scan	TCP PORT SCAN	Bidirectional	Log + Drop Packet	4026531848
2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Scan	UDP PORT SCAN	Bidirectional	Log + Drop Packet	4026531849
3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Scan	IP SWEEP	Bidirectional	Log + Drop Packet	4026531850
4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Scan	TCP PORT SYN SCAN	Bidirectional	Log + Drop Packet	4026531851
5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Scan	TCP PORT FIN SCAN	Bidirectional	Log + Drop Packet	4026531852
6	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Scan	TCP PORT NULL SCAN	Bidirectional	Log + Drop Packet	4026531853
7	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Scan	TCP PORT XMAS SCAN	Bidirectional	Log + Drop Packet	4026531854
8	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Scan	CLASS C TCP BROADCAST	Bidirectional	Log	4043309057
9	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Scan	SCAN Worm.Blaster.D Ping	Bidirectional	Log + Drop Packet	1050695
10	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Scan	SCAN eEye RPC DCOM Scanner	Incoming	Log + Drop Packet + Block Connection	1050421
11	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Scan	SCAN MS RPC DCOM Scanner	Incoming	Log + Drop Packet + Block Connection	1050420
12	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Scan	MISC SNMP NT UserList	Bidirectional	Log	1049024
13	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Scan	FINGER search query	Bidirectional	Log + Drop Packet	1048841
14	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Scan	FINGER root query	Bidirectional	Log + Drop Packet	1048842
15	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Scan	FTP adm scan	Bidirectional	Log + Drop Packet	1048870
16	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Scan	FTP iss scan	Bidirectional	Log + Drop Packet	1048871

### 6.3.6 Buffer Overflow

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. The excess information can overflow into adjacent buffers, corrupting or overwriting the valid data held in them.

Intruders could run codes in the overflow buffer region to obtain control of the system, install a backdoor or use the victim to launch attacks on other devices.

To find a list of all buffer overflow related signatures supported by the ZyWALL, do a policy search by name or policy query by type (**Buffer Overflow**). The following screen shows some of the buffer overflow related signatures supported by the ZyWALL at the time of writing.

**Figure 31** Buffer Overflow Signatures

#	Enable	Alarm	Type	Name	Direction	Action	Policy ID
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Buffer Overflow	Exploit Firebird Database Remote Database Name Overflow	Incoming	Log + Drop Packet + Block Connection	105123
2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Buffer Overflow	EXPLOIT CVS server heap overflow attempt (target Linux)	Incoming	Log + Drop Packet + Block Connection	105124
3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Buffer Overflow	EXPLOIT CVS server heap overflow attempt (target BSD)	Incoming	Log + Drop Packet + Block Connection	105125
4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Buffer Overflow	EXPLOIT CVS server heap overflow attempt (target Solaris)	Incoming	Log + Drop Packet + Block Connection	105126
5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Buffer Overflow	EXPLOIT Windows Lsasrv.dll RPC Overflow (Sasser)	Bidirectional	Log + Drop Packet + Block Connection	105119
6	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Buffer Overflow	EXPLOIT Windows Lsasrv.dll RPC Overflow (Sasser)-1	Bidirectional	Log + Drop Packet + Block Connection	105127
7	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Buffer Overflow	EXPLOIT Windows Lsasrv.dll RPC Overflow Unicode (Sasser)	Bidirectional	Log + Drop Packet + Block Connection	105119
8	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Buffer Overflow	EXPLOIT Windows Lsasrv.dll RPC Overflow Unicode (Sasser)-1	Bidirectional	Log + Drop Packet + Block Connection	105128

### 6.3.7 Virus/Worm

A computer virus is a small program designed to corrupt and/or alter the operation of other legitimate programs. A worm is a program that is designed to copy itself from one computer to another on a network. A worm's uncontrolled replication consumes system resources thus slowing or stopping other tasks.

To find a list of all virus/worm related signatures supported by the ZyWALL, do a policy search by name or policy query by type (**Virus/Worm**). The following screen shows some of the virus/worm related signatures supported by the ZyWALL at the time of writing.

**Figure 32** Worm/Virus Signatures

#	Enable	Alarm	Type	Name	Direction	Action	Policy ID
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Virus/Worm	Virus - W32/Swen	Bidirectional	Log + Drop Packet + Block Connection	1050426
2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Virus/Worm	Virus - W32/Gibe.B	Bidirectional	Log + Drop Packet + Block Connection	1050427
3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Virus/Worm	Worm - W32/Blaster	Bidirectional	Log + Drop Packet + Block Connection	1050406
4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Virus/Worm	Worm - W32/MSBLAST over TFTP	Bidirectional	Log + Drop Packet	1050405
5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Virus/Worm	Virus - W32/Fizzer Worm	Bidirectional	Log + Drop Packet + Block Connection	1050331
6	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Virus/Worm	Virus - W32/Fizzer Worm.s1	Bidirectional	Log + Drop Packet + Block Connection	1050332
7	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Virus/Worm	Virus - W32/Fizzer Worm.s2	Bidirectional	Log + Drop Packet + Block Connection	1050333
8	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Virus/Worm	Virus - W32/Fizzer Worm.s3	Bidirectional	Log + Drop Packet + Block Connection	1050334
9	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Virus/Worm	NETBIOS nimda .eml	Bidirectional	Log + Drop Packet	1049030
10	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Virus/Worm	NETBIOS nimda .nws	Bidirectional	Log + Drop Packet	1049031
11	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Virus/Worm	NETBIOS nimda RICHEL20.DLL	Bidirectional	Log	1049991
12	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Virus/Worm	Virus - W32/BugBear.B	Bidirectional	Log + Drop Packet + Block Connection	1050353
13	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Virus/Worm	Worm.BugBear.C - 1	Bidirectional	Log + Drop Packet + Block Connection	1051137
14	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Virus/Worm	Worm.BugBear.C - 2	Bidirectional	Log + Drop Packet + Block Connection	1051138
15	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Virus/Worm	Worm.BugBear.C - 3	Bidirectional	Log + Drop Packet + Block Connection	1051139
16	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Virus/Worm	Worm.Sexer.B/C/E - 1	Bidirectional	Log + Drop Packet + Block Connection	1050496
17	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Virus/Worm	Worm.Sexer.B/C/E - 2	Bidirectional	Log + Drop Packet + Block Connection	1050497

### 6.3.8 Backdoor/Trojan

A backdoor (also called a trapdoor) is hidden software or a hardware mechanism that can be triggered to gain access to a program, online service or an entire computer system. A Trojan horse is a harmful program that is hidden inside apparently harmless programs or data.

To find a list of all backdoor/Trojan related signatures supported by the ZyWALL, do a policy search by name or policy query by type (**Backdoor/Trojan**). The following screen shows some of the backdoor/Trojan related signatures supported by the ZyWALL at the time of writing.

**Figure 33** Backdoor/Trojan Signatures

#	<input type="checkbox"/> Enable	<input type="checkbox"/> Alarm	Type	Name	Direction	Action	Policy ID
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trojan Horse	TROJAN LSASS.EXE 53/TCP	Bidirectional	Log + Drop Packet + Block Connection	1051226
2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trojan Horse	BACKDOOR Malice over SMTP	Outgoing	Log + Drop Packet + Block Connection	1050430
3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trojan Horse	BACKDOOR Malice IRC server ping	Outgoing	Log + Drop Packet + Block Connection	1050429
4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trojan Horse	BACKDOOR Malice IRC server message	Outgoing	Log + Drop Packet + Block Connection	1050428
5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trojan Horse	ACKcmdC trojan scan	Bidirectional	Log	1048593
6	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trojan Horse	QAZ Worm Client Login access	Bidirectional	Log	1048596
7	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trojan Horse	CDK	Bidirectional	Log	1048669
8	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trojan Horse	w00w00 attempt	Bidirectional	Log	1048693
9	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trojan Horse	MISC r00t attempt	Bidirectional	Log	1048695
10	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trojan Horse	MISC linux rootkit attempt - 1 (wh00t!)	Bidirectional	Log	1048697
11	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trojan Horse	MISC linux rootkit attempt lrrk0x	Bidirectional	Log	1048698

### 6.3.9 Access Control

Access control refers to procedures and controls that limit or detect access. Access control is used typically to control user access to network resources such as servers, directories, and files.

To find a list of all access control related signatures supported by the ZyWALL, do a policy search by name or policy query by type (**Access Control**). The following screen shows some of the access control related signatures supported by the ZyWALL at the time of writing.

**Figure 34** Access Control Signatures

#	<input type="checkbox"/> Enable	<input type="checkbox"/> Alarm	Type	Name	Direction	Action	Policy ID
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Access Control	ATTACK-RESPONSE Microsoft cmd.exe banner	Outgoing	Log + Drop Packet + Block Connection	1050435
2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Access Control	FTP .forward	Bidirectional	Log	1048852
3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Access Control	UNIX ftp rhosts write attempt	Bidirectional	Log + Drop Packet	1050061
4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Access Control	FTP .rhosts	Bidirectional	Log	1048853
5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Access Control	FTP CWD ~root	Incoming	Log	1048854
6	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Access Control	FTP site exec	Bidirectional	Log + Drop Packet	1048879
7	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Access Control	FTP tar parameters	Bidirectional	Log	1048880
8	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Access Control	FTP ADMw0rm ftp login attempt	Bidirectional	Log + Drop Packet	1048886
9	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Access Control	ICMP SoftEther Keep-Alive PING	Bidirectional	Log + Drop Packet	1051140
10	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Access Control	TELNET Bad Login - 1	Bidirectional	Log	1049005
11	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Access Control	TELNET Bad Login - 2	Bidirectional	Log	1049006

### 6.3.10 Web Attack

Web attack signatures refer to attacks on web servers such as IIS.

To find a list of all web attack related signatures supported by the ZyWALL, do a policy search by name or policy query by type (**Web Attack**). The following screen shows some of the web attack related signatures supported by the ZyWALL at the time of writing.

Figure 35 Web Attack Signatures

#	<input type="checkbox"/> Enable	<input type="checkbox"/> Alarm	Type	Name	Direction	Action	Policy ID
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Web Attacks	EXPLOIT IIS 5 SSL remote root exploit	Incoming	Log + Drop Packet + Block Connection	1051158
2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Web Attacks	EXPLOIT IIS 5 remote .printer overflow	Incoming	Log + Drop Packet + Block Connection	1050871
3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Web Attacks	WEB-PHP PHP-NUKE version 6.9 cid sql injection attempt	Incoming	Log + Drop Packet + Block Connection	1050697
4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Web Attacks	WEB-PHP phpBB 2.06 search.php SQL injection attempt	Incoming	Log + Drop Packet + Block Connection	1050694
5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Web Attacks	WEB-CLIENT IE address bar URL spoofing attempt	Incoming	Log	1050690
6	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Web Attacks	EXPLOIT Apache 1.3.*-2.0.48 remote users disclosure	Incoming	Log + Drop Packet + Block Connection	1050582
7	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Web Attacks	EXPLOIT WebFS Long File Overflow	Incoming	Log + Drop Packet + Block Connection	1050558
8	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Web Attacks	EXPLOIT IA Web mail buffer overflow	Incoming	Log + Drop Packet + Block Connection	1050478

### 6.3.11 Porn

The ZyWALL can block web sites if their URLs contain certain pornographic words. It cannot block web pages containing those words if the associated URL does not.

To find a list of all porn related signatures supported by the ZyWALL, do a policy search by name or policy query by type (**Porn**). The following screen shows some of the porn related signatures supported by the ZyWALL at the time of writing.

**Figure 36** Porn Signatures

#	<input type="checkbox"/> Enable	<input type="checkbox"/> Alarm	Type	Name	Direction	Action	Policy ID
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Porn	PORN free XXX	Incoming	Log	1050375
2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Porn	PORN hardcore anal	Incoming	Log	1050376
3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Porn	PORN nude cheerleader	Incoming	Log	1050377
4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Porn	PORN up skirt	Incoming	Log	1050378
5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Porn	PORN young teen	Incoming	Log	1050379
6	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Porn	PORN hot young sex	Incoming	Log	1050380
7	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Porn	PORN fuck fuck fuck	Incoming	Log	1050381
8	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Porn	PORN anal sex	Incoming	Log	1050382
9	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Porn	PORN hardcore rape	Incoming	Log	1050383
10	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Porn	PORN real snuff	Incoming	Log	1050384
11	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Porn	PORN fuck movies	Incoming	Log	1050385
12	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Porn	PORN dildo	Incoming	Log	1050386
13	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Porn	PORN nipple clamp	Incoming	Log	1050387
14	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Porn	PORN oral sex	Incoming	Log	1050388
15	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Porn	PORN nude celeb	Incoming	Log	1050389

### 6.3.12 Others

This category refers to signatures for attacks that do not fall into the previously mentioned categories.

To find a list of all “others” related signatures supported by the ZyWALL, do a policy search by name or policy query by type (**Others**). The following screen shows some of the “others” related signatures supported by the ZyWALL at the time of writing.

