IntraGuard Firewall Installation Guide

Compatible Systems Corporation
4730 Walnut Street
Suite 102
Boulder, Colorado 80301

303-444-9532
800-356-0283
http://www.compatible.com

IntraGuard Firewall Installation Guide,
March 16, 2000

Part number: A00-1696

FCC Notice: This product has been certified to comply with the limits for a Class A computing device, pursuant to Subpart J of Part 15 of FCC Rules. It is designed to provide reasonable protection against radio or television communication interference in a commercial environment. Operation of this equipment in a residential area could cause interference with radio or television communication.

Chapter 1 - Introduction

About the IntraGuard Firewall

Congratulations on your purchase of the IntraGuard Firewall. This stand-alone hardware device delivers hassle-free, high-performance Internet security. The IntraGuard is designed to effectively operate as a "plug and play" system, or it can be easily configured to implement a customized security policy.

The IntraGuard's three 10/100 Ethernet ports allow you to separate your internal/private network from the Internet. You can also create a third "DMZ" segment which provides limited, carefully monitored external access to selected internal resources such as an FTP or Web server.

IntraGuard Firewall Installation Overview

This manual will help you install the IntraGuard Firewall on your Local Area Network.

In short, the installation steps are:

1. **Install** the IntraGuard hardware and connect the 10/100 twisted-pair Ethernet interfaces to Fast Ethernet or Ethernet hubs.
2. **Connect** a management console to the IntraGuard or set up Telnet management.
3. **Turn on** the device and allow the default configuration to provide your network with Internet security, or configure the IntraGuard with your customized security parameters.

If you have any difficulties during the installation or use of the IntraGuard that are not answered by this guide or the Reference Guides which were included with your firewall, please call Compatible Systems Corporation or your reseller. Compatible Systems' phone number is listed on the front of this guide. We will be happy to help you.

The manual is divided into several sections that should provide you with all the information you will need to start using the IntraGuard on your network.

Chapter 2 - Getting Started

This part of the manual describes the contents of the IntraGuard package and outlines the preparation and equipment you will need to install the device.

Chapter 3 - Network Installation

Here you will find step-by-step instructions on how to physically install the firewall and connect it to your local Ethernet(s). Instructions are included for twisted-pair Ethernet environments.

Chapter 4 - CompatiView Software Installation

If you plan to use CompatiView, Compatible Systems' GUI (Graphical User Interface) management software which is included with your firewall, then read this section. Instructions are provided on how to install CompatiView for Windows environments.

Chapter 5 - Command Line Preparation

This part of the manual provides basic instructions on setting up command line management and text-based configuration.

Chapter 6 - Basic Configuration Guide

This section provides a list of parameters that must be entered into a router for proper operation.

Appendices

This part of the manual includes additional information that might be of interest to you such as technical specifications, default settings (including the default factory password) and instructions for downloading current software.

Chapter 2 - Getting Started

A Few Notes

Please Read the Manuals

The manuals included with your IntraGuard Firewall contain very important information about the IntraGuard Firewall and local and wide area networking in general. Please read this manual thoroughly, and refer to the management reference guides as required. It's worth the few minutes it will take.

Also, please fill out the warranty registration card and return it to us today. This will help us keep you informed of updates to the IntraGuard Firewall and future products available from Compatible Systems. You can also register on the web at http://www.compatible.com. If you'd like to be notified via e-mail about new products and receive important news from Compatible Systems, please join our email list on the web.

Warranty and Service

The IntraGuard Firewall is covered by the Compatible Systems Integrated Support Package, which includes a lifetime comprehensive warranty, a twenty-four hour advanced replacement program, unlimited technical support, and software upgrades for the life of the product.

Compatible Systems maintains copies of current software updates on the Internet. For more information on downloading software, see the appendices in this manual.

