

# ZyWAN

Application Note –  
Security And System  
Diagnostics



## Definitions

Arcom is the trading name for Arcom Control Systems Inc and Arcom Control Systems Ltd.

## Disclaimer

The information in this manual has been carefully checked and is believed to be accurate. Arcom assumes no responsibility for any infringements of patents or other rights of third parties, which may result from its use.

Arcom assumes no responsibility for any inaccuracies that may be contained in this document. Arcom makes no commitment to update or keep current the information contained in this manual.

Arcom reserves the right to make improvements to this document and /or product at any time and without notice.

## Warranty

This product is supplied with a full 3 year warranty. Product warranty covers failure caused by any manufacturing defects. Arcom will make all reasonable effort to repair the product or replace it with an identical variant. Arcom reserves the right to replace the returned product with an alternative variant or an equivalent fit, form and functional product. Delivery charges will apply to all returned products. Please go to [www.arcom.com/support](http://www.arcom.com/support) for information about Product Return Forms.

## Trademarks

Windows XP, Windows 2000, Internet Explorer, are trademarks of the Microsoft Corporation.

Linux is a registered trademark of Linus Torvalds.

All other trademarks recognized.

## Revision History

<i>Revision</i>	<i>Date</i>	<i>Comments</i>
Issue A	July 25, 2008	First full release of ZyWAN Application Note – Security and System Diagnostics

© 2008 Arcom.

Arcom is a subsidiary of Eurotech Group.

For contact details, see page [38](#).



Arcom operates a company-wide quality management system which has been certified by the British Standards Institution (BSI) as compliant with ISO9001:2000

## Contents

About this manual .....	5
Symbols.....	5
Introduction .....	6
Accessing the ZyWAN .....	7
Serial Connection to COM1 .....	7
SSH Client (PuTTY).....	7
SFTP/SCP Client (WinSCP) .....	9
Linux System Commands and Diagnostics .....	11
Reset to Factory Default Configuration.....	11
ZyWAN Software Update – Alternate Methods .....	12
Standard Update Via Command Line .....	12
General Linux Commands .....	13
Keyboard Shortcuts.....	13
‘cd’ – Change Directory .....	13
‘pwd’ – Print Working Directory .....	13
‘ls’ – List Files .....	14
‘cat’ and ‘more’ – Show File Contents.....	15
‘nano’ – Edit a Text File .....	15
‘find’ – Find a File .....	15
Move, Copy, Rename, Delete .....	16
Command Line Reboot .....	16
Diagnostic Commands .....	17
‘uptime’ – Time Since Last Reboot.....	17
‘free’ and ‘df’ – Amount of RAM and Flash Memory.....	17
‘ps’ – Process Status .....	17
‘ifconfig’ – Interface Status .....	18
iptables – Firewall .....	18
‘route’ – Checking route table .....	19
Checking DNS settings .....	19
Checking network configuration.....	19
Checking WiFi settings.....	19
Collect Diagnostic Files from ZyWAN .....	19
Basic Network Security .....	22
Security features .....	22
Authentication .....	23
Encryption .....	23
Accounts and Passwords.....	24
‘root’ Account.....	24
Changing the ‘root’ Password .....	24
‘arcom’ Account.....	25
Web Configuration Password.....	25
Disabling the Serial Login .....	25
Setting SSH configuration.....	26
Setting sshd Parameters.....	26
Disabling ‘root’ Login.....	26




Public/Private Key Authentication .....	28
Generating Public/Private Key Pair.....	28
Loading Public Key onto ZyWAN .....	29
Convert Key to OpenSSH Format.....	29
Adding Public Key to ZyWAN authorized_keys File .....	30
Test Authentication With New Key .....	30
Regenerating ZyWAN Keys .....	32
Creating new SSL certificate.....	33
Firewall Configuration .....	35
Default Firewall Configuration.....	35
Open Ports .....	36
Port Forwarding .....	36
Network Address Translation (NAT).....	37
Adding Custom Firewall Options (iptables).....	37
Appendix A – Contacting Arcom.....	38

## About this manual

This Application Note provides detailed information on security features and diagnostic information for the ZyWAN Cellular Routing Modem.

### *Symbols*

The following symbols are used in this guide:

Symbol	Explanation
	Information that requires your attention.
	A handy hint that may provide a useful alternative or save time.
	Proceeding with a course of action may damage your equipment or result in loss of data.

## Introduction

The ZyWAN is a cellular routing modem for GSM/GPRS, EvDO/1xRTT CDMA, and iDEN networks. The ZyWAN operates as a fully configurable embedded Linux router enabling firewall, DHCP, DNS and NAT. ZyWAN provides real-time network access to any Ethernet, 802.11 or serial device for mobile and fixed data applications.

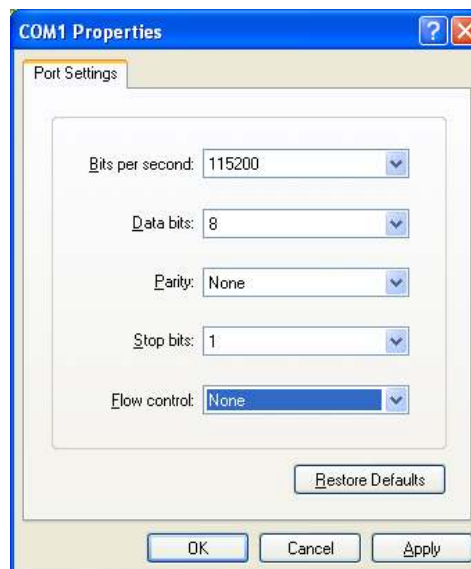
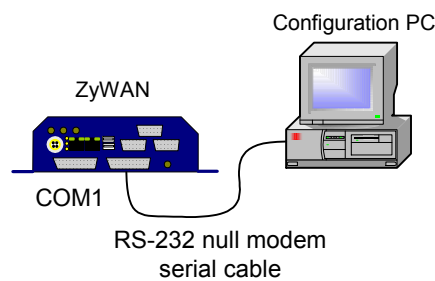
This Application Note describes several advanced configuration options related to network security which are not discussed in the *ZyWAN User Manual*. This document does not discuss the configuration of IPsec or PPTP, which are given in the *ZyWAN Application Note – IPsec Security and PPTP VPN*.

## Accessing the ZyWAN

This section describes several ways to gain access to the ZyWAN for diagnostic and system maintenance purposes.

### Serial Connection to COM1

The COM1 port of the ZyWAN is used for a serial console. Typically, this allows a local administrative ('root') login to the ZyWAN using a null modem serial cable. The ZyWAN *User Manual* describes the settings for Windows HyperTerminal. This connection will be made at 115,200 baud, 8 data bits, 1 stop bit, no parity, and no flow control.



Press the **Enter** key to get a login prompt. The default login is `root` and the default password is `arcom` (case-sensitive).

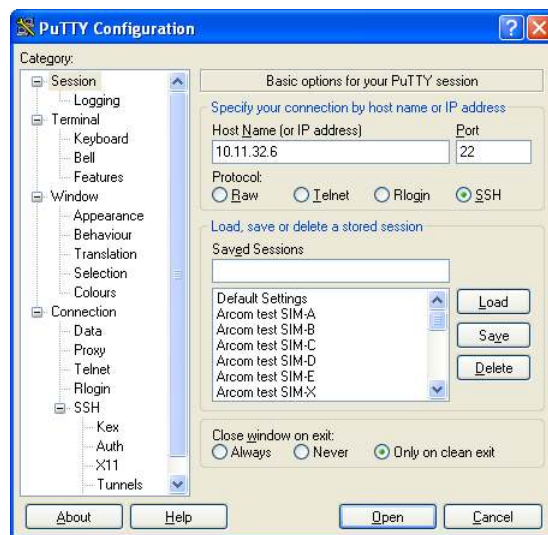
### SSH Client (PuTTY)

The ZyWAN allows remote console logins using Secure Shell (SSH). Unencrypted Telnet is not an option. This requires an SSH client to establish the connection with the ZyWAN.