**Figure 37** Others Signatures

#	Enable	Alarm	Type	Name	Direction	Action	Policy ID
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Other	TCP LAND	Bidirectional	Log + Drop Packet	4043309056
2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Other	UDP LAND	Bidirectional	Log + Drop Packet	4043309058
3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Other	IP OVERSIZE	Bidirectional	Log + Drop Packet	4043309059
4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Other	IP FRAGMENT TEARDROP	Bidirectional	Log + Drop Packet	4043309060
5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Other	IP FRAGMENT OVERSIZE	Bidirectional	Log + Drop Packet	4043309061
6	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Other	IP FRAGMENT ATTACK	Bidirectional	Log + Drop Packet	4043309062
7	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Other	IP FRAGMENT BOINK	Bidirectional	Log + Drop Packet	4043309063
8	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Other	IP FRAGMENT TIMEOUT	Bidirectional	Log + Drop Packet	4043309064
9	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Other	IP TRUNCATED	Bidirectional	Log + Drop Packet	4043309065
10	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Other	IP BAD	Bidirectional	Log + Drop Packet	4043309066
11	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Other	IP_BAD_VERSION	Bidirectional	Log + Drop Packet	4043309068
12	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Other	IP_BAD_LENGTH	Bidirectional	Log + Drop Packet	4043309069
13	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Other	IP_BAD_FLAG_UF	Bidirectional	Log + Drop Packet	4043309070
14	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Other	IP_BAD_TCP_L4_SIZE	Bidirectional	Log + Drop Packet	4043309071
15	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Other	IP_BAD_UDP_L4_SIZE	Bidirectional	Log + Drop Packet	4043309072
16	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Other	IP_BAD_ICMP_L4_SIZE	Bidirectional	Log + Drop Packet	4043309073
17	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Other	IP_BAD_IGMP_L4_SIZE	Bidirectional	Log + Drop Packet	4043309074
18	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Other	IP_BAD_IP_OPTION	Bidirectional	No Action	4043309075
19	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Other	IP_BAD_DF_MF	Bidirectional	Log	4043309076
20	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Other	BAD_TCP_STATE	Bidirectional	No Action	4043309078
21	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Other	OVER_TCP_CONN	Bidirectional	Log	4043309079
22	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Other	DROP_TCP_CONN	Bidirectional	Log + Drop Packet	4043309080
23	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Other	OVER_PING_LENGTH	Bidirectional	Log + Drop Packet	4043309081

### 6.3.13 Policy Severity

Intrusions are assigned a severity level based on the following table. The intrusion severity level then determines the default signature action.

**Table 14** Policy Severity

SEVERITY	DESCRIPTION
Severe (5)	These are intrusions that try to run arbitrary code or gain system privileges. The default action for this level of intrusion is to block the traffic.
High (4)	These are known serious vulnerabilities or intrusions that are probably not false alarms. The default action for this level of intrusion is to block the traffic.
Medium (3)	These are medium threats, access control intrusions or intrusions that could be false alarms. The default action for this level of intrusion is to log the traffic.
Low (2)	These are mild threats or intrusions that could be false alarms. The default action for this level of intrusion is to log the traffic.
Very Low (1)	These are possible intrusions caused by traffic such as Ping, trace route, ICMP queries etc. The default action for this level of intrusion is to log the traffic.



### 6.3.14 Policy Actions

The following table describes the (configurable) actions for a policy.

**Table 15** Policy Actions

ACTION	DESCRIPTION
No Action	The intrusion is detected and an alarm may be sent (if the <b>Alarm</b> check box is selected) but no other action is taken. If the <b>Alarm</b> check box is also cleared, it is recommended you simply disable the rule.
Log	The packet is marked as an intrusion and a log is recorded (an alarm may also be sent if the <b>Alarm</b> check box is selected) but the packet is allowed to pass through the ZyWALL.
Log + Drop Packet	The packet is marked as an intrusion, a log is recorded and the packet is silently discarded. (An alarm may also be sent if the <b>Alarm</b> check box is selected).
Log + Block Connection	The packet is marked as an intrusion, a log is recorded and the whole TCP connection session is blocked (including subsequent TCP packets belonging to the same connection) with both sender and receiver being sent TCP RST packets. (An alarm may also be sent if the <b>Alarm</b> check box is selected).
Log + Drop Packet + Block Connection	The packet is marked as an intrusion, a log is recorded, the triggering packet is silently discarded, and the whole TCP connection session is blocked (including subsequent TCP packets belonging to the same connection) with both sender and receiver being notified. (An alarm may also be sent if the <b>Alarm</b> check box is selected).

## 6.4 Configuring Pre-defined Policies

Click **IDP** from the navigation panel. **Pre-defined** is the first screen as shown in the following figure.

**Figure 38** Pre-defined IDP Policies Summary

**IDP Policy**

Pre-defined | Update | User-defined | Registration

**Pre-defined Policy Group Setting**

Click **Modify** to change the group setting to enable or disable the intrusion detection and prevention.

Modify

**Pre-defined Policy**

Policy Search: By Policy ID [ ] Search

Policy Query: You can hold the "Ctrl" and click the items for multiple selection and click QUERY

By Type: ALL, P2P, IM, SPAM, Dos/DDos

By Severity: ALL, Severe, High, Medium, Low

By Operating System: ALL, Windows 95/98, Windows NT, Windows 2000/XP, Linux

25 Per Page

#	Enable	Alarm	Type	Name	Direction	Action	Policy ID
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DDoS	TCP FLOOD	Bidirectional	Log + Drop Packet	4026531841
2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DDoS	UDP FLOOD	Bidirectional	Log + Drop Packet	4026531842
3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DDoS	ICMP FLOOD	Bidirectional	Log + Drop Packet	4026531844
4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DDoS	IGMP FLOOD	Bidirectional	Log + Drop Packet	4026531846
5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DDoS	IP FLOOD	Bidirectional	Log + Drop Packet	4026531847
6	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DDoS	TCP SYN	Bidirectional	Log + Drop Packet	4026531840
7	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Scan	TCP PORT SCAN	Bidirectional	Log + Drop Packet	4026531848
8	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Scan	UDP PORT SCAN	Bidirectional	Log + Drop Packet	4026531849
9	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Scan	IP SWEEP	Bidirectional	Log + Drop Packet	4026531850
10	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Scan	TCP PORT SYN SCAN	Bidirectional	Log + Drop Packet	4026531851

Apply | Reset

**Table 16** Selecting Pre-defined Policies

LABEL	DESCRIPTION
	Pre-defined Policy Group Setting
Modify	Click this button to display a screen where you can batch enable or disable policy types based on severity and/or target operating system. You can also batch enable or disable peer-to-peer, instant messaging and spam signature categories.
	Pre-defined Policy

**Table 16** Selecting Pre-defined Policies (continued)

LABEL	DESCRIPTION
Policy Search	You can search for policies based on policy name or ID number. Select <b>By Name</b> or <b>By Policy ID</b> from the drop-down list box, enter a (partial) name or a complete, exact ID number in the text box and then click <b>Search</b> . The name entered in the text box is not case sensitive. After a search is performed, click <b>IDP</b> in the navigation panel to display all policies again.
Policy Query	Alternatively, you can search for policies based on a combination of signature category (policy type), severity and/or attack target operating system. Hold the <CTRL> key to select multiple items and then click <b>Query</b> . After a search is performed, click <b>IDP</b> in the navigation panel to display all policies again.
By Type	Select one item or hold the <CTRL> key to select multiple items. See <i>section Signature Categories</i> for more information on signature categories.
AND/OR	Logical <b>AND</b> means that all criteria must be fulfilled before a match is deemed found. Logical <b>OR</b> means that at least one of the criteria must be fulfilled before a match is deemed found.
By Severity	Select one item or hold the <CTRL> key to select multiple items. See <a href="#">Table 14 on page 64</a> for more information on policy severity.
By Operating System	This search category finds policies that were intended to defend specific operating systems due to the intrusion being targeted at a weakness in that operating system. Select one item or hold the <CTRL> key to select multiple items.
<Prev Next >	Use these buttons to navigate between first, previous, next and last pages of the pre-defined policies downloaded.
#	This is the pre-defined policy index number. Pre-defined rules have already been ordered for you and cannot be re-ordered.
Enable	Clear this checkbox to have the ZyWALL skip this rule when detecting intrusions. You can enable or disable individual policies here or enable/disable a batch of policies using the screen that appears after you click <b>Modify</b> .
Alarm	An alarm is an action (an e-mail is sent) to be taken on the policy when a packet matches a rule. Alarm e-mails are not sent instantly but rather at periodic intervals (minimum five minutes). Select this checkbox to enable the alarm action. For other actions, select from the <b>Action</b> drop-down list box.
Type	This field refers to the signature category as described in <i>section Signature Categories</i> .
Name	The (read-only) policy name identifies a specific signature targeted at a specific intrusion.
Direction	A policy rule direction refers to the intent of the policy rule. <b>Incoming</b> means the policy applies to traffic coming from the WAN to the LAN. <b>Outgoing</b> means the policy applies to traffic coming from the LAN to the WAN. <b>Bidirectional</b> means the policy applies to traffic coming from and going to either direction. Some rules such as blocking MSN Login would only apply to outgoing traffic as the intent is to block outgoing attempts to log into MSN Messenger. Similarly other rules would only apply to incoming traffic where the intent is to take an action on traffic initiated from somewhere on the WAN side. Pre-defined policies have the direction pre-determined.

**Table 16** Selecting Pre-defined Policies (continued)

LABEL	DESCRIPTION
Action	<p>This field defines the action to be taken for a rule match. See <a href="#">Table 15 on page 65</a> for details on actions.</p> <p>You can change the specified default action for pre-defined rules. After you apply these changes, your specified actions for pre-defined rules remain in effect even after you update new rules or change modes (<b>Inline</b> to <b>Monitor</b> and back to <b>Inline</b> again).</p> <p>An alarm is also an action to be taken on the policy, but you must select the <b>Alarm</b> checkbox to have the ZyWALL send an alarm when a traffic flow matches a rule.</p>
Policy ID	<p>This field displays a policy ID number that gives details on the intrusion and the policy fix. Log in and subscribe to the advisories at <a href="http://mysecurity.com">mysecurity.com</a> for more information.</p>
Apply	<p>Click this button to save your changes back to the ZyWALL.</p>
Reset	<p>Click this button to begin configuring this screen afresh.</p>

### 6.4.1 Search Example

The following screen displays when you perform a search for the “Sasser” virus. It shows that three policies for the virus have been found. If the search finds more policies than one page can display, then click **Search** again to display the next page.

**Figure 39 Search Example**

The screenshot shows the ZyWALL IDP search interface. At the top, there is a 'Policy Search' section with a dropdown set to 'By Name' and a search box containing 'Sasser'. Below this is a 'Policy Query' section with instructions: 'You can hold the "Ctrl" and click the items for multiple selection and click QUERY'. It features three filters: 'By Type' (set to ALL), 'By Severity' (set to ALL), and 'By Operating System' (set to ALL). A 'Query' button is located to the right of these filters. Below the filters, there is a 'Per Page' dropdown set to '25' and a pagination control showing 'Page 1' of '5' items.

#	Enable	Alarm	Type	Name	Direction	Action	Policy ID
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Buffer Overflow	EXPLOIT Windows Lsasrv.dll RPC Overflow (Sasser)	Bidirectional	Log + Drop Packet + Block Connection	1051195
2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Buffer Overflow	EXPLOIT Windows Lsasrv.dll RPC Overflow (Sasser)-1	Bidirectional	Log + Drop Packet + Block Connection	1051255
3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Buffer Overflow	EXPLOIT Windows Lsasrv.dll RPC Overflow Unicode (Sasser)	Bidirectional	Log + Drop Packet + Block Connection	1051196
4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Buffer Overflow	EXPLOIT Windows Lsasrv.dll RPC Overflow Unicode (Sasser)-1	Bidirectional	Log + Drop Packet + Block Connection	1051256
5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Scan	SCAN Sasser IP sweep attempt	Bidirectional	Log + Drop Packet	1051198

At the bottom of the interface, there are 'Apply' and 'Reset' buttons.

### 6.4.2 Query Example

The following screen shows severe and high impact DoS/DDoS policies for intrusions that exploit vulnerabilities on Windows 2000 and Windows XP computers. Use the <CTRL> key to select multiple items. If the query finds more policies than one page can display, then click **Query** again to display the next page.

Figure 40 Query Example

By Type: ALL P2P IM SPAM **Dos/DDos** AND By Severity: ALL Severe High Medium Low AND By Operating System: ALL Windows 95/98 Windows NT **Windows 2000/XP** Linux Query

25 Per Page

|< Prev. Page 1 Next >| Items 1 to 5 (of 5)

#	Enable	Alarm	Type	Name	Direction	Action	Policy ID
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DDoS	NETBIOS DoS RFPoison	Bidirectional	Log + Drop Packet	1049033
2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DDoS	SMTP exchange mime DoS	Bidirectional	Log + Drop Packet	1049202
3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DDoS	DoS-ath0-modem-disconnect	Bidirectional	Log + Drop Packet	1050273
4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DDoS	DoS MS-SQL Slammer Worm	Bidirectional	Log + Drop Packet	1050295
5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DDoS	DoS WebDAV XML Message Handler Denial of Service (MS04-030)	Incoming	Log + Drop Packet + Block Connection	1051740

|< Prev. Page 1 Next >| Items 1 to 5 (of 5)

### 6.4.3 Modify Screen

Click **Modify** in Pre-defined IDP Policies Summary 6-13 to display a screen where you can batch enable or disable policy types based on severity and/or target operating system. You can also batch enable or disable peer-to-peer, instant messaging and spam signature categories.

As you can enable certain “attack group” items and at the same time disable certain “application group” items (and vice versa), in some instances, conflict may occur. If conflict should occur, then the action determined under “application group” takes precedence.