Getting Help with the IntraGuard Firewall

If you have a question about the IntraGuard Firewall and can't find the answer in one of the manuals included with the product, please visit the technical support section of our Web site (http://www.compatible.com). This site includes extensive technical resources which may answer many of your questions. You can also request technical support by filling out a brief form. Technical support requests received via the Web form will receive expedited treatment. You may also call Compatible Systems Corporation or send support questions via e-mail to *support@compatible.com.* Compatible Systems' phone number is listed on the front of this guide. We will be happy to help you.

What You Will Need To Get Started

Before installing the IntraGuard Firewall, please check the list below to make sure that you have received all of the items supplied with the firewall package.

You should also make sure you have any additional items that are necessary to connect the firewall to your network.

Supplied with the IntraGuard Firewall

Please check your shipping package for the following items:

- IntraGuard unit
- Wall-mount power supply
- One DB-25 male to DB-25 female RS232 console cable
- CD-ROM including:
  - CompatiView software
  - Operating software
  - HTML version of product documentation (which can be viewed with your favorite web browser)
- *CompatiView Management Software Reference Guide*
- *Text-Based Configuration and Command Line Management Reference Guide*
- Warranty Registration card

Needed for Installation

Before connecting the IntraGuard Firewall to your network, you need to make sure that you have the necessary equipment for connecting to a local Ethernet.

Ethernet Connection Requirements

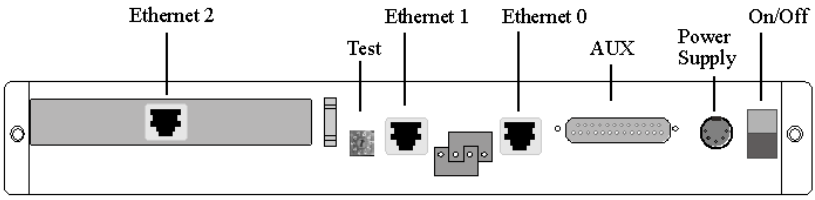
The firewall's Ethernet interfaces directly support full or half duplex 100BaseTx or 10BaseT twisted-pair Ethernet. To connect the firewall's Ethernet interfaces to twisted-pair Ethernet cabling, you will need an unshielded twisted-pair station cable that is connected to a 10BaseT-compatible twisted-pair hub (for a transmit speed of 10 Mbps) or a 100Mbps Fast Ethernet hub (at either transmit speed) for each interface you plan to connect.

Other Connection Requirements

If connecting any of the firewall's Ethernet interfaces directly to another router, a server or a similar device (*i.e.* not an Ethernet switch or hub), then you must use a crossover cable to connect the firewall to the other device.

❖ **Note:** *Ethernet cables, crossover cables and cable connectors are not supplied with the IntraGuard product. Please contact your reseller or your Compatible Systems representative for information on obtaining the correct Ethernet cabling supplies. Cable diagrams for the most commonly used cables are provided in the technical support section of our website.*

Chapter 3 - Network Installation



IntraGuard Firewall Back Panel

This section of the manual describes how to connect the IntraGuard Firewall to your Ethernet network. In summary, the steps for installation are:

1. Make sure the firewall is powered down and not connected to any power source.
2. Connect the firewall to the Ethernet network(s).
3. Connect a management console to the firewall (optional).
4. Plug in the power cable and power up the firewall.

Placing the Firewall

The IntraGuard Firewall is meant to be left stand-alone on a desktop or equipment table.

❖ **Note:** *When stacking other equipment on the IntraGuard, do not exceed 25 pounds of evenly distributed weight on top of the device. Additional weight may bend the case.*

Connecting the Firewall to the Ethernet

If your twisted-pair hub or switch is already in place, you can connect the firewall to an active network without interrupting network activity. The firewall must be powered off.

Connecting to Twisted-Pair Ethernet

Before connecting the firewall to twisted-pair cabling, you need an unshielded twisted-pair cable that is already connected to your 10BaseT-compatible or 100BaseTx-compatible twisted-pair hub or switch.

To connect the firewall to the twisted-pair network, simply plug the

twisted-pair cable into the RJ-45 Ethernet connector on the back of the unit.