From a Linux system, the 'ssh' command is available as an SSH client.

From Windows systems, there are a number of third-party applications which can be used. This document will only give details on a free SSH client package, PuTTY. The PuTTY application may be downloaded from <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html> (only the putty.exe is required, although a full Windows installer is available which contains other utilities).

Once the PuTTY application is on the Windows computer, run it and enter the IP address of the ZyWAN. Set the protocol to "SSH" and the port to 22 (unless the port has been changed from its default).



This should usually be enough to connect, but see below for a few additional options. Click the **Open** button to connect.

The first time a connection is made with PuTTY, a security warning is given as PuTTY tries to authenticate with the ZyWAN. Click **Yes** to continue, as long as you are sure that this is the correct ZyWAN device. Then log in with the correct username and password. The default login is `root` and the default password is `arcom` (case-sensitive).

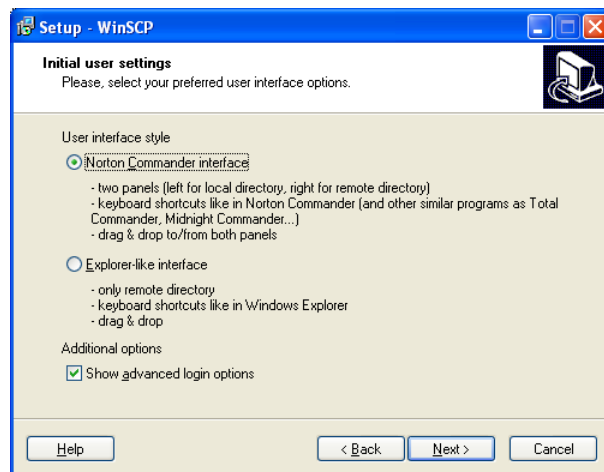




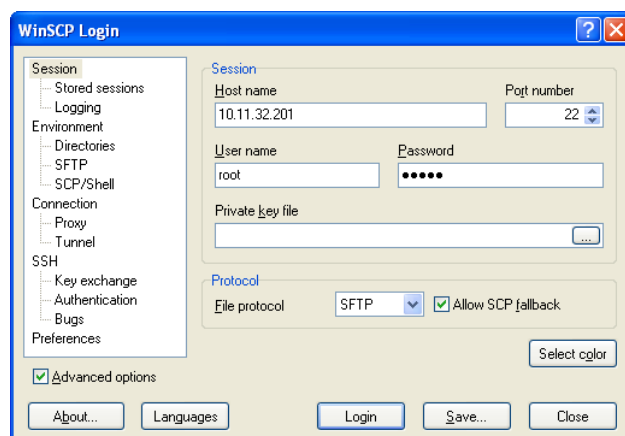
## SFTP/SCP Client (WinSCP)

There may be occasions where it is desired to upload or download files to/from the ZyWAN. Unencrypted FTP is not an option. This requires an SFTP or SCP (Secure FTP or Secure Copy) connection. SFTP and SCP use an encrypted SSH network connection.

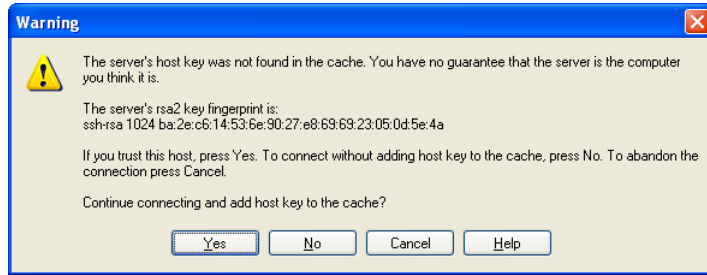
One SFTP/SCP application which is available as a free download is WinSCP. This is available from [www.winscp.net](http://www.winscp.net). Download and install the latest version of WinSCP from this site. One option presented during installation is the user interface style. Either style can be used, but the Norton Commander interface allows display of both the local and remote directories, which is a little more convenient.



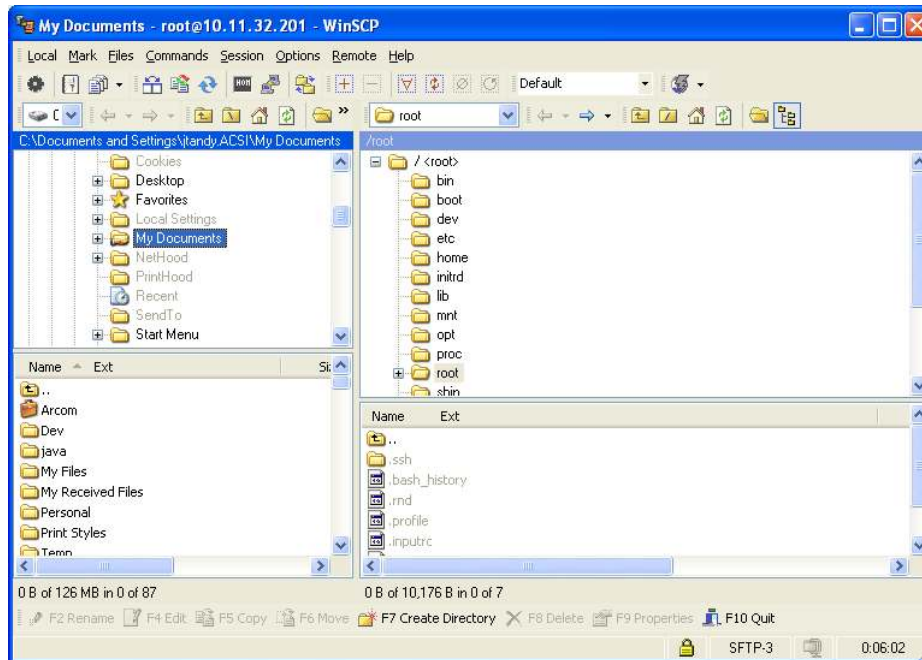
After installing, run WinSCP and enter the IP address to connect to. The username and password can also be entered at this time. Individual session configurations may be saved, if repeated connections need to be made to the same address.



Click **Login** to connect. The first time a connection is made with WinSCP, a security warning is given as WinSCP tries to authenticate with the ZyWAN. Click **Yes** to continue, as long as you are sure that this is the correct ZyWAN device.



The left panes shows the local directories and files, and the right panes show the directories and files on the ZyWAN. Files can be dragged and dropped between the panes, if files need to be uploaded to the device or downloaded from it.



# Linux System Commands and Diagnostics

The ZyWAN uses an embedded Linux operating system. This provides many common system commands from a command line, which can be used in diagnosing a system or performing other functions. This section describes some of the basic system commands. This is provided for user reference, but is not a fully description of all available commands.

## Reset to Factory Default Configuration

The system configuration of the ZyWAN may be reset to a near-factory default condition by using either a serial or SSH (e.g. PuTTY) connection. See Accessing the ZyWAN on page 7. This procedure resets all of the property files **except** for the properties on the *Cellular* page (network provider for IDEN or GPRS).