**Figure 41** Pre-defined Policies: Modify



**Table 17** Pre-defined IDP Policies

LABEL	DESCRIPTION
ALL	Select this checkbox and then select <b>Enable</b> or <b>Disable</b> to automatically enable or disable all policies. When <b>ALL</b> is selected, <b>Attack Group</b> and <b>Application Group</b> choices are not available. When <b>ALL</b> is cleared, you can enable or disable a group of policies by severity (see <a href="#">Table 14 on page 64</a> ), operating system or signature category (P2P, IM or SPAM – see <a href="#">Section 6.3 on page 53</a> ).
Attack Group	Select <b>Enable</b> to enable all policies that meet the following criteria.
Severity	If <b>ALL</b> is cleared (not selected), you may choose to enable or disabled policies based on their seriousness (pre-determined by the IDP policy engineering team). See also <a href="#">Table 14 on page 64</a> .
Operation	Logical <b>AND</b> means that all criteria must be fulfilled before a match is deemed found. Logical <b>OR</b> means that at least one of the criteria must be fulfilled before a match is deemed found. Choose from the logical <b>AND</b> (rules that match both severity type and selected operating systems are displayed) or logical <b>OR</b> ((rules that match either severity type or selected operating systems are displayed) operators.
Operating System	If <b>ALL</b> is not selected you may choose to display policies based on intrusions that attack specific operating systems as shown in the screen. SGI refers to Silicon Graphics Incorporated, who manufactures multi-user Unix workstations that run the IRIX operating system (SGI's version of UNIX).
Application Group	If <b>ALL</b> is cleared (not selected), you may choose to enable or disabled policies based on their signature category ( <b>P2P</b> , <b>IM</b> or <b>SPAM</b> – see <a href="#">Section 6.3 on page 53</a> ) The action determined under “application group” takes precedence over any confliction action determined under “attack group”.
Apply	Click this button to save your changes back to the ZyWALL.
Cancel	Click this button to close this screen without saving any changes.

## 6.5 Update

The ZyWALL comes with a “pre-defined” set of policies that can be regularly updated. Regular updates are vital as new intrusions evolve. Use the **Update** screen to immediately download or schedule (pre-defined) new policy downloads. You should have already registered the ZyWALL (see the **Registration** screen).

Click **IDP** from the navigation panel and then click the **Update** tab.

**Figure 42** Update Policies

**Table 18** Update Policies

LABEL	DESCRIPTION
Update Server	Enter the IP address or URL of the IDP policy server (from which you download the updated IDP policies).The default server at the time of writing is updateidp.zyxel.com. It is also possible to use updateidp.zyxel.com.tw.
Check	Click this button to have the ZyWALL verify that the connection to the specified <b>Update Server</b> is valid.
Update Now	Click this button to begin downloading policies from the <b>Update Server</b> immediately.
Auto Download & Update	Select <b>Enable</b> to have the ZyWALL automatically download policies from the <b>Update Server</b> regularly at the time and day specified below.
Update Schedule	This is only relevant when you select <b>Enable</b> in <b>Auto Download &amp; Update</b> .
Day	Select the day(s) you want the ZyWALL to automatically download policies from the <b>Update Server</b> .
Time	Select the time you want the ZyWALL to begin automatically downloading policies from the <b>Update Server</b> .
Apply	Click this button to save your changes back to the ZyWALL.
Reset	Click this button to close this screen without saving any changes.



## 6.6 User-defined Policies

You need some knowledge of packet header types and OSI (Open System Interconnection) to create your own **User-defined** rules.

Rule ordering is important as rules are applied in turn. You can order user-defined rules as you wish.

The total number of pre-defined and user-defined rules allowed on the ZyWALL is 3,000. The total number of user-defined rules allowed is 128. You can import up to a maximum of 128 rules as long as the total (pre-defined and user-defined) number of rules does not exceed 3,000. Therefore if you have 2,900 pre-defined rules and 50 user-defined rules, you may only import up to an additional 50 user-defined rules. If you try to import more than this the import will fail.

User-defined policies of the same name are allowed as the ZyWALL uniquely identifies each user-defined rule by assigning a (hidden) ID number; however it is recommended you give unique names to identify each rule more easily.

Click **IDP** from the navigation panel and then click the **User-defined** tab.


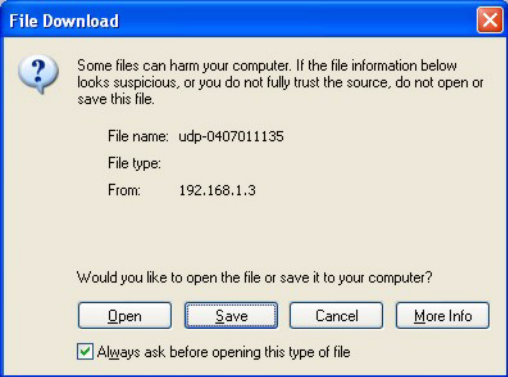
**Figure 43** User-defined Policies

The screenshot shows the 'IDP Policy' configuration window with the 'User-defined' tab active. It includes a checkbox to 'Enable User-defined Policy', an 'Import User-defined Policy' section with a 'File Path' input and 'Browse...' and 'Import' buttons, and a 'Create User-defined Policy' section with a 'User-defined Policy: (0/128)' counter. Below this is a table with columns: #, Enable, Alarm, Type, Name, Direction, Action, Note, Modify, Export. The table content is 'No User-define Policy.'. There are 'Delete ALL' and 'Export' buttons. At the bottom, there are 'Insert' and 'Move' buttons with text boxes for policy placement.

**Table 19** User-defined Policies

LABEL	DESCRIPTION
Enable User-defined Policy	This checkbox must be selected to have the ZyWALL check traffic using your custom IDP rules. You may clear it to keep the rules but not have them applied to traffic.
Import User-defined Policy	Use these fields to import another person's user-defined rules. The imported rules are in binary format ( <i>not</i> a text file), so they must be imported to the ZyWALL first and then edited one by one if so desired. They cannot be edited before being imported.
File Path	Save the file with the user-defined rules you want to import to your computer first. Then type the file path and name in the text box or click <b>Browse</b> to find it on your computer and finally click <b>Import</b> to import the file. You can import up to a maximum of 128 rules as long as the total (pre-defined and user-defined) number of rules does not exceed 3,000. User-defined rules of the same name are allowed so existing rules of the same name as imported rules will not be overwritten.
Create User-defined Policy	
User-defined Policy	This text box shows the number of user-defined rules already configured or imported in the ZyWALL (maximum 128).
#	This is the policy index number. Rule ordering is important as rules are applied in turn. You can reorder user-defined rules using the <b>Move</b> button.
Enable	Use this checkbox to enable or disable an individual user-defined rule without deleting it. Clear this checkbox to have the ZyWALL skip this (user-defined) rule when detecting intrusions.

**Table 19** User-defined Policies (continued)

LABEL	DESCRIPTION
Alarm	<p>An alarm is an action (an e-mail is sent) to be taken on the policy when a packet matches a rule. Alarm e-mails are not sent instantly but rather at periodic intervals (minimum five minutes).</p> <p>Select this checkbox to enable the alarm action. For other actions, select from the <b>Action</b> drop-down list box.</p>
Type	<p>Assign a signature category to your rule as described in <a href="#">Section 6.3 on page 53</a>.</p>
Name	<p>This is the rule name you configured for this intrusion type.</p>
Direction	<p>A policy rule direction refers to the intent of the policy rule.</p> <p><b>Incoming</b> means the policy applies to traffic coming from the WAN to the LAN.</p> <p><b>Outgoing</b> means the policy applies to traffic coming from the LAN to the WAN.</p> <p><b>Bidirectional</b> means the policy applies to traffic coming from and going to either direction.</p>
Action	<p>This field defines the action to be taken for a rule match. See <a href="#">Table 15 on page 65</a> for details on actions. An alarm is also an action to be taken on the policy, but you must select the <b>Alarm</b> checkbox to have the ZyWALL send an alarm when a traffic flow matches a rule.</p>
Note	<p>This field displays your added description of the rule you configured.</p>
Modify	<p>You may edit or delete an individual rule using these icons. Click the edit icon to modify a rule or click the delete icon to delete a rule. Before the rule is deleted, you will first see a confirmation dialog box.</p> 
Export	<p>Select the rule(s) you want to export and the click the <b>Export</b> button. You are then prompted to save the file to your computer.</p>  <p>A name is generated for the file but you may change this name to something more meaningful.</p>
Delete ALL	<p>Click this button to delete all user-defined IDP policies in one go.</p>
Insert	<p>Click this button to configure a new user-defined policy. Type a number where the rule should be inserted in the textbox that follows this label. Rule ordering is important as rules are applied in turn.</p>

**Table 19** User-defined Policies (continued)

LABEL	DESCRIPTION
Move	Type the rule number that should be moved in the first textbox (that follows this label), type the index number it should be moved to in the second textbox and then click <b>Move</b> to rearrange this rule. Rule ordering is important as rules are applied in turn.
Apply	Click this button to save your changes back to the ZyWALL.

### 6.6.1 Configuring a User-defined IDP Policy

All “policy attributions” have a logical AND relationship, that is, all “policy attributions” criteria must be met before a match is deemed found. Similarly, all “packet contents” have a logical AND relationship, that is, all “packet contents” criteria must be met before a match is deemed found. “Policy attributions” and “packet contents” also have a logical AND relationship, that is, both of the criteria (“policy attributions” and “packet contents”) must be met before a match is deemed found. From [Figure 43 on page 74](#), click **Insert** to create a new user-defined IDP policy.

**Figure 44** Configuring a User-defined IDP Policy

### ADD USER-DEFINE POLICY

**Attributions**

Name:

Type:

Note:

Severity:  Severe  High  Medium  Low  Very Low

Operating System:  Windows 95/98  Windows NT  Windows 2000/XP  
 Linux  FreeBSD  Solaris  
 SGI  Other Unix  Network Device  
 General

Protocol:

Repetition:  packet /  second

**Action**

Drop packet  Block connection  E-mail alarm  Log

**IP Header**

Direction:  Bidirectional  Incoming  Outgoing

Source IP:       
Mask:

Destination IP:       
Mask:

**TCP Header**

Source Port:  From  To

Destination Port:  From  To

**UDP Header**

Source Port:  From  To

Destination Port:  From  To

**ICMP Header**

Type:

Code:

**IGMP Header**

Type:

**Packet Content**

Matching Offset:  byte(s)

Matching Depth:  byte(s)

Method:

Content 1:

Method:

Content 2:

Method:

Content 3:

Method:

Content 4:

Method:

Content 5:


Method:

Content 6:

**Table 20** Configuring a User-defined IDP Policy

LABEL	DESCRIPTION
Attributions	The "attributions" define the characteristics of the intrusion for which you're configuring a policy. A traffic flow must match your operating system selections, your protocol definition and your repetition designation before your rule is invoked.
Name	Type a meaningful rule name to identify this policy. You can enter up to 128 single-Byte or double-Byte characters.
Type	Select an appropriate signature category as described in <i>section Signature Categories</i> .
Note	Type some added description for the rule you're configuring.
Severity	Assign a severity level based on the seriousness of the intrusion for which you're configuring a policy. See <a href="#">Table 14 on page 64</a> as a reference on policy severity.
Operating System	Select the target operating systems that the intrusion for which you're configuring a policy apply (that is, the operating systems you want to protect from this intrusion). SGI refers to Silicon Graphics Incorporated, who manufactures multi-user Unix workstations that run the IRIX operating system (SGI's version of UNIX).
Protocol	Select the protocol ( <b>IP</b> , <b>ICMP</b> , <b>IGMP</b> , <b>TCP</b> or <b>UDP</b> ) that characterizes this intrusion type. You then fill in the corresponding protocol header information further below in this screen. For example, if you choose <b>IP</b> , then fill in the corresponding <b>IP Header</b> fields (the other header fields will not be editable).
Repetition	For the protocol defined, type how many packets of the type defined, received on the ZyWALL per second constitute an "intrusion".
Action	Select what the ZyWALL should do in response to detecting packets with the above-defined attributes. You can choose to drop the packet, block the connection, e-mail an alarm and/or create a log.
IP Header	The next fields define the traffic flow direction, source IP address and destination IP address to which the policy applies. These fields are only editable when you select <b>IP</b> from the <b>Protocol</b> field above.
Direction	<p>A policy rule direction refers to the intent of the policy rule.</p> <p><b>Incoming</b> means the policy applies to traffic coming from the WAN to the LAN.</p> <p><b>Outgoing</b> means the policy applies to traffic coming from the LAN to the WAN.</p> <p><b>Bidirectional</b> means the policy applies to traffic coming from and going to either direction.</p> <p>Some rules such as blocking MSN Login would only apply to outgoing traffic as the intent is to block outgoing attempts to log into MSN Messenger. Similarly other rules would only apply to incoming traffic where the intent is to take an action on traffic initiated from somewhere on the WAN side. Select a direction for user-defined policies if you are clear on which direction the initiating traffic (from somewhere on the WAN or somewhere on the LAN) the policy action should apply to; if you're unsure, select <b>Bidirectional</b>.</p>