The default configuration of the IntraGuard is appropriate for many network applications. To operate the IntraGuard using the default configuration, connect your insecure/gateway network to the Red/Ethernet 2 interface, and connect your secure/internal network to the Green/Ethernet 0 interface. You may also use the Yellow/Ethernet 1 interface to connect a "DMZ" (Demilitarized Zone) network which will allow limited access to some secured resources such as a web or mail server. For other applications or for more information on the default security policy, see the Configuration Guide.

❖ **Note:** *The servers available on the DMZ/Yellow network should have appropriate security features such as passwords already configured.*

Connecting a Management Console

If you wish to connect an out-of-band management console, use the supplied cable and connect to the Console interface on the back of the IntraGuard. You can use a dumb terminal or a PC equipped with VT100 terminal emulation.

The default settings for the Console interface are VT100 terminal emulation, 9600 bps, 8 bits, no parity, 1 stop bit and no Flow Control.

Powering Up the Firewall

Power up the firewall. If you are using the firewall's Standard security policy, this is all that is required. To configure the firewall or to use the management and logging features, you must first configure an IP address into the firewall with either an out-of-band console or with a reconfigured IP host or workstation on the same Ethernet segment as the firewall. See ***Chapter 5 - Command Line Management*** for instructions.

Chapter 4 - CompatiView Software Installation

All of the devices in Compatible Systems' multiprotocol family, including the IntraGuard, can be managed from a single management platform called CompatiView. CompatiView for Windows is included on the CD-ROM which was shipped with your IntraGuard unit.

❖ **Note:** *An older version of CompatiView for Mac OS was included on the CD-ROM shipped with your firewall. The Mac OS version can be used with other Compatible products such as MicroRouters and RISC Routers; however, it is not compatible with the IntraGuard software. You must use CompatiView for Windows, versions 5.0 or later, to manage your firewall with CompatiView. PC emulator software may be used for this purpose, if your Macintosh supports it.*

CompatiView for Windows

CompatiView for Windows allows you to manage the IntraGuard from an IBM-compatible PC running Windows 95/98 or Windows NT. The PC can either be configured as an IPX client on a Novell NetWare internet, or as an IP WinSock client on an IP internet.

System Requirements

In order to successfully run CompatiView for Windows, you need:

- IBM PC or compatible w/486 or later processor
- Microsoft Windows 95/98, or Windows NT installed
- VGA or better monitor
- IP - A WinSock-compatible transport stack

  - and/or -
- IPX - A Netware or Microsoft Client installation

❖ **Note:** *To choose the active transport protocol on a Windows machine which has both IPX and IP installed, select "Options" from the Administration menu and click the appropriate radio button under "Default Transport."*

Installation and Operation

The Windows version of the CompatiView program can be found in the Network Management/CompatiView/Windows directory on the CD-ROM that was included with your IntraGuard.

Run the auto-installation program (CV5x file) by double-clicking on it. The installation program will ask you to select (or create) a directory in which it should locate CompatiView and its associated files and database subdirectory.

Once the installation is complete, double-click on the CompatiView icon to open the program. For further information on using CompatiView, see the *CompatiView Management Software Reference Guide* included with your router.

❖ **Note:** *For an up-to-date description of the changes (if any) made to Windows system files by the installation program, see the README.TXT file located in the CompatiView installation directory.*

Transport Protocols and CompatiView

CompatiView will be able to use the transport protocol (IP or IPX) you have selected to access Compatible Systems products anywhere on your internetwork. This means you can use the IP transport option to manage the firewall across the Internet. However, the firewall's Standard security policy does not allow management from the Internet side of the IntraGuard. For secure remote management of the IntraGuard, a Compatible Systems IntraPort VPN Access Server is recommended to provide VPN-protected remote Telnet.