NOTE: This procedure will cause any existing configuration to be lost. To backup an existing configuration, the `.properties` files in `/var/www/props` may be copied to a different location first.

---

Execute the following command to reset the configuration:

```
cp /var/www/props/default/* /var/www/props
```

This will copy the default properties files, install the configuration, and cause the ZyWAN to reboot automatically.

## ZyWAN Software Update – Alternate Methods

The ZyWAN User Manual describes the normal method of updating the ZyWAN software using the “Update” tab on the Web configuration page. In some cases, it may be necessary to use an alternate method of loading software updates. A few of these alternate methods are described here.

### **Standard Update Via Command Line**

This method will download any available update files from a server and install the updates in the ZyWAN.

```
touch /tmp/update.log
```

```
tail -f /tmp/update.log &
```

```
/var/www/cgi-bin/update.sh
```

**or**     /var/www/cgi-bin/update.sh ***http://files.arcom.com/Zywan/updates***

where “*http://files.arcom.com/Zywan/updates*” is the address of a Web server where all the ZyWAN software updates are stored. The Web server must support file download using HTTP protocol. If this server is set up on a customer machine, the required files will need to be obtained from Eurotech.

The server location must contain the latest versions of the files:

```
version_multi.txt
Zywan-update-1_x.star     (where files named 1_5 and higher would be
                           required to update a version 1.4 ZyWAN)
```

If the server only supports FTP download, not HTTP, the following commandline can be used instead:

```
/var/www/cgi-bin/update.sh --ftp-user=username --ftp-password=password
ftp://ip_address/somepath
```

where “*ftp://ip\_address/somepath*” is the address of an FTP server, using ***username*** and ***password*** to log in.

## General Linux Commands

This section lists several common commands for working in the command prompt.

The Linux command prompt consists of several parts. First is the user name of the account currently logged in (such as “root”), followed by the ZyWAN system name (such as “zeus”). After this is the current directory name, followed by the # prompt (such as “tmp#”). Commands are entered after the # sign.

```
root@zeus tmp#
```

### Keyboard Shortcuts

A few keyboard shortcuts may help when entering commands at the Linux command prompt.

<b>Up/down arrow</b>	Browse forward and backward through previous commands entered at the command prompt.
<b>Backspace</b>	Delete characters to the left of the cursor.
<b>Left/right arrow</b>	Moves left and right through the current command pending at the command prompt.
<b>Tab</b>	Used to complete file and directory names, when possible. For instance, after typing <code>cd /o</code> followed by the <b>Tab</b> key, the path will be completed automatically ( <code>cd /opt/</code> ). Type a ‘w’ and press the <b>Tab</b> key, and it will fill out a further pathname ( <code>cd /opt/wsdd5.0/</code> ). Further file or directory names can be entered similarly. Pressing the <b>Tab</b> key twice will give a list of matching files, if more than one exist with the same starting characters.
<b>Ctrl-C</b>	Stop a current operation that has been issued from the command line, or to cancel a partially entered command without executing it.

### ‘cd’ – Change Directory

The ‘cd’ command allows changing to a different Linux directory. The slash / character is used between directory names, as opposed to the backslash \ character used in the Windows file system.

```
root@zeus root# cd /etc/init.d
root@zeus init.d#
```

### ‘pwd’ – Print Working Directory

The ‘pwd’ command prints the current Linux directory.

```
root@zeus root# pwd
```

```

/root

root@zeus root# cd /

root@zeus /# pwd

/

```

### 'ls' – List Files

From the Linux command line, the 'ls' command lists files.

```

root@zeus root# ls

bin          etc          lib          proc          stunnel.pid  usr
boot         home         mnt         root          sys          var
dev          initrd      opt         sbin         tmp          zyram

```

Using the 'ls -l' command gives much more information about each file or directory. The "d" at the beginning of a row specifies a directory. The lines containing "->" are a link to another file or directory.

```

root@zeus /# ls -l

drwxr-xr-x  2 root  root    0 Oct 10 21:02 bin
drwxr-xr-x  2 root  root    0 Mar  7 18:36 boot
drwxr-xr-x  9 root  root    0 Mar  7 18:37 dev
drwxr-xr-x 37 root  root    0 Nov 30 1999 etc
drwxr-xr-x  3 root  root    0 Nov  1 2006 home
drwxr-xr-x  2 root  root    0 Nov  1 2006 initrd
drwxr-xr-x  4 root  root    0 Mar  7 18:37 lib
drwxr-xr-x  2 root  root    0 Nov  1 2006 mnt
drwxr-xr-x  3 root  root    0 May 21 2007 opt
dr-xr-xr-x 45 root  root    0 Jan  1 1970 proc
drwx----- 3 root  root    0 Mar 17 22:32 root
drwxr-xr-x  2 root  root    0 Mar  7 18:37 sbin

```

```

-rw-r--r--    1 root    root          6 Mar 11 23:41 stunnel.pid
drwxr-xr-x   11 root    root          0 Jan  1  1970 sys
lrwxrwxrwx    1 root    root          7 May 15  2007 tmp -> var/tmp
drwxr-xr-x    8 root    root          0 Jul 24  2006 usr
drwxr-xr-x   10 root    root          0 Mar  7 18:37 var
lrwxrwxrwx    1 root    root         10 Mar  7 18:37 zyram ->
/var/zyram

```

### 'cat' and 'more' – Show File Contents

The 'cat' command will dump the contents of a file. The 'more' command will do the same, but pause after each page full of information. Pressing the spacebar will show another page, the **Enter** key will show one additional line at a time, and **Ctrl-C** will return to a command prompt.

```
root@zeus root# more /var/log/messages
```

### 'nano' – Edit a Text File

If the contents of a text file need to be edited, there are two file editors available: 'nano' and 'vi'. Nano is generally easier to use, but those familiar with Unix/Linux may prefer 'vi' (commands for working in 'vi' are available on the Internet). To edit a file, enter the command such as:

```
root@zeus root# nano -w /tmp/test
```

If the file doesn't exist, it will be created. Several control keys are available, including:

<b>Ctrl-X</b>	Exit from 'nano' (prompt to save changes if any were made).
<b>Ctrl-V</b>	Page down through the file.
<b>Ctrl-Y</b>	Page up through the file.
<b>Ctrl-K</b>	Cut a line
<b>Ctrl-U</b>	Paste a line previously cut.
<b>Ctrl-W</b>	"Where is" – find some text in the file.
<b>Ctrl-G</b>	Get help (list all commands).

### 'find' – Find a File

From the Linux command line, the 'find' command can be used to find a file or files in the Linux system. The format is "find *path* -name *filename*". The listed *filename* will be searched for (wildcards are allowed), beginning at *path* (use / to search the entire filesystem) and through each of its sub-directories.

```
root@zeus root# find / -name equinox.log
```

```
/var/tmp/equinox.log
```

### **Move, Copy, Rename, Delete**

Files can be moved with the 'mv' command (or renamed by moving to same directory), copied with the 'cp' command, and deleted (removed) with the 'rm' command. Add a '-r' flag to the 'rm' command to delete directories, whether empty or not.

```
root@zeus root# cp /zyram/etc/resolv-eth1.conf /tmp
```

```
root@zeus root# mv /tmp/resolv-eth1.conf /tmp/test.conf
```

```
root@zeus root# rm /tmp/test.conf
```

### **Command Line Reboot**

The ZyWAN may be rebooted from the command prompt.

```
root@zeus root# reboot
```



## Diagnostic Commands

Following are some basic Linux commands which can be used to perform some diagnostic functions.