**Table 20** Configuring a User-defined IDP Policy (continued)

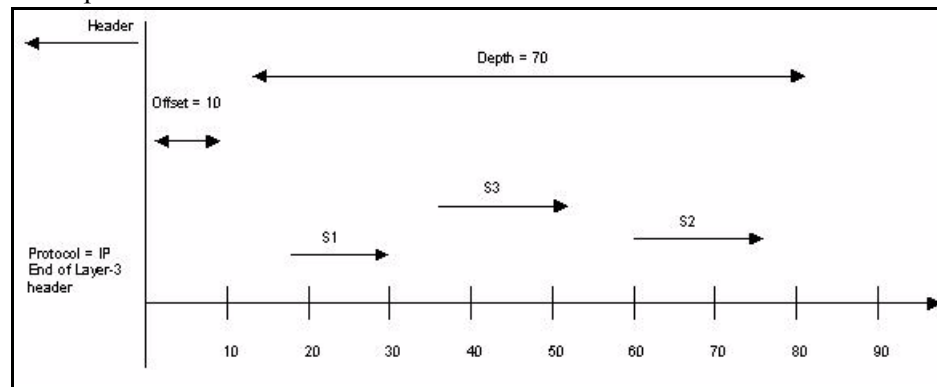
LABEL	DESCRIPTION
Source IP	<p>Select whether the policy applies to source packets that match (<b>Equal</b>), don't match (<b>Not Equal</b>), are within the range (<b>In Set</b>), are outside the range (<b>Not In Set</b>), have IP addresses that come after the number specified in the range (<b>Greater</b>), have IP addresses that come before the number specified in the range (<b>Lesser</b>) or all source IP addresses (<b>Don't Care</b>)</p>  <p>Then type an IP address and subnet mask in the corresponding textboxes to define a network range of IP addresses (subnet).</p>
Destination IP	<p>Select whether the policy applies to destination packets that match (<b>Equal</b>), don't match (<b>Not Equal</b>), are within the range (<b>In Set</b>), are outside the range (<b>Not In Set</b>), have IP addresses that come after the number specified in the range (<b>Greater</b>), have IP addresses that come before the number specified in the range (<b>Lesser</b>) or all source IP addresses (<b>Don't Care</b>). Then type an IP address and subnet mask in the corresponding textboxes to define a network range of IP addresses (subnet).</p>
TCP Header	<p>These fields are only editable when you select <b>TCP</b> from the <b>Protocol</b> field described above.</p>
Source Port	<p>Select whether the policy applies to source ports that match (<b>Equal</b>), don't match (<b>Not Equal</b>), are greater than (&gt;), or lesser than (&lt;) the port range you type in the <b>From</b> and <b>To</b> text boxes that follows.</p>
Destination Port	<p>Select whether the policy applies to destination ports that match (<b>Equal</b>), don't match (<b>Not Equal</b>), are greater than (&gt;), or lesser than (&lt;) the port range you type in the <b>From</b> and <b>To</b> text boxes that follows.</p>
UDP Header	<p>These fields are only editable when you select <b>UDP</b> from the <b>Protocol</b> field described above.</p>
Source Port	<p>Select whether the policy applies to source ports that match (<b>Equal</b>), don't match (<b>Not Equal</b>), are greater than (&gt;), or lesser than (&lt;) the port range you type in the <b>From</b> and <b>To</b> text boxes that follows.</p>
Destination Port	<p>Select whether the policy applies to destination ports that match (<b>Equal</b>), don't match (<b>Not Equal</b>), are greater than (&gt;), or lesser than (&lt;) the port range you type in the <b>From</b> and <b>To</b> text boxes that follows.</p>
ICMP Header	<p>These fields are only editable when you select <b>ICMP</b> from the <b>Protocol</b> field described above.</p>
Type	<p>Select whether the policy applies to ICMP types that match (<b>Equal</b>), don't match (<b>Not Equal</b>), are greater than (&gt;), or lesser than (&lt;) the ICMP type you type in the text box that follows.</p>
Code	<p>Select whether the policy applies to ICMP codes that match (<b>Equal</b>), don't match (<b>Not Equal</b>), are greater than (&gt;), or lesser than (&lt;) the ICMP code you type in the text box that follows.</p>
IGMP Header	<p>These fields are only editable when you select <b>IGMP</b> from the <b>Protocol</b> field described above.</p>
Type	<p>Select whether the policy applies to IGMP types that match (<b>Equal</b>), don't match (<b>Not Equal</b>), are greater than (&gt;), or lesser than (&lt;) the IGMP type you type in the text box that follows.</p>

**Table 20** Configuring a User-defined IDP Policy (continued)

LABEL	DESCRIPTION
Packet Content	<p>Packet Content parameters are for searching packet payloads. Do a traffic packet trace when an attack occurs and then isolate the part of the trace that identifies the attack, so you can paste the identifying portion into the following field(s) to identify the attack.</p> <p><b>Matching Offset</b> and <b>Matching Depth</b> apply to all strings. The order in which they're found doesn't matter (that is string 3 could be found before string 1 as long as it's within the depth defined). String overlaps are also allowed.</p> <p><b>Note:</b> All strings must be found to constitute a match.</p>
Matching Offset	<p><b>Matching Offset</b> defines the payload start point. If <b>Protocol</b> type is <b>IP</b>, then the matching starting point is at the end of the layer-3 header; otherwise, it starts matching from the end of the layer-4 header.</p>
Matching Depth	<p><b>Matching Depth</b> the length of the payload to search for a match.</p>
Method	<p>Choose from <b>Case sensitive</b> (upper case and lower case letters are considered different), <b>Case insensitive</b> (upper case and lower case letters are considered the same), <b>URL string</b> (a complete web site address), <b>Hexadecimal</b> (0-9 and a -f characters).</p> <p>The <b>URL string</b> is case insensitive, can include the character '?' and spaces and ignores character order. Therefore "/cgi-bin/foo.exe?p1=abc&amp;p2=def" and "/cgi-bin/foo.exe?p2=def&amp;p1=abc" are considered a match. Extra parameters in the payload don't matter either. For example, a pattern "/cgi-bin/foo.exe?p1=abc&amp;p2=def" would match a packet with URL string "/cgi-bin/foo.exe?p0=xyz&amp;p1=abc&amp;p2=def".</p>
Content 1~6	<p>Type or paste the content (string or hexadecimal characters) into the corresponding content field(s).</p>
Apply	<p>Click this button to save your changes back to the ZyWALL.</p>
Cancel	<p>Click this button to close this screen without saving any changes.</p>

## 6.6.2 Packet Content Example

In the following example, the rule is for the **IP** protocol, so the payload search begins at the end of layer-3. Three strings (S1, S2 and S3) have been defined and have been found after the **Matching Offset** (10) and within the **Matching Depth** (70). The order in which they are found doesn't matter. The same matching offset and depth applies to all strings and string overlaps are allowed.





## 6.7 Registering your ZyWALL

Use the **Registration** screen to enable IDP service on the ZyWALL. You need to do this before you update new policies. Follow this procedure to do this.

- 1** Go to <http://www.myZyXEL.com>, ZyXEL Communications online services center.
- 2** If you have not already done so for another ZyXEL product, create a myZyXEL.com account containing a login name and password. You will need a valid e-mail address to which a subscription code is sent that validates your e-mail address and login name/ password.
- 3** Register your ZyXEL product, for example the ZyWALL IDP 10. You will need the product serial number and authentication code (product MAC address), which should be found on a label in the package that contained the product.
- 4** After you have registered the product, go to the product details and click the intrusion policy service **Activate**<sup>1</sup> link.
- 5** A screen then displays showing an **Activation Key**. This information is also sent to your myZyXEL.com-registered e-mail address. Store this e-mail for future reference.
- 6** Log into the ZyWALL web configurator; click **IDP** and then the **Registration** tab to display the screen as shown next.
- 7** Paste the generated key into the **Registration** screen<sup>1</sup> and click **Apply**.

---

1. Actual label names are liable to change, but the intent should remain the same. These are the label names used at the time of writing.

**Figure 45** Registering ZyWALL

**IDP Policy**

Pre-defined    Update    User-defined    **Registration**

**Registration**

Before enabling IDP service, you should go to [myZyXEL.com](http://myZyXEL.com) for service activation. By entering your L/K (License Key), you would acquire an A/K (Activation Key) on the web page. Please copy & paste it onto the following field.

**Note:** After successful registration, return to the ZyXEL device web configurator screen to configure IDP.

Registration Status: **Registered**

myZyXEL.com

Activation Key

Apply    Reset

**Table 21** Registering ZyWALL

LABEL	DESCRIPTION
Registration Status	This read-only label displays <b>Unregistered</b> even after you paste the <b>Activation Key</b> and click <b>Apply</b> in this screen. It will only display <b>Registered</b> after you paste the <b>Activation Key</b> , click <b>Apply</b> in this screen and then update your pre-defined policies at <a href="http://updateidp.zyxel.com">updateidp.zyxel.com</a> or <a href="http://updateidp.zyxel.com.tw">updateidp.zyxel.com.tw</a> .
Activation Key	Paste the generated key as described on <a href="#">page 81</a> . Be careful to avoid pasting trailing spaces.
Apply	Click this button to save your changes back to the ZyWALL.
Reset	Click this button to close this screen without saving any changes.



# CHAPTER 7

## Log and Report

This chapter describes how to use the Log and Report screens.

### 7.1 Logs

To view logs and alert messages, click **LOGS** under the **LOG & REPORT** heading in the MAIN MENU of the Web Configurator.

The log wraps around and deletes the old entries after it fills. You can re-order the logs according to time generated by clicking the **Time** column title. A triangle indicates the direction of the sort order.


To configure your ZyWALL's system logs, click **LOGS** in the MAIN MENU of the Web Configurator.

**Figure 46** View Log

#	Time▲	Message	Source	Destination	Action	Note
1	2002/02/18 16:40:22	WEB: Change Administrator Inactivity Timer to 0	192.168.1.10:3384	192.168.1.3:80		Information
2	2002/02/18 16:40:02	WEB: Login OK!	192.168.1.10:3384	192.168.1.3:80		Information
3	2002/02/18 15:38:10	System: Time synchronization failed				Warning
4	2002/02/18 15:36:20	System: Time synchronization failed				Warning
5	2002/02/18 15:34:30	System: Time synchronization failed				Warning
6	2002/02/18 15:32:38	WEB: Login OK!	192.168.1.10:3191	192.168.1.3:80		Information
7	2002/02/18 15:32:25	System: ZyWALL IDP 10 startup!				Information

The following table describes the fields in this screen.

**Table 22** View Log

LABEL	DESCRIPTION
Logs	
Display	<p>Select a log category from the drop down list box to display logs within the selected category:</p>  <p><b>All Logs</b> (view all logs)  <b>System Log</b> (view logs related with the ZyWALL such as login to the ZyWALL or startup)  <b>IDP Event Log</b> (view logs related to detected intrusions)</p>
Clear	Click this button clear all the logs.
Refresh	Click this button to refresh the log screen.
Page	Use the dropdown list to select the log page you want.
<Prev Next >	Use these buttons to navigate between first, previous, next and last pages of the logs.
#	This displays the number of the log that was recorded.
Time	This field displays the date and time the log was recorded. Click the <b>Time</b> label to sort logs in ascending or descending order.
Message	This field states the reason for the log.
Source	This field lists the source IP address and the port number of the packet that caused the log.
Destination	This field lists the destination IP address and the port number of the packet that caused the log.
Action	This field displays the action taken on the packet that caused the (IDP event) log.
Note	This field displays additional information about the log entry.

## 7.2 Report

You can send logs by e-mail or send them to a syslog server.

### 7.2.1 E-Mail

Use the **E-Mail** Setup screen to configure to where and when the ZyWALL is to send logs by e-mail. Logs may be e-mailed as soon as the log is full (see **Report Schedule**).

Click **REPORT** under the **LOG & REPORT** heading in the MAIN MENU of the web configurator, and then click the **E-MAIL** tab.

Figure 47 Report: E-Mail

The following table describes the fields in this screen.

Table 23 Report: E-Mail

LABEL	DESCRIPTION
E-Mail Setup	
Active	Click this button to enable e-mailed reports and allow editing of the fields below.
Report Schedule	Select the frequency of e-mailed reports: weekly, daily, hourly, or only when the log is full. If the <b>Weekly</b> or <b>Daily</b> option is selected, specify a time of day when the e-mail should be sent. If the <b>Hourly</b> option is selected, specify the time (minutes and hour) that the e-mail should be sent. If the <b>Weekly</b> option is selected, then also specify which day of the week the e-mail should be sent. If the <b>When Log is Full</b> option is selected, a log is sent as soon as the log fills up.
Day	Select which day of the week to send the logs.
Time	Type the time of the day in 24-hour format (for example 23:00 equals 11:00 PM) to send the logs.
Mail Server	Type the IP address or URL of the mail server. If this field is left blank, reports will not be sent via e-mail. Your mail server must not request a username or password. If it does, you must disable this first before using it to send ZyWALL reports. If this field is left blank, reports will not be sent via e-mail.
Send From	Type the sender e-mail address in this field.
Recipient(s)	Type up to three e-mail address(es) separated by semi-colons of people who should receive these reports.

**Table 23** Report: E-Mail (continued)

LABEL	DESCRIPTION
Subject	Type a title that you want to be in the subject line of the report that the ZyWALL sends.
SMTP Authentication	SMTP (Simple Mail Transfer Protocol) is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another. Select the check box to activate SMTP authentication if your mail server requires a user name and password. If mail server authentication is needed but this feature is not selected, you will not receive e-mail logs.
User Name	Enter the your mail account user name (up to 31 characters).
Password	Enter the password associated with the user name above.
Apply	Click this button to save your changes back to the ZyWALL.
Reset	Click this button to begin configuring this screen afresh.

## 7.2.2 Syslog

Syslog logging sends a log to an external syslog server used to store logs.

**Figure 48** Report: syslog

The following table describes the fields in this screen.

**Table 24** Report: syslog

LABEL	DESCRIPTION
Syslog Logging	
Active	Click <b>Active</b> to enable syslog logging.
Syslog Server	Enter the server name or IP address of the syslog server that will log the selected categories of logs.