The IP protocol does not provide a method for CompatiView to automatically discover the firewall. To initially contact the firewall over IP using CompatiView, you must first enter a valid IP address into the firewall. You can do this either on a console directly connected to the firewall or by setting a workstation's IP address to 198.41.12.2 with a Class C subnet mask (255.255.255.0) so that it can communicate over Ethernet with 198.41.12.1 (the shipping default of the bridge interface on the firewall). After setting the firewall's IP address, be sure to change the workstation's configuration back to its original settings.

The IPX protocol does allow CompatiView to automatically discover the router. Compatible Systems devices are configured to autoseed the two most common IPX frame types upon startup (802.2 and 802.3 (raw)). If CompatiView has the IPX/SPX protocol selected as its trans-

port, it will be necessary to either powerup the router before powering up the workstation, or reboot the workstation after the router has completed its boot sequence. This process will ensure that the workstation and the router have the proper IPX network bindings for communication.

Chapter 5 - Command Line Management

The command line interface allows you to configure and monitor the firewall in-band via Telnet or out-of-band with a terminal connected to the firewall's Console interface.

❖ **Note:** *Proper syntax is vital to effective operation of command line management. Case is not significant – you may enter commands in upper case, lower case, or a combination of the two.*

Out-of-Band Command Line Management

You can use command line management and text-based configuration out-of-band as a permanent management method, or only temporarily in order to set the firewall's IP parameters to allow in-band Telnet access.

In order to access the command line out-of-band, do the following:

1. Set a terminal or a PC equipped with VT100 terminal emulation to a baud rate of 9600, 8 bits, no parity, 1 stop bit and no Flow Control.
2. Connect it to the firewall's Console interface using the cable which was supplied with the IntraPort 2/2+.
3. Press the <Return> key one or two times.
4. Enter the default password ***letmein*** at the password prompt. The command line interface prompt will appear on the screen.

If you plan to use out-of-band access for ongoing management of your firewall, you can find further information on using the command line interface in the *Text-Based Configuration and Command Line Management Reference Guide* that was supplied with your firewall. Otherwise, see the section on Setting Up Telnet Operation for information on setting the firewall to allow Telnet access from hosts on its network.

Temporarily Reconfiguring a Host for Command Line Management

You can temporarily reconfigure an IP host in order to set the firewall's IP parameters to allow in-band Telnet access.

If you wish to set the firewall's basic IP parameters in this fashion, the host must be on the same Ethernet segment as one of the firewall's Ethernet interfaces. You can then do the following:

1. Set the host's IP address to 198.41.12.2, with a Class C subnet mask (255.255.255.0) and then Telnet to 198.41.12.1.
2. Enter the default password ***letmein*** at the password prompt. The command line interface prompt will appear on the screen.
3. Use the **configure** command and set the **IPAddress**, **SubnetMask**, and **IPBroadcast** keywords in the **IP Ethernet 0** section.
4. Use the **save** command to save the changes to the device's Flash ROM.
5. Change the host's configuration back to its original settings.

See the next section (*Setting Up Telnet Operation*) for information on setting the firewall to allow Telnet access from hosts on its network.

Setting Up Telnet Operation

Telnet is a remote terminal communications protocol based on TCP/IP. With Telnet you can log into and manage the IntraGuard from anywhere on your internal IP network. However, the Standard security policy does not allow management from the Internet side of the IntraGuard. For secure remote management and configuration, a Compatible Systems IntraPort VPN Access Server is recommended to provide VPN-protected remote Telnet.

To manage the firewall via Telnet, you must run Telnet client software on your local computer, which will communicate with the Telnet server built into the unit.

You must also set some basic IP parameters for the firewall bridge interface. There are several ways to do this. You may set them using command line commands either out-of-band via the Console interface or in-band via a reconfigured IP host. Instructions for setting up these two methods were given earlier in this chapter.

You may also use CompatiView from a reconfigured IP host (if using

the IP transport protocol), or anywhere on your network (if using the IPX transport protocol). Instructions for these two methods are given in Chapter 4 on CompatiView installation.

The required parameters for Telnet access to an interface are the IP address, IP subnet mask, and IP broadcast address.