### 'uptime' – Time Since Last Reboot

The 'uptime' command gives the amount of time the system has been up since the last reboot.

```
root@zeus root# uptime
09:49:44 up 10 days, 10:39, load average: 0.00, 0.00, 0.00
```

### 'free' and 'df' – Amount of RAM and Flash Memory

The 'free' command gives the amount of free RAM, and the 'df' command lists the number of 1 Kb blocks of Flash memory used and free.

```
root@zeus root# free
```

	total	used	free	shared	buffers
Mem:	127608	31548	96060	0	0
Swap:	0	0	0		
Total:	127608	31548	96060		

```
root@zeus root# df
```

Filesystem	1k-blocks	Used	Available	Use%	Mounted on
/dev/mtdblock1	32384	21360	11024	66%	/

### 'ps' – Process Status

The list of currently running processes is displayed with the 'ps' command.

```
root@zeus root# ps
```

PID	Uid	VmSize	Stat	Command
3263	root	1192	S	/bin/sh /opt/wsdd5.0/equinox/start_equinox.sh
3264	root	1212	S	/bin/sh /usr/local/bin/process.sh
3265	root	12156	S	j9 -Xint -Dorg.eclipse.soda.sat.core.util.logLevel=IN
3275	root	12156	S	j9 -Xint -Dorg.eclipse.soda.sat.core.util.logLevel=IN
3276	root	12156	S	j9 -Xint -Dorg.eclipse.soda.sat.core.util.logLevel=IN
12253	root	624	R	ps

**'ifconfig' – Interface Status**

The 'ifconfig' command is used to list information about the network interfaces, including the current IP addresses. This is useful for instance on cellular and WiFi, and networks using DHCP, to determine the current network address. The information about a specific network can be obtained by adding the specific interface name; for instance, 'ifconfig ppp0' gives the current status of the cellular link.

```
root@zeus root# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:80:66:04:49:22
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Interrupt:46 Base address:0xa000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1448 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1448 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:439282 (428.9 KiB)  TX bytes:439282 (428.9 KiB)

ppp0      Link encap:Point-Point Protocol
          inet addr:10.23.6.2  P-t-P:10.23.6.1  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1452  Metric:1
          RX packets:16599 errors:1 dropped:0 overruns:0 frame:0
          TX packets:16650 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:3
          RX bytes:571859 (558.4 KiB)  TX bytes:1408969 (1.3 MiB)
```

**iptables – Firewall**

The firewall configuration can be viewed with the following commands. The firewall is set automatically based on the configuration in the *Networking* Web page.

```
root@zeus root# iptables -L -n -v
```

```
root@zeus root# iptables -L -n -v -t nat
```

### **'route' – Checking route table**

The 'route -n' command lists the current routing table.

```
root@zeus root# route -n
```

### **Checking DNS settings**

The current DNS server addresses, which will be contacted to locate a named network server, are given by the following command.

```
root@zeus root# more /etc/resolv.conf
```

```
nameserver 170.206.225.21
```

```
nameserver 170.206.225.22
```

### **Checking network configuration**

The network configuration file can be viewed with the following command. This file is updated automatically based on the configuration of the system via the *Ethernet* and *WiFi* Web configuration pages.

```
root@zeus root# more /etc/network/interfaces
```

### **Checking WiFi settings**

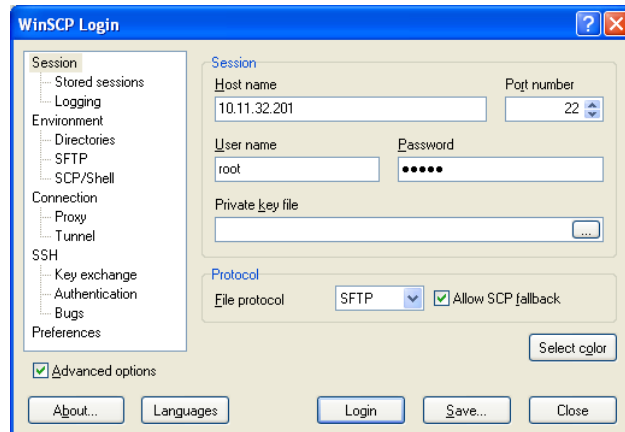
The settings and some diagnostics on the WiFi connection can be obtained with:

```
root@zeus root# iwconfig
```

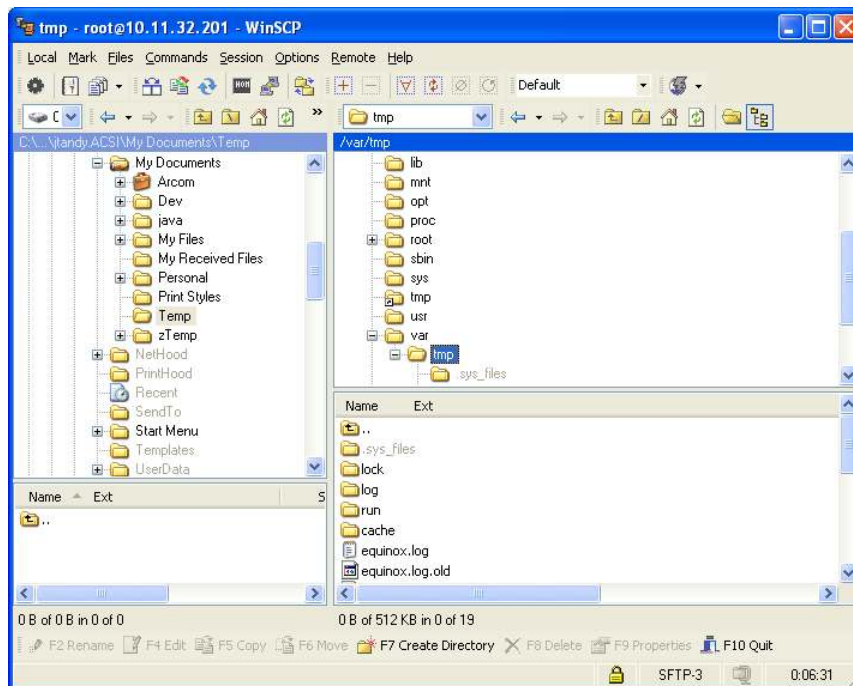
### **Collect Diagnostic Files from ZyWAN**

These are instructions to get log files from a ZyWAN for debugging information.

1. Install WinSCP (see section [SFTP/SCP Client \(WinSCP\)](#), page 9)
2. Open WinSCP and establish a connection with the ZyWAN.



3. Now you should see a screen that look like this



The right hand pane is the ZyWAN filesystem. The lefthand pane is the PC (if using the Norton Commander view).

4. These are the files that need to be copied from the ZyWAN to the PC

- /var/log/messages
- /var/tmp/equinox.log
- /var/tmp/equinox.crash and /var/tmp/equinox.old (if present)

- Any other files requested by Arcom, not listed here.
  - All of the files in /var/www/props/. These include the following:  
master.properties  
reboot.properties  
tab-x.properties
5. Once on the PC, zip these files up and send to Arcom for diagnostics.

# Basic Network Security

This section gives an overview of the ZyWAN security features and some specific information for network administrators to be able to customize the security settings of the ZyWAN.

## Security features

In today's world, network security is a large and growing problem. The ZyWAN addresses these security concerns by utilizing OpenSSH, an open-source implementation of Secure Shell (SSH).