**Table 24** Report: syslog (continued)

LABEL	DESCRIPTION
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Traffic Logging	
Send Raw Traffic Statistics to Syslog Server for Analysis	Select the check box and click <b>Apply</b> to have the ZyWALL send unprocessed traffic statistics to a syslog server for analysis. You must have the syslog server already configured in this screen.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 7.3 Alarm Schedule

An alarm is a “warning log” generated by an event that warrants more serious attention. They include system errors and serious intrusions.

Click **ALARM** under the **LOG & REPORT** heading in the MAIN MENU of the Web Configurator.

**Figure 49** Alarm

The screenshot shows the 'ALARM' configuration page with the following fields and controls:

- Active:**
- Period:** every  minutes. (minimum 5)
- Mail Server:**
- Send From:**
- Recipient(s):**
- Subject:**
- SMTP Authentication:**
- User Name:**
- Password:**
- Buttons:** Apply, Reset

The following table describes the fields in this screen.



**Table 25** Alarm

<b>LABEL</b>	<b>DESCRIPTION</b>
Alarm Schedule	
Active	Select this field to activate your ZyWALL's alarm schedule as configured in the fields below.
Period	This field is used to configure the frequency of alarm messages. Alarm messages are not sent instantaneously. There is a minimum wait period of five minutes between when alarm messages are sent out.
Mail Server	Type the IP address or URL of the mail server. If this field is left blank, alarms will not be sent via e-mail. Your mail server must not request a username or password. If it does, you must disable this first before using it to send ZyWALL alarms.
Send From	Type the sender e-mail address in this field.
Recipient(s)	Type up to three e-mail address(es) separated by semi-colons of people who should receive these reports.
Subject	Type a title that you want to be in the subject line of the alarm that the ZyWALL sends.
SMTP Authentication	SMTP (Simple Mail Transfer Protocol) is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another. Select the check box to activate SMTP authentication if your mail server requires a user name and password. If mail server authentication is needed but this feature is not selected, you will not receive e-mail logs.
User Name	Enter the your mail account user name (up to 31 characters).
Password	Enter the password associated with the user name above.
Apply	Click this button to save your changes back to the ZyWALL.
Reset	Click this button to begin configuring this screen afresh.

# CHAPTER 8

## Maintenance

### 8.1 Maintenance Overview

Use the maintenance screens to change the ZyWALL password, ZyWALL time, upload firmware, manage configuration files and restart the ZyWALL.

### 8.2 Password

Use the **Password** screen to change the ZyWALL password. You should do this regularly for security reasons.

**Figure 50** Maintenance: Password

**Table 26** Maintenance: Password

LABEL	DESCRIPTION
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type your new system password (minimum of 1 to 64 printable characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type.
Password Confirm	Type the new password again in this field.
Apply	Click this button to save your changes back to the ZyWALL.
Reset	Click this button to begin configuring this screen afresh.

## 8.2.1 Forget Password

If you forgot your password, then you will have to reset it to the factory defaults (“1234”) from debug mode via the console port.

- 1 Turn off and then turn on the ZyWALL or use the `reboot` command to restart the ZyWALL.
- 2 As the ZyWALL restarts you must enter debug mode before the login screen appears. Press `<ENTER>` within 5 seconds of when the console screen displays “Press ENTER to enter Debug Mode”.
- 3 Type `reset` after the “debug” prompt. You will lose all your custom ZyWALL configurations including your user-defined rules. (If you type `reset all`, then all pre-defined rules will be erased too). The IP address of the ZyWALL will be “192.168.1.3” and the password will be “1234”.
- 4 Type `reboot` to restart the ZyWALL and complete the reset. (This is also how you exit debug mode.)

The following screen is an example of how you reset the ZyWALL to the factory defaults while in debug mode.

**Figure 51** Debug Mode Reset Example

```
IDS system kernel loader v1.0.0.0 2004/04/02
(ZyXEL)
Press ENTER to enter Debug Mode
Enter DEBUG Mode
...
Loading Kernel Image <DBGBOOT>
.....
Checksum is valid.
Starting address is at 0x100000
Kernel image load completed.
Starting kernel...
DebugKernel Version 1.0.4 (2004/05/05)
DBG>
Are you sure to reset all settings to
manufacturing defaults? (y/n)y
Reset to defaults OK. Please reboot to apply new
change.
DBG>reboot
```

## 8.3 Time and Date

To change your ZyWALL's time and date, click **MAINTENANCE**, then the **Time and Date** tab. The screen appears as shown. Use this screen to configure the ZyWALL's time based on your local time zone.

### 8.3.1 Pre-defined NTP Time Servers List

The ZyWALL uses the following pre-defined list of NTP time servers if you do not specify a timeserver or it cannot synchronize with the timeserver you specified.

**Note:** The ZyWALL can use this pre-defined list of time servers regardless of the Time Protocol you select.

When the ZyWALL uses the pre-defined list of NTP time servers, it randomly selects one server and tries to synchronize with it. If the synchronization fails, then the ZyWALL goes through the rest of the list in order from the first one tried until either it is successful or all the pre-defined NTP time servers have been tried.

**Table 27** Default Time Servers

ntp1.cs.wisc.edu
ntp1.gbg.netnod.se
ntp2.cs.wisc.edu
tock.usno.navy.mil
ntp3.cs.wisc.edu
ntp.cs.strath.ac.uk
ntp1.sp.se
time1.stupi.se
tick.stdtime.gov.tw
tock.stdtime.gov.tw
time.stdtime.gov.tw

**Figure 52** Maintenance: Time Setting

**Table 28** Time and Date

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your ZyWALL. Each time you reload this page, the ZyWALL synchronizes the time with the timeserver (if configured).
Current Date	This field displays the date of your ZyWALL. Each time you reload this page, the ZyWALL synchronizes the date with the timeserver (if configured).
Time and Date Setup	
Manual	Select this radio button to enter the time and date manually. When you configure a new time and date manually, the <b>Time Zone</b> settings are ignored.
New Time (hh:mm:ss)	This field displays the last updated time from the timeserver or the last time configured manually. When you set <b>Time and Date Setup</b> to <b>Manual</b> , enter the new time in this field and then click <b>Apply</b> .

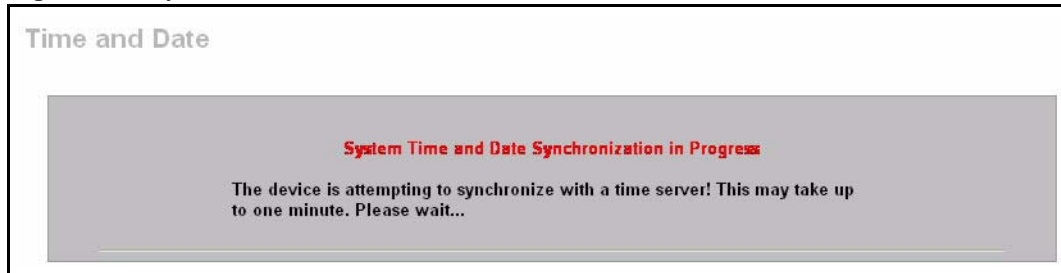
**Table 28** Time and Date (continued)

LABEL	DESCRIPTION
New Date (yyyy-mm-dd)	This field displays the last updated date from the timeserver or the last date configured manually. When you set <b>Time and Date Setup</b> to <b>Manual</b> , enter the new date in this field and then click <b>Apply</b> .
Get from Time Server	Select this radio button to have the ZyWALL get the time and date from the timeserver you specify below.
Time Protocol	Select the time service protocol that your time server uses. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main difference between them is the format. <b>Daytime (RFC 867)</b> format is day/month/year/time zone of the server. <b>Time (RFC 868)</b> format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. The default, <b>NTP (RFC 1305)</b> , is similar to <b>Time (RFC 868)</b> .
Time Server Address	Enter the IP address or URL of a timeserver. Check with your ISP/network administrator if you are unsure of this information. The ZyWALL uses a pre-defined list of NTP time servers if you do not specify a timeserver or it cannot synchronize with the timeserver you specified (see <a href="#">Table 27 on page 92</a> ).
Synchronize Now	Click this button and wait for one minute to have the ZyWALL get the time and date from a timeserver (see the <b>Time Server Address</b> field). This also saves your changes (including the time server address).
Time Zone Setup	
Time Zone	This field is only applicable when the ZyWALL gets the time from a timeserver. Choose the time zone of the location of the ZyWALL from the drop-down list box. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Enable Daylight Saving	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use daylight savings time.
Start Date (mm-dd)	Enter the month and day that your daylight-savings time starts on if you selected <b>Enable Daylight Saving</b> .
End Date (mm-dd)	Enter the month and day that your daylight-savings time ends on if you selected <b>Enable Daylight Saving</b> .
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

### 8.3.2 Time Server Synchronization

Click the **Synchronize Now** button to get the time and date from the predefined timeserver or the timeserver you specified in the **Time Server Address** field.

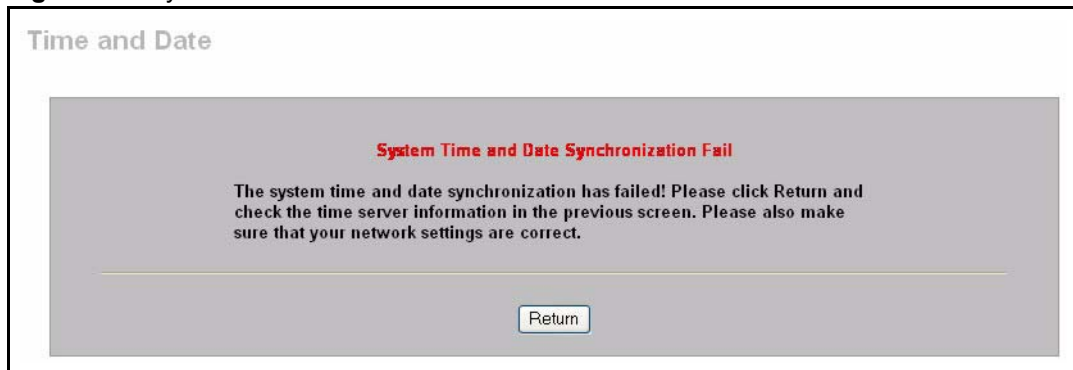
When the **System Time and Date Synchronization in Process** screen appears, wait up to one minute.

**Figure 53** Synchronization in Process

Click the **Return** button to go back to the **Time and Date** screen after the time and date is updated successfully.

**Figure 54** Synchronization is Successful

If the update was not successful, the following screen appears. Click **Return** to go back to the **Time and Date** screen.

**Figure 55** Synchronization Fail

## 8.4 Firmware Upload

Find firmware at [www.zyxel.com](http://www.zyxel.com) in a file that (usually) uses the system model name with a "\*.bin" extension, e.g., "zywall.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. Use the **Firmware Upload** screen to schedule and upload firmware to the ZyWALL.

**Figure 56** Maintenance: F/W Upload

**FIRMWARE UPLOAD**

Password | Time and Date | F/W Upload | Configuration | Restart

---

**Local Upgrade**

To upgrade the IDP firmware, browse to the location of the binary (.BIN) upgrade file and click Upload. Upgrade files can be downloaded from website. If the upgrade file is compressed (.ZIP file), please extract the binary (.BIN) file first.

File Path

---

**Remote Upgrade**

Update Server

Auto Download & Update  Enable  Disable

---

**Schedule**

**Check & Download**

Day  
 Sun  Mon  Tue  Wed  Thu  Fri  Sat

Time  
 Start:  (hour):  (Minute)

**Upgrade & Reboot**

Day  
 Sun  Mon  Tue  Wed  Thu  Fri  Sat

Time  
 Start:  (hour):  (Minute)

**Table 29** Maintenance: F/W Upload

LABEL	DESCRIPTION
Local Upgrade	
File Path	Type in the location of the file you want to upload in this field or click Browse... to find it.
Browse...	Click <b>Browse...</b> to find the BIN file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click <b>Upload</b> to begin the upload process. This process may take up to two minutes.
Remote Upgrade	
Update Server	Type in the IP address of the server from which to download the firmware to your ZyWALL. Remember that you must first decompress compressed (.ZIP) files. The default server at the time of writing is updateidp.zyxel.com. It is also possible to use updateidp.zyxel.com.tw.