With CompatiView, these can be set using the TCP/IP Routing: Bridge 0 dialog box.

With text-based configuration, these can be set using the **configure** command and the **IPAddress**, **SubnetMask**, and **IPBroadcast** keywords in the **IP Bridge 0** section. Use the **save** command to save the changes to the device's Flash ROM.

To change the configuration parameters in the IntraGuard, the firewall will request a password. The default for this password is ***letmein***.

After you have set these IP parameters and saved the changes, you can use Telnet to access the firewall from any node on your internal IP internetwork. Invoke the Telnet client on your local host with the IP address of the firewall you wish to manage.

Chapter 6 - IntraGuard Configuration Guide

The default settings of the IntraGuard Firewall should work for many installations, with no additional configuration required. If changes to the default configuration are necessary, this Configuration Guide provides an outline of the parameters that may be set.

This section includes information on the default configuration, the five different security levels, the protocol-specific security options, and NAT (Network Address Translation) configuration. This section does not include information on setting up packet filters in the IntraGuard. See the **[IP Filter *<Name>*]** section in the *Text-Based Configuration and Command Line Management Reference Guide* or *CompatiView Management Software Reference Guide* for more information on creating IP packet filters.

❖ **Note:** *More information on the meaning of the firewall's parameters is provided in the* ***Text-Based Configuration and Command Line Management Reference Guide*** *and* ***CompatiView Management Software Reference Guide****. You should use this Configuration Guide as a starting point to look up more specific information in the other reference guides.*

Setting Up Firewall Paths

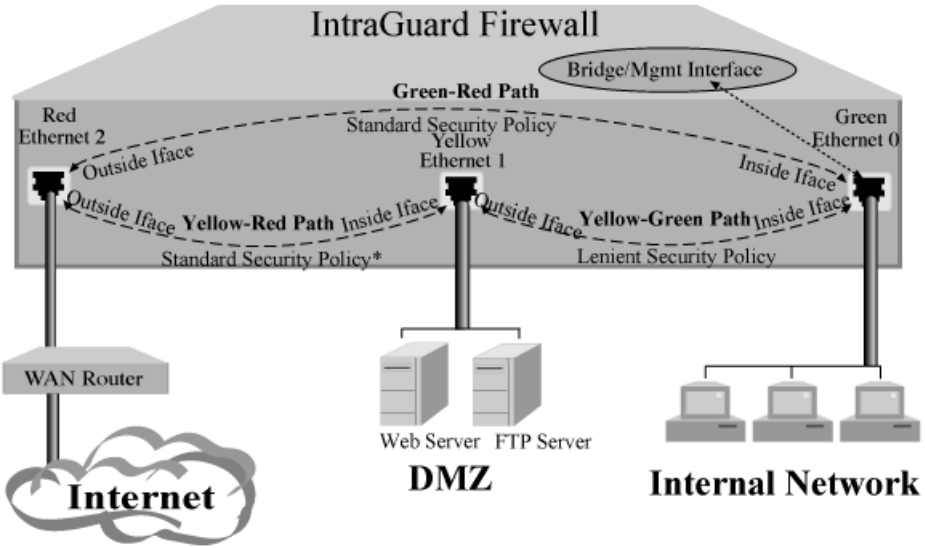
There are three pre-set paths in the IntraGuard Firewall. Paths define a route for packets through the firewall. Each of the three paths already has a name, a security policy and interface definitions. The default settings of each path are shown below.

```
[ Dynamic Firewall Path "Green-Red" ]
SecurityPolicy           = Standard
OutsideInterfaces        = Ether 2
InsideInterfaces         = Ether 0
InsideInterfaces         = Bridge

[ Dynamic Firewall Path "Yellow-Red" ]
SecurityPolicy           = Standard
DNSUse                   = Both
WebUse                   = Both
MailUse                  = Both
OutsideInterfaces        = Ether 2
InsideInterfaces         = Ether 1

[ Dynamic Firewall Path "Green-Yellow" ]
SecurityPolicy           = Lenient
InsideInterfaces         = Ether 0
InsideInterfaces         = Bridge
OutsideInterfaces        = Ether 1
```

Each path has two endpoints – inside interfaces and outside interfaces. Typically, inside interfaces are secure while the outside interfaces are less secure.