SSH is a powerful software-based approach to complete network security. SSH makes network connections between computers, giving strong assurance that the applications on both ends of the connection are genuine. It also ensures that any data passing over these connections arrives unmodified and unread by any third party.

Secure remote access technologies must satisfy the following three core requirements:

- **Authentication:** The identity and credentials of both parties must be reliably determined, so that a foreign computer may not masquerade as the other party.
- **Encryption:** Data must be confidential as it passes over the network, so only the intended recipient can read it.
- **Integrity:** No third party should be allowed to modify the data in transit without detection.

SSH provides protection from security threats such as eavesdropping, name server and IP spoofing, connection hijacking, man-in-the-middle attacks, and insertion attacks, along with the following standard features:

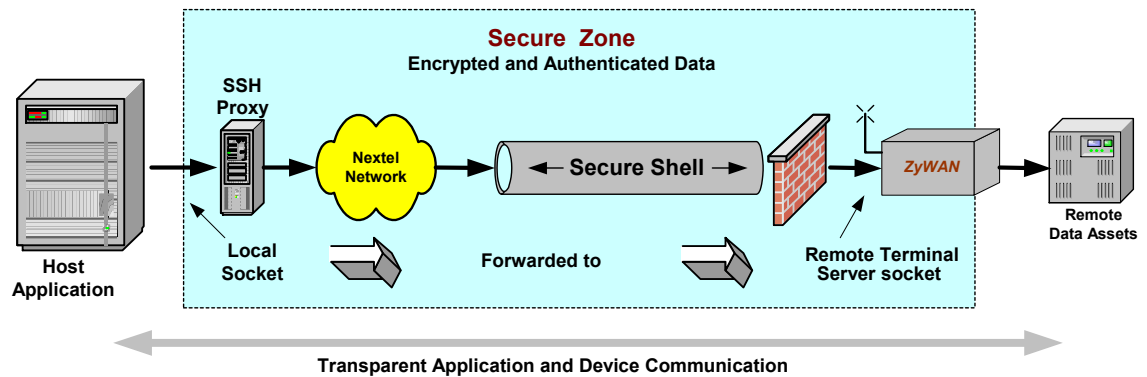
- Secure Remote Login.
- Secure File Transfer.
- Secure Command Execution.
- Authentication Key Management.
- Access Control.
- Port Forwarding.
- Native Data Compression.
- Transaction Logging.

SSH operates as a communication tunnel, allowing applications to interact securely and transparently. A proxy server or proxy application on the host machine allows non-SSH applications to make a secure connection.

Existing unsecure applications do not need to be modified to take advantage of the security features, as security is handled in the proxy. This allows the security model to

be managed separately or changed later, without having to modify all the data applications to fit new network security requirements.

This is illustrated in the following diagram:



### Authentication

SSH offers the following authentication management techniques:

- Simple Password.
- Complex Passphrase clear text.
- Complex Passphrase encrypted.
- Public/Private key pair authentication with 512/1024/2048 bit encryption.
- Kerberos.
- Rhosts.
- RhostsRSA.
- TIS.

### Encryption

SSH offers the following cipher algorithms for data encryption:

- ARC-FOUR.
- Blowfish.
- DES.
- 3DES.
- aes-128.
- aes-192.
- IDEA.

## Accounts and Passwords

The ZyWAN uses an embedded Linux operating system, which uses Secure Shell (SSH) and Secure Socket Layer (SSL) for security and provides multiple user accounts and passwords. This section describes the 'root' login, Web configuration page password, the SSL certificate for the HTTPS Web configuration page, and some details on setting advanced options in SSH.

### 'root' Account

The administrative account on the system is the 'root' login. The default login is `root` and the default password is `arcom` (case-sensitive). This login is available by default on the console port (COM1) or through an SSH network login. Access to the 'root' account is required for most system commands.




---

It is highly recommended to change the 'root' account password from the default before commissioning.

---

### Changing the 'root' Password

The 'root' login is the main administrative account on the ZyWAN, and most systems will come with the factory default password configured. This should be changed before commissioning. To do this, follow these steps: .

- 1 Log in as 'root'.
- 2 Issue the `'passwd'` command to change the 'root' password. The prompts shown and commands you enter to do this are as follows:

```
root@ZYWAN root# passwd
Changing password for root
Enter the new password (minimum of 5, maximum of 8 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password: [hidden]
Re-enter new password: [hidden]
Password changed.
root@ZYWAN root#
```




---

For better security, choose a longer password and use a combination of upper and lowercase letters, numbers and symbols.

The password is case-sensitive.

---



### 'arcom' Account

There is another account which comes by default on the ZyWAN, which has limited (not administrative) rights. The default login is `arcom` and the default password is `arcom` (case-sensitive).

### Web Configuration Password

The normal method of changing the Web configuration password is through the ZyWAN *Security* page. However, it is possible to change the Web password through the command line. The commands are given below:

```
/var/www/cgi-bin/encryptPasswd currentUsername currentPassword
newUsername newPassword
```

```
echo $?
```

The output of the `'echo $?'` command should be `'0'`, otherwise there was an error in changing the password. An error will occur, for instance, if the wrong `currentUsername` or `currentPassword` were entered.

### Disabling the Serial Login

The ZyWAN comes default with a serial console port on COM1. This is useful for diagnostics or determining the IP address when network connections are not working properly. However, in some cases it may be required to prevent access to this serial port for security reasons. This can be done by modifying the file `/etc/inittab`. Toward the end of the file is a line that will look like this:

```
T0:23:respawn:/sbin/getty -L ttyS0 115200 vt100
```

which should be changed to:

```
#T0:23:respawn:/sbin/getty -L ttyS0 115200 vt100
```

Add a hash sign (`#`) at the beginning of this line to comment it out, save changes, then reboot. Access to the serial console will be disabled. See ['nano' – Edit a Text File](#), page [15](#), for information on editing files.



Warning: If network access is lost to the device through improper configuration, it may be very difficult to gain access again if the serial login has been disabled. It is not recommended to disable the serial console port unless absolutely required for security reasons.

---



Another way to secure the console port without disabling it completely may be to prevent direct login to the 'root' account. See [Disabling 'root' Login](#) on page [26](#) for details.

## Setting SSH configuration

The ZyWAN uses Secure Shell (SSH) for secure access to the system. There are several settings which can be changed from default to make the ZyWAN more secure. Only a few of these options will be discussed here. Other standard SSH options may be possible, for which information is publicly available.

### Setting sshd Parameters

The file `/etc/ssh/sshd_config` contains the configuration for incoming SSH connections. The configuration can be changed by editing the parameters in this file.

The parameters are listed in this file, with the default settings containing a hash sign (#) at the beginning of the line. If one of the default settings is to be changed, remove the hash sign and change the setting as needed. Some useful changes are listed below:

Default Setting	Possible change	Explanation
<code>#Port 22</code>	<code>Port 2222</code>	Change the default SSH port of 22 to a non-standard port.
<code>#Protocol 2,1</code>	<code>Protocol 2</code>	Require SSH level 2 (more secure), don't allow level 1.
<code>#PermitRootLogin yes</code>	<code>PermitRootLogin no</code>	Disable 'root' login, require 'su' to the admin account.
<code>#PasswordAuthentication yes</code>	<code>PasswordAuthentication no</code>	Disable password login, require keys or other authentication.

See [Disabling 'root' Login](#), page [26](#), for more information on disabling the 'root' account. See [Public/Private Key Authentication](#), page [28](#), for more information on key authentication.