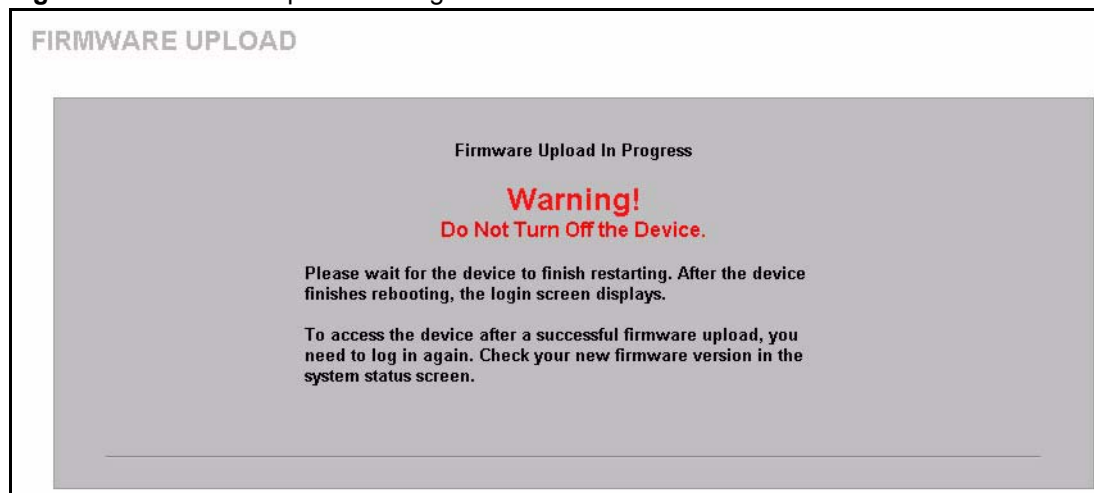


**Table 29** Maintenance: F/W Upload (continued)

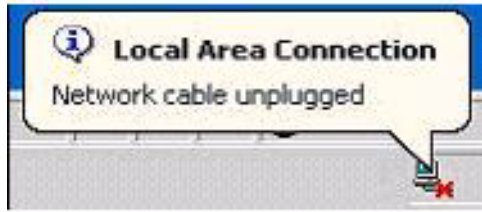
LABEL	DESCRIPTION
Check	Click <b>Check</b> to check that the link to the remote server is valid.
Update Now	Click <b>Update Now</b> to immediately download the firmware file from the server and upload it your ZyWALL.
Auto Download & Update	Click <b>Enable</b> to allow your ZyWALL to automatically download and update firmware (need restart) on the days and times specified below. Click <b>Disable</b> to disallow your ZyWALL from automatically downloading and updating firmware.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Schedule: You need to select <b>Enable</b> in the <b>Auto Download &amp; Update</b> field before setting a schedule.	
Check & Download	Select the day(s) to check for new firmware downloads. Select the time (hour and minutes) to check for new firmware downloads. If there is new firmware found on the specified update server, it is downloaded to the ZyWALL but not updated, so the ZyWALL does not have to restart. Choose a day and time to download new firmware to the ZyWALL when the network path from the ZyWALL to the update server will be least busy.
Upgrade & Reboot	Select the day(s) to upload new firmware to the ZyWALL. The firmware should have already been downloaded to the ZyWALL. Select the time (hour and minutes) to upload new firmware to the ZyWALL. The ZyWALL will automatically restart after uploading, so it is recommended to choose a day and time to upload new firmware when your network is not so busy, so as to minimize interruption.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.

After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the ZyWALL again.

**Figure 57** Firmware Upload in Progress



The ZyWALL automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

**Figure 58** Network Temporarily Disconnected

After two minutes, log in again and check your new firmware version in the **System Status** screen.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **F/W Upload** screen.

**Figure 59** Firmware Upload Error

## 8.5 Configuration

Use the **Configuration** screen to backup and restore ZyWALL configuration files or reset to the factory default configuration file.

The ZyWALL configuration file includes all ZyWALL system settings and user-defined rules, but NOT pre-defined rules.

**Figure 60** Maintenance: Configuration



### 8.5.1 Backup Configuration

**Backup Configuration** allows you to back up (save) the ZyWALL’s current configuration to a file on your computer. Once your ZyWALL is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the ZyWALL’s current configuration to your computer.

### 8.5.2 Restore Configuration

**Restore Configuration** allows you to upload a new or previously saved configuration file from your computer to your ZyWALL.

**Table 30** Restore Configuration

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Browse ...</b> to find it.
Browse...	Click <b>Browse...</b> to find the file you want to upload.
Upload	Click <b>Upload</b> to begin the upload process.

After you see a “configuration upload successful” screen, you must then wait one minute before logging into the device again.

The device automatically restarts in this time causing a temporary network disconnect.

If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address. See your *Quick Start Guide* for details on how to set up your computer's IP address.

If the upload was not successful, you will see a **Restore configuration error** screen.

### 8.5.3 Back to Factory Defaults

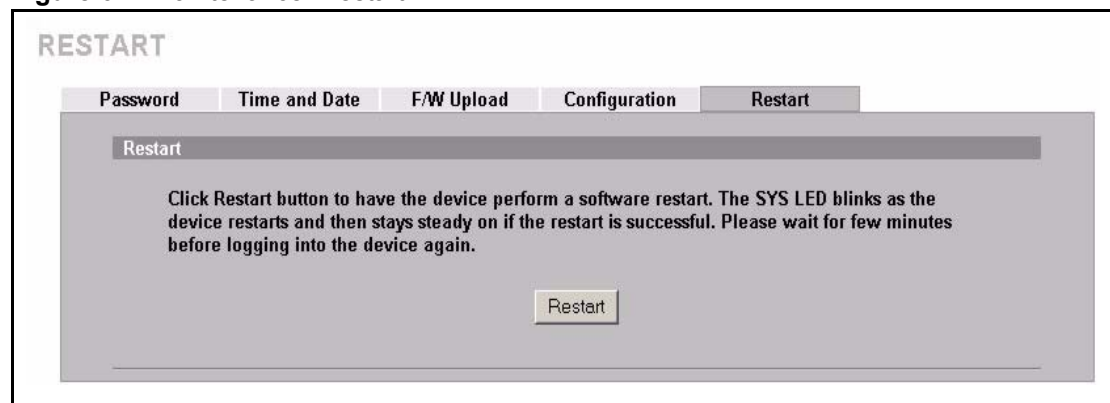
Pressing the **Reset** button in this section clears all user-entered configuration information, including user-defined rules (not pre-defined rules) and returns the ZyWALL to its factory defaults as shown on the screen. A warning screen appears first.

If you want to revert to factory default configurations (with no user-defined rules) AND clear all pre-defined rules use the `reset all` command from the console port.

## 8.6 Restart

**Restart** allows you to reboot the ZyWALL without turning the power off. Click **MAINTENANCE**, and then **Restart**. This does not affect the ZyWALL's configuration.

**Figure 61** Maintenance: Restart





# CHAPTER 9

## Command Line Interface Overview

This chapter briefly introduces the command line interface and lists the available commands. See the Support CD for detailed information on using commands.

In addition to the web configurator, you can use commands to configure the ZyWALL.

However, if you have problems with your ZyWALL, customer support may request that you issue some of these commands to assist them in troubleshooting.

Telnet to your ZyWALL or connect a computer to the console port and use terminal emulation software configured to the following parameters:

- VT100 terminal emulation
- 9600 bps
- No parity, 8 data bits, 1 stop bit
- No flow control

### 9.1 Command Syntax Conventions

The command keywords are in `courier new` font.

- 1 There is no command history. Previously typed commands are not remembered and must be reentered.
- 2 The command keywords must be entered exactly as shown, or abbreviate each part of the command to three letters (only).
- 3 The required fields in a command are enclosed in angle brackets (<>), for instance,

```
list port <port #>
```

means that you must specify the port number for this command.

- 4 The optional fields in a command are enclosed in square brackets ([ ]), for instance,

```
config [save]
```

means that the `save` field is optional.

- 5 A “|” means “or”

[on|off] means that you can use either on or off.

**6** “Command” refers to a command used in the command line interface (CLI command).

### 9.1.1 Help Facility

You can issue the `help` or `help all` command at any time. The system will display a list of available commands in response.

## 9.2 Login

When you log in you will be prompted for the username (“admin”) and password (default is “1234”). If you changed the password in the web configurator, then use that new password here. If the password prompt appears before the username prompt, press <ENTER> until you are prompted for the username. Then enter `admin` (this is not changeable) followed by the password at the password prompt followed by <ENTER>.

## 9.3 Commands

The following table lists all of the commands that you can use with the ZyWALL.

**Table 31** Commands Summary

COMMAND					DESCRIPTION
Set	Log	logmax			Set the maximum number of logs the device generates every second
	System	passwd <value>			Set up the login password. This is same password used for console, SSH and web login.
		system timeout			Set up the management idle timeout
		backup			Back up configuration
		restore			Restore configuration
		vlan	id		Set up vlan id
			link <UnTAg Tag>		Enable/disable vlan tag
		ip <ip address>			Set up device ip address
		mask			Set up device subnet mask
		gateway			Set up device gateway ip address

**Table 31** Commands Summary (continued)

COMMAND				DESCRIPTION
		detect	vpnbyypass <ON/OFF>	Allow/disallow bypass of VPN packets it doesn't recognize.
			portscan <ON/OFF>	Allow/disallow port scanning
			fragment <ON/OFF>	Enable/disable fragment function
			stateful <ON/OFF>	Enable/disable TCP state check
			integrity <ON/OFF>	Enable /disable TCP packet state integrity using this command
			tcptimeout <value>	Set the maximum TCP idle timeout (this is how long a TCP connection is allowed to remain idle.
			pinglen <value>	Set up maximum ping length
			pingmax <value>	wan Set up maximum ping packet accepted at wan port
				lan Set up maximum ping packet accepted at lan port
			policy	wan <ON/OFF> Set up policy check on/off wan port. Policy checks include both user-defined and pre-defined rules.
				lan <ON/OFF> Set up policy check on/off loan port
	Interface	link	wan	10 <half/full> Set up wan port speed 10 at full/half duplex
				100 <half/full> Set up wan port speed 100 at full/half duplex
				auto <half/full> Enable auto negotiation
			lan	10 <half/full> Set up lan port speed 10 at full/half duplex
				100 <half/full> Set up lan port speed 100; atfull/half duplex
				auto <half/full> Enable auto negotiation
		stealth	wan <ON/OFF>	Enable/disable stealth mode on the wan port. Replies to outgoing traffic are not allowed. When a port is in stealth mode, you cannot do remote management nor policy checks on that port.
			lan <ON/OFF>	Enable/disable stealth mode on the lan port



**Table 31** Commands Summary (continued)

COMMAND				DESCRIPTION	
	Remote	snmp	on <LAN+MGMT/WAN+MGMT/MGMT/ALL>	Enable remote snmp access from LAN+MGMT/WAN+MGMT/MGMT ONLY/ALL port	
			off	Disable remote snmp access	
			acl <ip address>	Set up access control list ip address	
			community	ro <value>	Set up community read only string
				rw <value>	Set up community read/write string
				trap <value>	Set up snmp trap
			system name <value>	Set up remote snmp system name	
			trap <ON/OFF>	Enable/disable remote snmp trap	
			trap ip <value>	Set up remote snmp trap send to ip address	
		ssh	on <LAN+MGMT/WAN+MGMT/MGMT/ALL>	Enable remote SSH access from LAN+MGMT/WAN+MGMT/MGMT ONLY/ALL port	
			off	Disable remote SSH access	
			acl <ip address>	Set up access control list ip address	
		web	on <LAN+MGMT/WAN+MGMT/MGMT/ALL>	Enable remote web access from LAN+MGMT/WAN+MGMT/MGMT ONLY/ALL port	
			off	Disable remote we access	
			acl <ip address>	Set up access control list ip address	
Get	State			Get system state (Inline, Monitor or Bypass).	
	Log			Get device log	
	System			Get system information	
	Time			Get device time	
	Interface			Get interface information	
	All			Get all information	
	Remote			Get remote access information	
Reboot				Restart the device. Use this command to also exit debug mode.	

**Table 31** Commands Summary (continued)

COMMAND					DESCRIPTION
Help					Displays a "help" message
Reset					Resets the ZyWALL to the factory defaults and erases all user-defined policies.
Reset All					As Reset and erases all pre-defined policies too.
Netstat					Display network state
Ping					Perform Ping from the ZyWALL
Arp					Display address resolution protocol information (device MAC address and IP address table).



# Appendix A

## Introduction to Intrusions

### Introduction to Ports

Computers share information over the Internet using a common language called TCP/IP. An “extension number”, called the "TCP port" or "UDP port" identifies these protocols, such as HTTP (Web), FTP (File Transfer Protocol), POP3 (e-mail), etc. For example, Web traffic by default uses TCP port 80.

When computers communicate on the Internet, they are using a client/server model, where the server "listens" on a specific TCP/UDP port for information requests from remote client computers on the network.

Some of the most common IP ports are:

**Table 32** Common IP Ports

21	FTP	53	DNS
23	Telnet	80	HTTP
25	SMTP	110	POP3

### Introduction to Denial of Service

The goal of Denial of Service (DoS) attacks is not to steal information, but to disable a device or network on the Internet.

The following are some DoS example attacks.

### Buffer Overflow Attacks

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. The excess information can overflow into adjacent buffers, corrupting or overwriting the valid data held in them.

Intruders could run codes in the overflow buffer region to obtain control of the system, install a backdoor or use the victim to launch attacks on other devices.

## Ping of Death

Ping of Death uses a "ping" utility to create an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. The oversize packet is then sent to an unsuspecting system. Systems may crash, hang or reboot.

## Teardrop

Teardrop attack exploits weaknesses in the reassembly of IP packet fragments. As data is transmitted through a network, IP packets are often broken up into smaller chunks. Each fragment looks like the original IP packet except that it contains an offset field that says, for instance, "This fragment is carrying bytes 200 through 400 of the original (non fragmented) IP packet." The Teardrop program creates a series of IP fragments with overlapping offset fields. When these fragments are reassembled at the destination, some systems will crash, hang, or reboot.

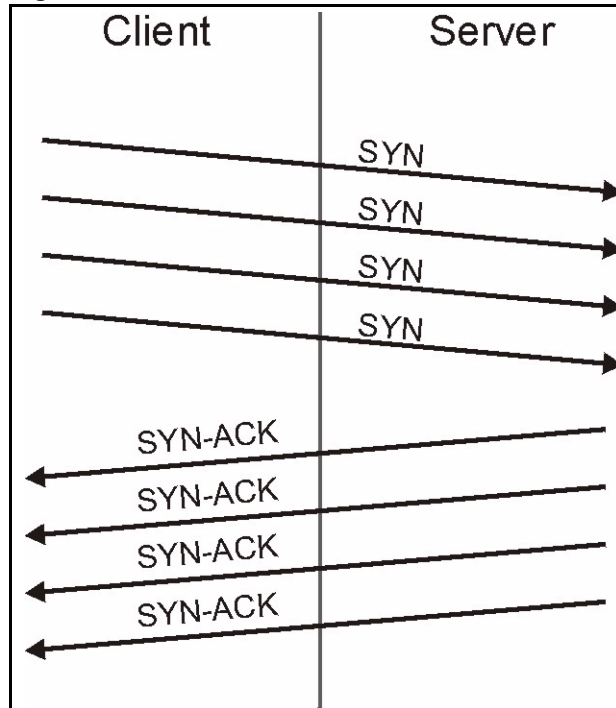
## SYN Attack

This attack is executed during the handshake that initiates a communication session between two applications.