The path name can be changed to anything between one and 126 alphanumeric characters. The interface assignments can also be changed.

The diagram below illustrates the default settings of the three Intra-Guard Firewall paths.



* The Yellow-Red Path's Standard security policy includes three modifications. It allows HTTP packets (WebUse), DNS packets (DNSUse) and SMTP packets (MailUse) both in and out along the path. See the next section on "Selecting a Security Policy" for more information.

If more than one interface is designated as an inside or outside interface on a particular path, those interfaces are considered to be open multiplexed and traffic will flow freely between them.

Selecting a Security Policy

There are five preconfigured security policies on the IntraGuard. These policies can be used as-is or can serve as the basis for a custom security policy.

- **Blocked** is the most secure policy, which does not allow packets in or out along the path. It is the equivalent of physically separating the internal and external networks. The Blocked policy can be used to create a very restrictive policy using the additional configuration options.
- **Strict** is a restrictive policy set. A small set of outgoing client sessions are permitted through the firewall and all incoming server sessions are excluded.
- **Standard** is the default policy set. Almost all outgoing client sessions are permitted and almost all incoming server sessions are excluded. The only exceptions to those rules are that the BGP and X Windows protocols are excluded from going in or out of the firewall.
- **Lenient** is a less secure policy. All outgoing client sessions are permitted and some incoming server sessions are permitted.
- **Open** is an insecure policy set. Everything is permitted through the firewall, thereby turning the firewall into a transparent bridge.

Based on the security policy, each path has an associated list of protocol "pushbutton" settings which define how the interfaces belonging to the path will handle those types of packets.

The chart below shows the different protocol-specific settings for each security policy.

Protocol Pushbuttons	Security Policy				
	Blocked	Strict	Standard	Lenient	Open
BGPUse	None	None	None	Both	Both
BSDUse	None	None	Out	Out	Both
CompatiViewUse	None	Out	Out	Both	Both
DNSUse	None	Out	Out	Both	Both
FTPUse	None	Out	Out	Both	Both
H323Use	None	None	Out	Out	Both
ICMPUse	None	None	Out	Out	Both
IPSecUse	None	Out	Out	Both	Both
IRCUse	None	None	Out	Out	Both
LPRUse	None	None	Out	Out	Both
MailUse	None	Out	Out	Both	Both
NFSUse	None	None	Out	Out	Both
NetBIOSUse	None	None	Out	Out	Both
NewsUse	None	None	Out	Out	Both
NonIPUse	None	None	Out	Out	Both
OSPFUse	None	None	Out	Out	Both
POPUse	None	None	Out	Out	Both
RIPUse	None	None	Out	Out	Both
RealAudioUse	None	None	Out	Out	Both
SunRPCUse	None	None	Out	Out	Both
TelnetUse	None	Out	Out	Out	Both
TFTPUse	None	Out	Out	Out	Both
TunnelUse	None	None	Out	Out	Both
WebUse	None	Out	Out	Both	Both
XWinUse	None	None	None	In	Both
ISAKMPUse	None	Out	Out	Both	Both
GopherUse	None	Out	Out	Out	Both
NTPUse	None	None	Out	Both	Both
OtherTCPUse	None	None	Out	Out	Both
OtherUDPUse	None	None	Out	Both	Both
OtherUse	None	None	Out	Both	Both

If you change the security policy – from Standard to Lenient, for example – the protocol-specific pushbutton settings will automatically be changed to reflect the new security policy. The protocol-specific options may then be changed individually to create a customized security policy.