### Disabling 'root' Login

On the ZyWAN, the 'root' administrative account name cannot be changed. For additional security, it may be desired to disable direct login to the 'root' account.

Instead, users can be required to login using a different account name and password, and only access the 'root' account with the superuser (su) command, requiring a second password.

To set this up, a custom account can be created with the `adduser` command, and give the new account a secure password. Then change the `sshd` configuration file to prevent 'root' login. See [Setting sshd Parameters](#), page 26, for changing this configuration file. Then restart the `sshd` service with the command:

```
/etc/init.d/sshd reload
```



Make sure to keep open a 'root' login over SSH or serial console session, to prevent losing access if something was done wrong. This change can be reversed by changing the `sshd.conf` back to original and reloading `sshd`.

---

Open a new SSH session to the ZyWAN, and attempt to login using the 'root' account password. It should fail. Now try to login using the new user account. It should succeed. Change to the 'root' account by typing the command 'su' and entering the 'root' password.

```
login as: test
test@10.11.32.201's password: [Enter the 'test' password]
$ su
Password: [Enter the 'root' password]
$ [Now you are logged in as 'root']
$ PATH=$PATH:/usr/sbin:/sbin
```

The last line adds some directories to the path which may not be set correctly for 'root', to allow access to all the programs.

## Public/Private Key Authentication

Public key authentication provides a secure and convenient way to connect automatically from host systems to the ZyWAN without requiring username/password logins. As shipped from the factory, the ZyWAN supports authorized key authentication in addition to password authentication, but does not include any public keys of other systems. In order to allow access into the ZyWAN, the public key of other machine(s) must be added to its `authorized_keys` file.

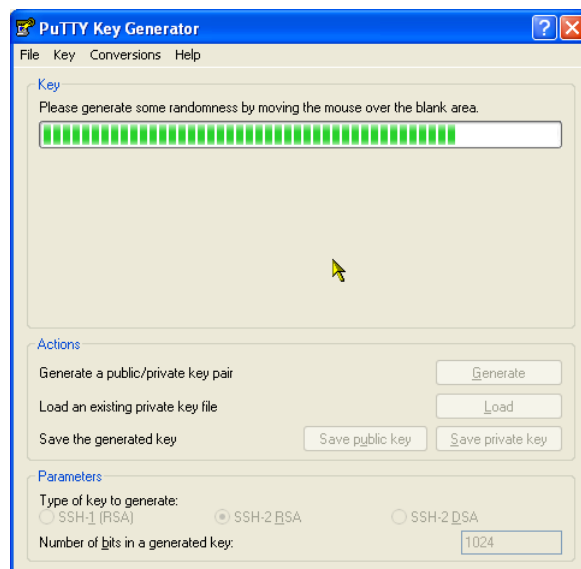
### Generating Public/Private Key Pair

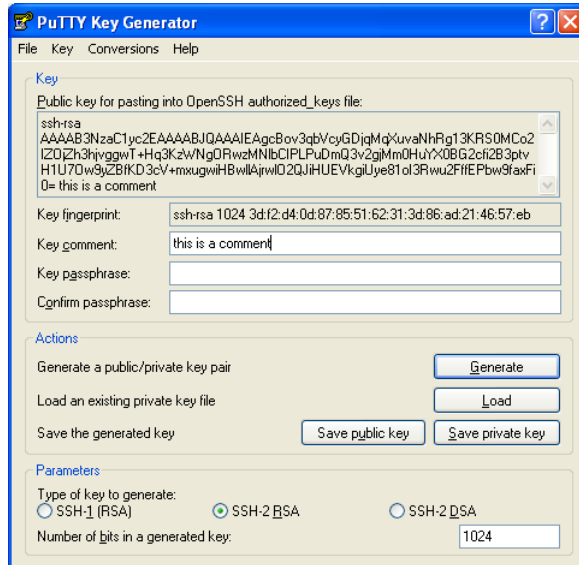
The process of generating a public and private key for a given client machine may vary based on an organization's administrative policies. Please contact your network administrator for more information.

Essentially, a public and a private key are generated for a given machine based on various levels and methods of encryption required. The private key (or secret key) remains on the client machine and is used for encrypting and decrypting messages with another computer. The server being logged into must have a copy of the client's public key in order to authenticate it.

The details of key generation may vary by customer. If no other facility exists for creating the keys, PuTTY or WinSCP supply a "PuTTYgen" application for this purpose.

Run the PuTTYgen application. Click the **Generate** button, then move the mouse randomly in the "Key" area. An optional key comment and passphrase can be entered.





Save the public and private key files to the local machine. The following names will be used in this example:

***rsa2-key.ppk*** - Private key for client machine (***do not transfer this to the ZyWAN*** – this should be stored in a safe location on client). This is the client machine’s identification when logging into the ZyWAN.

***rsa2-key.pub*** - Public key associated with client machine’s private key. This is the file which will reside on the ZyWAN to authenticate the client when it logs in.

Below is described the process of incorporating the client’s public key into the ZyWAN.

### **Loading Public Key onto ZyWAN**

The public key must be loaded into the ZyWAN. This can be done by using SFTP or SCP, using the WinSCP application (see [SFTP/SCP Client \(WinSCP\)](#), page 9). For this example, the file ***rsa2-key.pub*** will be transferred, and should be stored in the temporary folder `/tmp`.

### **Convert Key to OpenSSH Format**

The public key is then converted to the OpenSSH format used by the ZyWAN. This requires a ‘root’ level login to the ZyWAN. The command below will give the converted file a different name, ***sshkeytemp.pub***.

```
ssh-keygen -i -f /tmp/rsa2-key.pub >> /tmp/sshkeytemp.pub
```

This command creates a new file, `/tmp/sshkeytemp.pub`, which contains the client’s public key information in the correct format used by the ZyWAN. This file can be displayed, if desired, using the ‘more’ command. The example shown below is a 1024-bit RSA key, and there could be a plain text comment after the final ‘=’ sign. There should be no carriage return or line feed characters in the middle of this file.

```
more sshkeytemp.pub
```

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAIEAgcBov3qbVcyGDjqMqXuvaNhRg13KRS0M
Co2IZOjZh3hjvvggwT+Hq3KzWNgORwzMN1bCIPLPuDmQ3v2gjMm0HuYX0BG2cfi2B3ptv
H1U7Ow9yZBfKD3cV+mxugwiHBwllAjrw1O2QJiHUEVkgiUye81oI3Rwu2FffEPbw9fax
Fi0=
```

### Adding Public Key to ZyWAN `authorized_keys` File

Now that the public key is ready, it must be added to the file `/root/.ssh/authorized_keys` on the ZyWAN. The `authorized_keys` file may contain many different keys of many different client machines which are allowed to login to this server. Adding the public key requires a 'root' level SSH session.

As shipped from the factory, there is typically no `authorized_keys` file in the ZyWAN. If a customer has previously created this file, it is a good idea to back up the existing `authorized_keys` file before proceeding, to guard against error. It is also possible to use the 'more' command to list the contents of the existing `authorized_keys` file before and after adding the new key, to make sure the contents look correct.