### Figure 62 Three-Way Handshake

Under normal circumstances, the application that initiates a session sends a SYN (synchronize) packet to the receiving server. The receiver sends back an ACK (acknowledgment) packet and its own SYN, and then the initiator responds with an ACK (acknowledgment). After this handshake, a connection is established.

A SYN attack floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on what is known as a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer (which is set at relatively long intervals) terminates the three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.

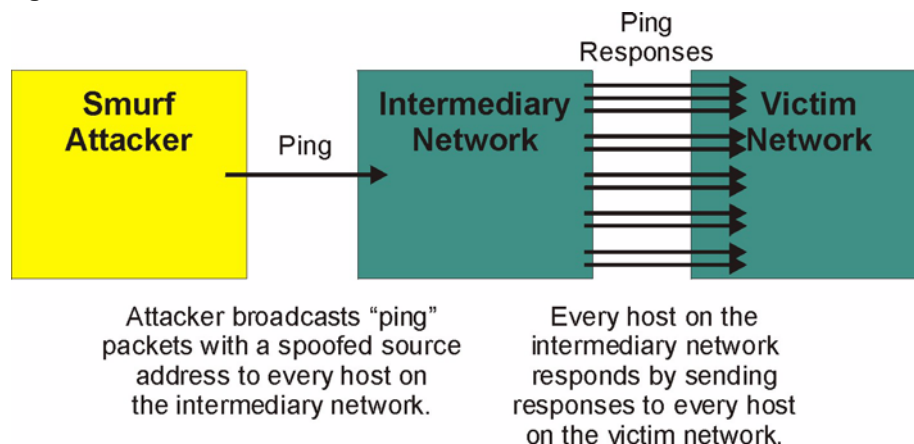
**Figure 63** SYN Flood

## LAND Attack

In a LAND attack, hackers flood SYN packets into the network with a spoofed source IP address of the targeted system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

## Smurf Attack

A Smurf attack targets a feature in the IP specification known as directed or subnet broadcasting, to quickly flood the target network with useless data. A Smurf hacker floods a router with Internet Control Message Protocol (ICMP) echo request packets (pings). Since the destination IP address of each packet is the broadcast address of the network, the router will broadcast the ICMP echo request packet to all hosts on the network. If there are numerous hosts, this will create a large amount of ICMP echo request and response traffic. If a hacker chooses to spoof the source IP address of the ICMP echo request packet, the resulting ICMP traffic will not only clog up the "intermediary" network, but will also congest the network of the spoofed source IP address, known as the "victim" network. This flood of broadcast traffic consumes all available bandwidth, making communications impossible.

**Figure 64** Smurf Attack

## Traceroute

Traceroute is a utility used to determine the path a packet takes between two endpoints. Sometimes when a packet filter firewall is configured incorrectly an attacker can traceroute the firewall gaining knowledge of the network topology inside the firewall.

## IP Spoofing

Often, many DoS attacks also employ a technique known as IP spoofing as part of their attack. IP spoofing may be used to break into systems, to hide the hacker's identity, or to magnify the effect of the DoS attack. IP spoofing is a technique used to gain unauthorized access to computers by tricking a router or firewall into thinking that the communications are coming from within the trusted network. To engage in IP spoofing, a hacker must modify the packet headers so that it appears that the packets originate from a trusted host and should be allowed through the router or firewall.

## Distributed Denial-Of-Service Attack

A distributed denial-of-service (DDoS) attack is one in which multiple compromised systems attack a single target, thereby causing denial of service for users of the targeted system. A hacker begins a DDoS attack by exploiting vulnerability in one computer system and making it the "DDoS source". It is from this source that the hacker identifies and communicates with other systems that can be compromised. The hacker instructs the "DDoS source(s)" to launch flood attacks against a specified target. The inundation of packets to the target causes a denial of service.

## Scanning

Hackers scan ports to find targets. Some example methods are as follows:

A TCP connect() call is used to open a connection to every interesting port on the machine. If the port is listening, connect() will succeed, otherwise the port isn't reachable.

SYN scanning (half-open scanning) does not open a full TCP connection. A SYN packet is sent, pretending to open a genuine connection and waits for a response. A SYN/ACK will indicate that the port is listening. If a SYN/ACK is received, a RST is sent to tear down the connection.

The Port Scanner Nmap uses raw IP packets to determine what hosts are available on the network, what services (ports) they are available, what operating system (and OS version) they are running, what type of packet filters/firewalls are in use, and other characteristics.

After a target has been found, a layer-7 scanner such as Nikto (web vulnerability scanner) can be used to exploit vulnerabilities.

## Malicious Programs

A computer virus is a small program designed to corrupt and/or alter the operation of other legitimate programs. The effect of a virus attack varies from doing so little damage that you are unaware your computer is infected to wiping out the entire contents of a hard drive to rendering your computer inoperable.

### Types of Malicious Programs

The following table describes some of the common malicious programs.

**Table 33** Common Malicious Programs

TYPE	DESCRIPTION
File Infector	This is a small program that embeds itself in a legitimate program. A file infector is able to copy and attach itself to other programs that are executed on an infected computer.
Boot Sector Virus	This type of virus infects the area of a hard drive that a computer reads and executes during startup. The virus causes computer crashes and to some extent renders the infected computer inoperable.
Macro Virus	Macros are small programs that are created to perform repetitive actions. Macros run automatically when a file to which they are attached is opened. Macro viruses spread more rapidly than other types of viruses as data files are often shared on a network.
Trojan Horse	A Trojan horse is a harmful program that is hidden inside apparently harmless programs or data.
Worm	A worm is a program that is designed to copy itself from one computer to another on a network. A worm's uncontrolled replication consumes system resources thus slowing or stopping other tasks.
E-mail virus	E-mail viruses are malicious programs that spread through e-mail. These can infect your computer even if you do not read the e-mail messages.



## Example Intrusions

The following are some examples of intrusions.

### SQL Slammer Worm

W32.SQLExp.Worm is a worm that targets the systems running Microsoft SQL Server 2000, as well as Microsoft Desktop Engine (MSDE) 2000. The worm sends 376 bytes to UDP port 1434, the SQL Server Resolution Service Port. The worm has the unintended payload of performing a Denial of Service attack due to the large number of packets it sends. Refer to Microsoft SQL Server 2000 or MSDE 2000 vulnerabilities in *Microsoft Security Bulletin MS02-039* and *Microsoft Security Bulletin MS02-061*.

### Blaster W32.Worm

This is a worm that exploits the DCOM RPC vulnerability (see *Microsoft Security Bulletin MS03-026* and *Microsoft Security Bulletin MS03-039*) using TCP port 135. The worm targets only Windows 2000 and Windows XP machines. While Windows NT and Windows 2003 Server machines are vulnerable (if not properly patched), the worm is not coded to replicate to those systems. This worm attempts to download the msblast.exe file to the %WinDir%\system32 directory and then execute it. W32.Blaster.Worm does not mass-mail to other devices.

### Nimda

Its name (backwards for "admin") refers to an "admin.DLL" file that, when run, continues to propagate the virus. Nimda probes each IP address within a randomly selected range of IP addresses, attempting to exploit weaknesses that, unless already patched, are known to exist in computers with Microsoft's Internet Information Server. A system with an exposed IIS Web server will read a Web page containing an embedded JavaScript that automatically executes, causing the same JavaScript code to propagate to all Web pages on that server. As Microsoft Internet Explorer browsers version 5.01 or earlier visit sites at the infected Web server, they unwittingly download pages with the JavaScript that automatically executes, causing the virus to be sent to other computers on the Internet in a somewhat random fashion. Nimda also can infect users within the Web server's own internal network that have been given a network share (a portion of file space). Finally, one of the things that Nimda has an infected system do is to send an e-mail with a "readme.exe" attachment to the addresses in the local Windows address book. A user who opens or previews this attachment (which is a Web page with the JavaScript) propagates the virus further.

Server administrators should get and apply the cumulative IIS patch that Microsoft has provided for previous viruses and ensure that no one at the server opens e-mail. You should update your Internet Explorer version to IE 5.5 SP2 or later. Scan and cleanse your system with anti-virus software.

## MyDoom

MyDoom W32.Mydoom.A@mm (also known as W32.Novarg.A) is a mass-mailing worm that arrives as an attachment with the file extension bat, cmd, exe, pif, scr, or zip. When a computer is infected, the worm sets up a backdoor into the system by opening TCP ports 3127 through 3198, which can potentially allow an attacker to connect to the computer and use it as a proxy to gain access to its network resources. In addition, the backdoor can download and execute arbitrary files. Systems affected are Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003 and Windows XP. Systems not affected are DOS, Linux, Macintosh, OS/2, UNIX and Windows 3.x.

W32/MyDoom-A is a worm that spreads by email. When the infected attachment is launched, the worm gathers e-mail addresses from address books and from files with the following extensions: WAB, TXT, HTM, SHT, PHP, ASP, DBX, TBB, ADB and PL. W32/MyDoom-A creates a file called Message in the temp folder and runs Notepad to display the contents, which displays random characters. W32/MyDoom-A creates randomly chosen email addresses in the "To:" and "From:" fields as well as a randomly chosen subject line. Attachment filenames body data doc document file message readme test [random collection of characters]. Attached files will have an extension of BAT, CMD, EXE, PIF, SCR or ZIP.



# Appendix B

## Intrusion Protection

### Firewalls and Intrusions

Firewalls are designed to block clearly suspicious traffic and forward other traffic through. Many exploits take advantage of weaknesses in the protocols that are allowed through the firewall, so that once an inside server has been compromised it can be used as a backdoor to launch attacks on other servers.

Firewalls are usually deployed at the network outskirts. However, many attacks (inadvertently) are launched from within an organization. Virtual private networks, laptops, memory sticks, floppy disks and wireless networks all provide access to the internal network without going through the firewall.

### Intrusion Detection and Prevention (IDP)

An Intrusion Detection and Prevention (IDP) system can detect suspicious activity, but do not take action against attacks. IDPs are proactive defense mechanisms designed to detect malicious packets within normal network traffic and take an action (block, drop, log, send an alert) against the offending traffic automatically before it does any damage. An IDS only raises an alert after the malicious payload has been delivered. Worms such as Slammer and Blaster (see the appendices) have such fast proliferation speeds that by the time an alert is generated, the damage is already done and spreading fast.

There are two main categories of IDP; Host IDP and Network IDP.

### Host Intrusions

The goal of host-based intrusions is to infiltrate files on an individual computer or server in with the goal of accessing confidential information or destroying information on a computer.

You must install Host IDP directly on the system being protected. It works closely with the operating system, monitoring and intercepting system calls to the kernel or APIs in order to prevent attacks as well as log them.

Disadvantages of host IDPs are that you have to install them on each device (that you want to protect) in your network and due to the necessarily tight integration with the host operating system, future operating system upgrades could cause problems.

## Network Intrusions

Network-based intrusions have the goal of bringing down a network or networks by attacking computer(s), switch(es), router(s) or modem(s). If a LAN switch is compromised for example, then the whole LAN is compromised, resulting in the equivalent of a LAN Denial of Service (DoS) attack. Host-based intrusions may be used to cause network-based intrusions when the goal of the host virus is to propagate attacks on the network, or attack computer/server operating system vulnerabilities with the goal of bringing down the computer/server. Typical “network-based intrusions” are SQL slammer, Blaster, Nimda, MyDoom etc. See the appendices for more details.

A Network IDP has at least two network interfaces, one internal and one external. As packets appear at an interface they are passed to the detection engine, which determines whether they are malicious or not. If a malicious packet is detected, an action is taken. The remaining packets that make up that particular TCP session are also discarded.

## Detection Methods

An IDP system employs a mix of detection methods to identify attacks.

### Pattern Matching

Pattern matching identifies a fixed sequence of bytes in a single packet. In addition to the signature byte sequence, the IDP should also be able to match various combinations of the source and destination IP addresses or ports and the protocol.

This method does not apply well to network streams such as HTTP sessions as it inspects single packets at a time.

### Stateful Pattern Matching

Stateful pattern matching operates based on the established session, rather than on a single packet. It considers arrival order of packets in a TCP stream and handles matching patterns across packets. For example, if an exploit is split across two packets, Stateful pattern matching will reassemble the traffic stream and make the complete string available to the detection engine. This requires large amounts of memory and processing power to track a potentially large number of open sessions for as long as possible.

### Protocol Decode

Protocol decode is also known as Protocol Anomaly Detection or Protocol Validation. The detection engine performs a full protocol analysis, decoding and processing the packet in order to highlight anomalies in packet contents. This is quicker than doing a search of a signature database. It is more flexible in capturing attacks that would be very difficult to catch using pattern-matching techniques, as well as new variations of old attacks, which would require a new signature in the database.

The protocol decode engine first applies rules defined by the appropriate RFCs to look for violations. This can help to certain anomalies such as binary data in an HTTP request, or a suspiciously long piece of data where it should not be (a sign of a possible buffer overflow attempt).

## **Heuristic Analysis**

Heuristic-based signatures use algorithms based often on statistics to judge whether a warning is warranted. An example of this type of signature is one that would be used to detect a port sweep. This signature might look for the presence of a threshold number of unique ports being probed on a particular device. Signatures of this type may react differently on different networks, and must be tuned correctly.

## **Anomaly Analysis**

This detection system identifies “normal” traffic on a network, and then anything considers “non-normal” traffic to be an “intrusion”. Anomaly detection can recognize previously unseen attacks, since it is not reliant on knowing what an attack looks like. However “normal” and “non-normal” may have to be defined for each network, so false positives may appear in the initial deployment. These types of attacks do not have a name.



# Index

## C

Cables, Connecting [4](#)  
 Certifications [3](#)  
 Changes or Modifications [3](#)  
 Charge [5](#)  
 CI Commands [103](#)  
 Circuit [3](#)  
 Class B [3](#)  
 coldStart [46](#)  
 Command Line Interface [102](#)  
 Command Syntax [102](#)  
     Abbreviations [102](#)  
     History (no) [102](#)  
 Commands Summary [103](#)  
 Communications [3](#)  
 Community [47](#)  
 Compliance, FCC [3](#)  
 Components [5](#)  
 Condition [5](#)  
 configuration file [98, 99, 100](#)  
 Connecting Cables [4](#)  
 Consequential Damages [5](#)  
 Contact Information [6](#)  
 Contacting Customer Support [6](#)  
 Copyright [2](#)  
 Correcting Interference [3](#)  
 Corrosive Liquids [4](#)  
 Covers [4](#)  
 Customer Support [6](#)

## D

Damage [4](#)  
 Dampness [4](#)  
 Danger [4](#)  
 Daylight Saving [94](#)  
 Daytime (RFC 867) [94](#)  
 DDoS [19, 111](#)  
 Dealer [3](#)  
 debug mode [91, 105](#)  
 Default Time Servers [92](#)  
 Defective [5](#)  
 Denial of Service [108](#)  
 Denmark, Contact Information [6](#)  
 Direction [67, 75, 78](#)  
 Disclaimer [2](#)  
 Discretion [5](#)

## Numerics

10/100Mbps [36](#)  
 110V AC [4](#)  
 230V AC [4](#)

## A

Abnormal Working Conditions [5](#)  
 AC [4](#)  
 Access control [60](#)  
 Accessories [4](#)  
 Activation Key. [81](#)  
 Acts of God [5](#)  
 Airflow [4](#)  
 ALARM [88](#)  
 Alarm [65, 67, 68, 75](#)  
 AND/OR [67](#)  
 anomaly [52](#)  
 application group [70, 71](#)  
 attack group [70, 71](#)  
 Attributions [78](#)  
 Authority [3](#)  
 auto-negotiation [36](#)

## B

Back Door [19](#)  
 backdoor [57, 59](#)  
 Backup [99](#)  
 Basement [4](#)  
 Bidirectional [67, 75, 78](#)  
 Boot Sector Virus [112](#)  
 Buffer Overflow [108](#)  
 Buffer overflow [19](#)  
 buffer overflow [57](#)  
 Bypass [19, 27, 34](#)



DNS server [30, 31](#)

DoS [19](#)

  Basics [108](#)

  Types [108](#)

duplex [36, 37](#)

Dust [4](#)

## E

e-Donkey [53](#)

Electric Shock [4](#)

Electrocution [4](#)

E-MAIL [85](#)

E-mail virus [112](#)

e-Mule [53](#)

Equal Value [5](#)

Europe [4](#)

Export [75](#)

Exposure [4](#)

## F

Factory Defaults [100](#)

Failure [5](#)

FCC [3](#)

  Compliance [3](#)

  Rules, Part 15 [3](#)

FCC Rules [3](#)

Federal Communications Commission [3](#)

File Infector [112](#)

Finland, Contact Information [6](#)

Firmware Upgrade [20](#)

Firmware Upload [95, 97, 98](#)

Fitness [5](#)

Flash Usage [27](#)

flow control [102](#)

France, Contact Information [6](#)

Functionally Equivalent [5](#)

## G

Germany, Contact Information [6](#)

God, act of [5](#)

## H

Harmful Interference [3](#)

Help Facility [103](#)

Heuristic Analysis [19](#)

High Voltage Points [4](#)

HTTP [108](#)

HTTPS [42, 43, 44](#)

## I

ICMP [37](#)

ICMP echo [110](#)

ICMP Header [79](#)

IDP

  Anomaly Analysis [118](#)

  Detection Methods [117](#)

  Heuristic Analysis [118](#)

  Pattern Matching [117](#)

  Protocol Decode [117](#)

  Stateful Pattern Matching [117](#)

IEEE 802.1Q [31](#)

IGMP Header [79](#)

Incoming [67, 75, 78](#)

Indirect Damages [5](#)

Inline [19, 27, 34, 68](#)

Insurance [5](#)

Interference [3](#)

Interference Correction Measures [3](#)

Interference Statement [3](#)

Internet Control Message Protocol (ICMP) [110](#)

Intrusion Detection & Prevention (IDP) [19](#)

Intrusions

  Firewalls [116](#)

  Host [116](#)

  IDP [116](#)

  Introduction [108](#)

  Network [117](#)

IP Ports [108](#)

IP Spoofing [111](#)

## L

Labor [5](#)

LAND [110](#)

Legal Rights [5](#)

Liability [2](#)

License [2](#)  
 Lightning [4](#)  
 Liquids, Corrosive [4](#)  
 Local Upgrade [96](#)  
 Log Facility [88](#)  
 Login [103](#)  
 LOGS [84](#)

## M

Macro Virus [112](#)  
 Mail Server [86, 89](#)  
 Malicious Programs [112](#)  
 Management Information Base (MIB) [45](#)  
 Matching Depth [80](#)  
 Matching Offset [80](#)  
 Materials [5](#)  
 Merchantability [5](#)  
 misuse [52](#)  
 Modifications [3](#)  
 Monitor [19, 27, 34, 68](#)  
 MyDoom [114, 117](#)  
 mySecurity Zone [52](#)

## N

Navigation Panel [27](#)  
 New [5](#)  
 Nimda [113, 117](#)  
 Nmap [56, 112](#)  
 North America [4](#)  
 North America Contact Information [6](#)  
 Norway, Contact Information [6](#)  
 NTP (RFC 1305) [94](#)  
 NTP Time Servers [92](#)

## O

Opening [4](#)  
 Operating Condition [5](#)  
 OSI (Open System Interconnection) [52](#)  
 OSI (Open System Interconnection) [73](#)  
 Out-dated Warranty [5](#)  
 Outgoing [67, 75, 78](#)

Outlet [3](#)

## P

Packet Content [80](#)  
 Parts [5](#)  
 Password [90](#)  
     Forget [91](#)  
 password [24, 25, 27, 28, 90, 91, 103](#)  
 Patent [2](#)  
 Pattern Matching [19](#)  
 Permission [2](#)  
 Photocopying [2](#)  
 Ping of Death [109](#)  
 Policy Actions [65](#)  
     Types [65](#)  
 Policy Check [28](#)  
 Policy check [38](#)  
 Policy Direction [39](#)  
 Policy ID [67, 68](#)  
 policy ID [52](#)  
 Policy Query [67](#)  
 Policy Search [67](#)  
 Policy Severity [64](#)  
     Levels [64](#)  
 Pool [4](#)  
 POP3 [108](#)  
 Porn [62, 63](#)  
 port scans [18, 19](#)  
 Postage Prepaid. [5](#)  
 Power Adaptor [4](#)  
 Power Cord [4](#)  
 Power Outlet [4](#)  
 Power Supply [4](#)  
 Power Supply, repair [4](#)  
 Pre-defined [28](#)  
     Modify [70](#)  
     Update [72](#)  
 Product Model [6](#)  
 Product Page [3](#)  
 Product Serial Number [6](#)  
 Products [5](#)  
 Proof of Purchase [5](#)  
 Proper Operating Condition [5](#)  
 Protocol Anomaly [19](#)  
 Purchase, Proof of [5](#)  
 Purchaser [5](#)  
 PuTTY [49, 50](#)

**Q**

Qualified Service Personnel [4](#)  
Quick Start Guide [24](#)

**R**

Radio Communications [3](#)  
Radio Frequency Energy [3](#)  
Radio Interference [3](#)  
Radio Reception [3](#)  
Radio Technician [3](#)  
Raw IP packets [112](#)  
Receiving Antenna [3](#)  
Recipient(s) [86, 89](#)  
Registered [2](#)  
Registered Trademark [2](#)  
Registering [81, 82](#)  
Registration [28](#)  
Registration Status [82](#)  
Regular Mail [6](#)  
Related Documentation [16](#)  
Relocate [3](#)  
Re-manufactured [5](#)  
Remote management [42](#)  
    SNMP [44](#)  
    SSH [47](#)  
    WWW [43](#)  
Remote Upgrade [96](#)  
Removing [4](#)  
Reorient [3](#)  
Repair [4, 5](#)  
Repetition [78](#)  
Replace [5](#)  
Replacement [5](#)  
REPORT [84, 85, 88](#)  
Report Schedule [85, 86](#)  
Reproduction [2](#)  
Restart [100, 102, 105](#)  
Restore [5, 99](#)  
Return Material Authorization (RMA) Number [5](#)  
Returned Products [5](#)  
Returns [5](#)  
Rights [2](#)  
Rights, Legal [5](#)  
Risk [4](#)  
Risks [4](#)  
RMA [5](#)

**S**

Safety Warnings [4](#)  
Sasser [68](#)  
Scanning [111](#)  
Secure Client IP Address [44, 47, 49](#)  
Separation Between Equipment and Receiver [3](#)  
Serial Number [6](#)  
Server [94](#)  
Server Access [44, 47, 49](#)  
Service [4, 5](#)  
Service Personnel [4](#)  
Shipping [5](#)  
Shock, Electric [4](#)  
Signature Categories [53](#)  
    Access Control [60](#)  
    Backdoor/Trojan [59](#)  
    Buffer Overflow [57](#)  
    DoS/DDoS [55](#)  
    IM [54](#)  
    Others [63](#)  
    P2P [53](#)  
    Porn [62](#)  
    Scan [56](#)  
    Spam [55](#)  
    Virus/Worm [58](#)  
    Web Attack [61](#)  
Smurf [110, 111](#)  
Smurf Attack [110](#)  
SNMP [30, 31, 42, 44, 45, 46, 47](#)  
    Get [45](#)  
    Manager [45](#)  
    MIBs [46](#)  
    Trap [46](#)  
    Traps [46](#)  
SNMPv2c [44](#)  
Spain, Contact Information [6](#)  
SSH [28, 29](#)  
State [27, 29](#)  
Stateful pattern matching [20](#)  
Stealth [27, 29, 37, 38, 43](#)  
Supply Voltage [4](#)  
Support CD [102](#)  
Support E-mail [6](#)  
Sweden, Contact Information [7](#)  
Swimming Pool [4](#)  
SYN Attack [109](#)  
SYN scanning [56, 112](#)  
SYN-ACK [109](#)  
Synchronize [94](#)  
Syntax Conventions [16](#)  
Syslog [87](#)

syslog [27](#), [28](#), [30](#), [31](#), [32](#)

## T

Tampering [5](#)  
TCP connect() [112](#)  
TCP Header [79](#)  
TCP/IP [108](#)  
TCP\_RST [37](#)  
Teardrop [109](#)  
Telephone [6](#)  
Television Interference [3](#)  
Television Reception [3](#)  
Terminal Emulation [102](#)  
Terminal emulation [102](#)  
Three-Way Handshake [109](#)  
Thunderstorm [4](#)  
Time (RFC 868) [94](#)  
Time and Date [91](#), [93](#), [94](#), [95](#)  
    Manual [93](#)  
Time Protocol [92](#), [94](#)  
Time Zone [93](#), [94](#)  
Traceroute [111](#)  
Trademark [2](#)  
Trademark Owners [2](#)  
Trademarks [2](#)  
Translation [2](#)  
Trojan Horse [19](#), [112](#)  
Trojan horse [59](#)  
TV Technician [3](#)

## U

UDP Header [79](#)  
Undesired Operations [3](#)  
updateidp [72](#), [82](#)  
User-defined [20](#), [28](#), [73](#), [74](#), [77](#), [78](#)  
    Add [76](#)  
username [103](#)

## V

Value [5](#)  
Vendor [4](#)

Ventilation Slots [4](#)  
View Log [84](#), [85](#)  
Viewing Certifications [3](#)  
virus [58](#), [68](#)  
VLAN [27](#), [31](#)  
    ZyWALL [32](#)  
Voltage Supply [4](#)  
Voltage, High [4](#)  
VT100 [102](#)

## W

warmStart [46](#)  
Warnings [4](#)  
Warranty [5](#)  
Warranty Information [6](#)  
Warranty Period [5](#)  
Water [4](#)  
Web attack [61](#)  
Web Configurator [24](#), [25](#)  
web configurator [18](#), [24](#), [25](#), [28](#)  
Web Site [6](#)  
Wet Basement [4](#)  
Workmanship [5](#)  
Worldwide Contact Information [6](#)  
Worm [112](#), [113](#)  
    Blaster [113](#)  
    SQL Slammer [113](#)  
worm [58](#)  
Worms [19](#)  
Written Permission [2](#)

## Z

ZyNOS [2](#)  
ZyXEL Communications Corporation [2](#)  
ZyXEL Home Page [3](#)  
ZyXEL Limited Warranty  
    Note [5](#)  
ZyXEL Network Operating System [2](#)