```
ls /root/.ssh
```

```
authorized_keys
```

*If "authorized\_keys" file exists, as shown above, back it up before proceeding:*

```
cp /root/.ssh/authorized_keys /tmp
```

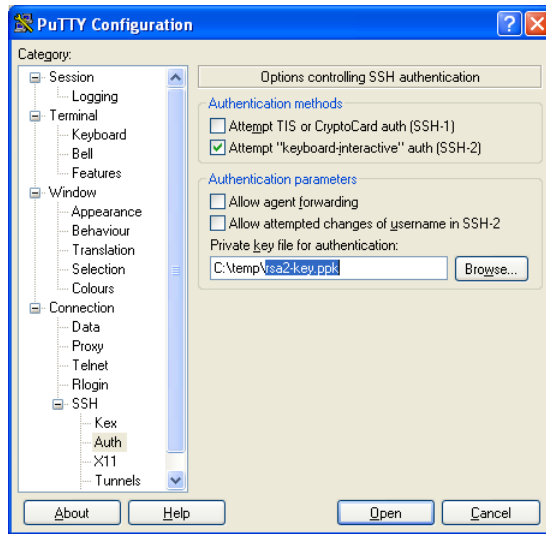
Now, add the new public key to the `authorized_keys` file, using the following command. This command will work whether or not the file already exists.

```
cat /tmp/sshkeytemp.pub >> /root/.ssh/authorized_keys
```

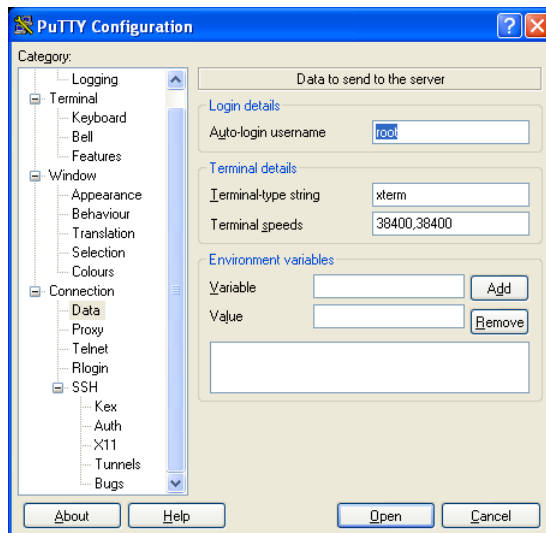
The new public key will be added to the end of the existing file, or a new file will be created. After verifying that the file is correct and the client can authenticate successfully, the temporary copy can be removed. Or, it will be removed automatically from `/tmp` up rebooting.

### Test Authentication With New Key

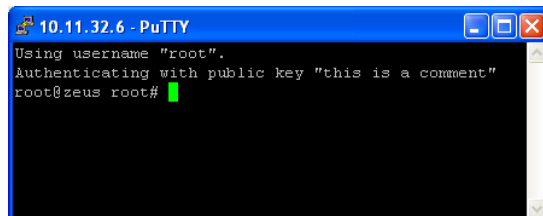
To verify that the public/private key can be used to authenticate to the ZyWAN, run the PuTTY application. Enter the IP address of the ZyWAN and SSH for the protocol. Then choose the "Connection | SSH | Auth" option, and enter or browse to the location where the private key is stored on the local client machine, such as:



Note, the 'root' username may also be entered under "Connection | Data" so that it doesn't have to be entered manually.



This PuTTY session may be saved under "Session" before proceeding, as usual. Upon connecting, PuTTY will use its local private key to validate its identify against the public key that resides on the ZyWAN. If this login is successful, without requiring a 'root' password, then the key authentication has been set up correctly.



## Regenerating ZyWAN Keys

The previous section described the use of public/private keys to allow a client machine to authenticate to the ZyWAN. The ZyWAN may also be set up to authenticate to another machine or a different ZyWAN using SSH keys. Whenever the ZyWAN boots, it automatically generates its own unique sets of public/private key pairs.

The keys that are created on the ZyWAN are its identity for logging onto other systems, if key authentication is used. These consist of a public/private pairs of SSH1 RSA, SSH2 RSA, and SSH2 DSA keys. After the initial boot, the keys are not automatically created unless they are deleted first.



Note that deleting the keys may have an impact on the ability to log into some systems, if the existing set(s) of keys have been registered on the remote server. Consult your network administrator before deleting these keys.

The ZyWAN keys are located under `/etc/ssh`. They may be removed with the 'rm' command shown below:

```
root@ZyWAN root# ls /etc/ssh

moduli                ssh_host_dsa_key.pub  ssh_host_rsa_key
ssh_config            ssh_host_key          ssh_host_rsa_key.pub
ssh_host_dsa_key      ssh_host_key.pub      sshd_config

root@ZyWAN root# rm /etc/ssh/*key*

root@ZyWAN root# ls /etc/ssh

moduli                ssh_config  sshd_config
```

Upon the next reboot, new keys will be generated. They may also be generated by issuing the following command:

```
/etc/rc2.d/S55sshd start
```

Alternatively, new keys can be generated and placed on the ZyWAN by a network administrator.



## Creating new SSL certificate

The Web configuration page uses an SSL certificate for its HTTPS encryption of Web pages. All ZyWAN's are sent from the factory with the same SSL certificate. This certificate may be regenerated on individual units by following the steps below. Commands are shown in **bold** font, and the required user input is indicated in ***bold Italic*** font. The “<ENTER>” indicates simply pressing the **Enter** key on the keyboard.

```
cd /usr/lib/ssl
misc/CA.sh -newca

CA certificate filename (or enter to create)
    <ENTER>
Enter PEM pass phrase
    arcom
Verifying - Enter PEM pass phrase
    arcom
Country Name (2 letter code) [AU]:
    <ENTER>
State or Province Name (full name) [Some-State]:
    <ENTER>
Locality Name (eg, city) []:
    <ENTER>
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
    <ENTER>
Organizational Unit Name (eg, section) []:
    <ENTER>
Common Name (eg, YOUR name) []:
    zywan
Email Address []:
    <ENTER>
```

```
openssl req -new -days 365 -nodes -out newreq.pem -keyout stunnel.pem

Country Name (2 letter code) [AU]
    <ENTER>
State or Province Name (full name) [Some-State]
    <ENTER>
Locality Name (eg, city) []
    <ENTER>
Organization Name (eg, company) [Internet Widgits Pty Ltd]
    <ENTER>
Organizational Unit Name (eg, section) []
    <ENTER>
Common Name (eg, YOUR name) []
    zywan
Email Address []:
    <ENTER>
A challenge password []
    arcom
An optional company name []
```

```
<ENTER>

misc/CA.sh -sign

Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/cakey.pem: arcom

Check that the request matches the signature
Signature ok
Certificate Details:
[followed by certificate details]

Certificate is to be certified until Mar  7 20:20:41 2009 GMT
(365 days)
Sign the certificate? [y/n]: y

1 out of 1 certificate requests certified, commit? [y/n] y
Write out database with 1 new entries
Data Base Updated
Certificate:
[followed by certificate details]

Signed certificate is in newcert.pem

cat newcert.pem >> stunnel.pem
cp stunnel.pem /etc/stunnel/stunnel.pem
chmod 700 /etc/stunnel/stunnel.pem
/etc/init.d/stunnel force-reload
```

Now the new certificate should be ready for use.

# Firewall Configuration

The ZyWAN firewall is controlled by the Linux 'iptables' program. This provides security, as well as sets up the Open Ports, Port Forwarding, and NAT operations configured through the Web interface. As changes are made to the *Networking* page of the Web configuration, a firewall script (/etc/init.d/firewall) is updated and executed immediately after the changes are saved. These settings are also implemented upon the ZyWAN system startup.

This section will describe the default firewall settings, explain in some detail how the Web configuration changes those settings, and tell how a network administrator may implement custom firewall rules independent of the ZyWAN Web interface. This section will not give a full explanation of Linux 'iptables', as this information is publicly available.

## Default Firewall Configuration

The default firewall configuration script is shown below. This is a script that clears any existing settings and immediately implements the new set of rules. By default, all incoming ports and forwarded traffic are blocked, except those required for ZyWAN operation (default TCP ports 22, 80, and 443). All output traffic (originating from the ZyWAN) and ping traffic are allowed.

The default Web configuration allows UDP ports 67 (DHCP) and 53 (DNS) under "Open Ports", no port forwarding, and a NAT (masquerade) from eth0 to ppp0. At the end of the script, a custom user firewall script is invoked, if present.

```

root@zeus root# more /etc/init.d/firewall
#!/bin/sh

#Clear all Built-in Chains
iptables -F INPUT
iptables -F OUTPUT
iptables -F FORWARD
iptables -t nat -F

#Block all ports for input traffic
iptables -P INPUT DROP

#Accept Output Traffic
iptables -P OUTPUT ACCEPT

#Block Forwarding
iptables -P FORWARD DROP

#Allow all traffic to loop back interface
iptables -A INPUT -i lo -j ACCEPT

#Allow Only incoming connection related to Outgoing connection
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

```

```
#allow inbound ssh, http, and https ports on any interface (22, 80, 443)
iptables -I INPUT -p tcp --dport 22 -j ACCEPT
iptables -I INPUT -p tcp --dport 80 -j ACCEPT
iptables -I INPUT -p tcp --dport 443 -j ACCEPT

#allow inbound ICMP requests
iptables -A INPUT -p icmp --icmp-type 8 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type 0 -m state --state ESTABLISHED,RELATED -j ACCEPT

#custom local service rules
iptables -I INPUT -p udp --dport 67 -j ACCEPT
iptables -I INPUT -p udp --dport 53 -j ACCEPT

#custom port forward service rules

#custom nat service rules
iptables -t nat -A POSTROUTING -o ppp0 -s 192.168.1.0/24 -j MASQUERADE; iptables -A FORWARD
-i eth0 -o ppp0 -j ACCEPT; iptables -A FORWARD -i ppp0 -o eth0 -j ACCEPT

#allow forwarding if any masquerade is defined
echo 1 > /proc/sys/net/ipv4/ip_forward

#source a custom firewall script
source firewall_cust 2> /dev/null
```

## Open Ports

The “Open Ports” section of the *Networking* page on the Web configuration allows specific TCP or UDP port connections to terminate on the ZyWAN. This must include DHCP and DNS (UDP ports 67 and 53), any TCP ports configured on the *Terminal Servers* page, or other ports which may be needed.

A typical ‘iptables’ command based on the “Open Ports” Web configuration is shown below. In this example, the port on the ZyWAN is 3000 (TCP), and the optional source fields are used. Only computers in the range of 192.168.1.1 to 192.168.1.255 may connect, the source TCP connection must be in the range of ports 4000-4010, and the source computer’s MAC address must be AA:BB:CC:DD:EE:FF (this is unrealistically qualified, but is used to illustrate the various parts of the configuration).

```
iptables -I INPUT -p tcp -s 192.168.1.0/24 -m mac --mac-source AA:BB:CC:DD:EE:FF --sport
4000:4010 --dport 3000 -j ACCEPT
```

## Port Forwarding

The “Port Forwarding” section of the *Networking* page allows certain ports to be opened on one interface of the ZyWAN, which may be forwarded to a device on another interface.

A typical ‘iptables’ command based on the “Port Forwarding” Web configuration is shown below. In this example, TCP port 5000 on the ZyWAN (eth0 interface) is forwarded to 192.168.2.40 port 5001 on the eth1 interface, and the optional source fields are used. Only computers in the range of 192.168.1.1 to 192.168.1.255 may

connect, the source TCP connection must be in the range of ports 6000-6010, and the source computer's MAC address must be AA:BB:CC:DD:EE:FF (this is unrealistically qualified, but is used to illustrate the various parts of the configuration).

```
iptables -I INPUT -p tcp -s 192.168.1.0/24 -m mac --mac-source AA:BB:CC:DD:EE:FF --sport 6000:6010 --dport 5000 -j ACCEPT

iptables -t nat -A PREROUTING -i eth0 -p tcp -s 192.168.1.0/24 -m mac --mac-source AA:BB:CC:DD:EE:FF --sport 6000:6010 --dport 5000 -j DNAT --to 192.168.2.40:5001
```

## Network Address Translation (NAT)

Network Address Translation allows a mapping to be made from one interface to the IP address of the interface where network traffic needs to go out. The 'iptables' command based on the default "NAT" Web configuration is shown below. In this example, devices in the range of 192.168.1.1 to 192.168.1.255 on the eth0 interface are allowed to go out the ppp0 (cellular) interface, and communication is forwarded between the two interfaces.

```
iptables -t nat -A POSTROUTING -o ppp0 -s 192.168.1.0/24 -j MASQUERADE; iptables -A FORWARD -i eth0 -o ppp0 -j ACCEPT; iptables -A FORWARD -i ppp0 -o eth0 -j ACCEPT
```

## Adding Custom Firewall Options (iptables)

The standard firewall options should be sufficient for the security of most applications. However, in some cases a network administrator may have specific security requirements that require modifications to the ZyWAN firewall script.

The ZyWAN provides for this by referencing another file containing iptables commands, to be provided by the network administrator. The custom iptables commands must be located in a file ( /etc/init.d/firewall\_cust ) on the ZyWAN system. This is not required to be an executable script, but simply contains the additional iptables commands to be executed. In the most extreme example, the commands in the custom file may clear all the ZyWAN iptables settings and replace them, effectively overriding the Web configuration entirely.

## Appendix A – Contacting Arcom

### Sales Support

Arcom's sales team is always available to assist you in choosing the product that best meets your requirements. Contact your local sales office or hotline.

#### **Sales office US**

Arcom  
7500W 161<sup>st</sup> Street  
Overland Park  
Kansas  
66085  
USA

Tel: 913 549 1000  
Fax: 913 549 1002  
E-mail: [us-sales@arcom.com](mailto:us-sales@arcom.com)

#### **Sales office Europe**

Eurotech Ltd.  
3 Clifton Court  
Cambridge  
CB1 7BN  
United Kingdom

Tel: +44 (0)1223 403410  
Fax: +44 (0)1223 410457  
E-mail: [sales@eurotech-ltd.co.uk](mailto:sales@eurotech-ltd.co.uk)

Full information about all Arcom products is available on our Web site at [www.arcom.com](http://www.arcom.com) and [www.zywan.com](http://www.zywan.com).



While Arcom's sales team can assist you in making your decision, the final choice of boards or systems is solely and wholly the responsibility of the buyer. Arcom's entire liability in respect of the boards or systems is as set out in Arcom's standard terms and conditions of sale. If you intend to write your own low level software, you can start with the source code on the disk supplied. This is example code only to illustrate use on Arcom's products. It has not been commercially tested. No warranty is made in respect of this code and Arcom shall incur no liability whatsoever or howsoever arising from any use made of the code.

### Technical support

Arcom has a team of technical support engineers who can provide assistance if you have any problems with your ZyWAN.

#### **Technical support US**

Tel: 913 549 1010  
Fax: 913 549 1001  
E-mail: [us-support@arcom.com](mailto:us-support@arcom.com)

#### **Technical support Europe**

Tel: +44 (0)1223 412428  
Fax: +44 (0)1223 403409  
E-mail: [support@eurotech-ltd.co.uk](mailto:support@eurotech-ltd.co.uk)