❖ **Note:** *CompatiView and the command line interface handle the push-button settings slightly differently. Changes made to an individual protocol-specific pushbuttons using text-based configuration (i.e., the command line interface) will not be automatically changed to reflect a new security policy.*

An example would be changing the **DNSUse** *keyword to None, which specifies that DNS packets will not be allowed in or out along the path. Even if the security policy is changed to Lenient, which has a default DNSUse setting of Both (specifying that DNS packets are allowed both in and out along the path) the* **DNSUse** *keyword will maintain the manually configured None setting.*

Changing the overall security policy with CompatiView will override any manual settings.

Customizing a Security Policy

In addition to allowing for customized protocol-specific pushbutton settings, each firewall path allows for the creation of two other types of filter policy sets.

The firewall applies the different policy sets in a particular order. First the pushbutton options are applied, then the Allow Ports/Protocol settings and lastly the IP filter sets are applied.

Allow Ports/Protocols

```
TCPInPort        =
TCPOutPort       =
UDPInPort        =
UDPOutPort       =
IPInProto        =
IPOutProto       =
```

The Allow Ports/Protocols options allow you to specify any numbered port or named protocol which isn't already a pushbutton option. RFC 1700 "Assigned Numbers" contains a listing of all currently assigned IP protocol keywords and numbers.

Static IP Packet Filters

```
OrFilterOut      =
OrFilterIn       =
AndFilterOut     =
AndFilterIn      =
```

"Or" filters are typically used to permit certain packets. These filters are checked only for those protocols or ports which have been denied by a pushbutton or Allow Ports/Protocols setting. For example, if **TelnetUse** has been set to **None**, then an "Or" filter can be used to permit Telnet sessions from a particular site which you trust.

"And" filters are typically used to deny certain packets, so they are checked only for those protocols or ports which have been permitted by a

pushbutton, Allow Ports/Protocol setting or an "Or" filter.

Any packets not explicitly allowed are dropped. This is particularly important to consider when applying static IP filter sets, where the final rule should always be

```
permit 0.0.0.0 0.0.0.0 ip
```

The pushbutton options are implemented in the IntraGuard using dynamic filtering technology which has been optimized for performance, whereas IP packet filters use static filtering technology. Performance of the firewall will be best if no static IP filter sets are defined.

CV: Static IP filter sets can be created using the TCP/IP Filtering dialog box (under Global/Filtering/TCP/IP Filtering). They can then be applied to a path using 'AND' Filters and 'OR' Filters options in the Settings: Firewall Path dialog box.

TB: Static IP filter sets can be created using the **edit config** command and the **[IP Filter <Name>]** section. They can then be applied here using the keywords listed above to specify a named filter set.

Other Path Settings

Each path has several other configurable parameters, which are shown below with their default settings.

```
SendTCPReset              = On
SynRejectOnly             = On
SendICMPReset             = On
ICMPtoTCPsession          = Off
PermitEstTCP              = Off
ResetRedirects            = Off
MinIPFragLen              = 40
RejectSRCRoute            = On
```

CV: To make changes to the default configuration for a particular path, use the Advanced Settings: Firewall Path Dialog Box. To access this dialog box, use the Advanced button on the Settings: Firewall Path Dialog Box.

TB: To make changes to the default configuration for a particular path,use the **configure** command and make changes in the **[Dynamic Firewall Path <Name>]** section.

Setting Global Firewall Parameters

Changing the Passwords

You may want to change the firewall's passwords.

CV: Use the System Configuration Dialog Box (under Global/System Configuration).

TB: Use the **configure** command and set the **Password** and **Enable-Password** keywords in the **[General]** section.

Global Settings

The default settings for the **[Dynamic Firewall Globals]** section should be adequate for most installations. This section is used to set timers for the firewall. The default configuration is shown below.

```
[ Dynamic Firewall Globals ]
SYNTimer                = 20
FINTimer                = 10
TCPTimeout              = 172800
UDPTimeout              = 60
DynamicTimer            = 60
RejectTimer             = 300
HalfShutTimer           = 120
```

CV: To make changes to the default configuration, use the Firewall Settings Dialog Box (under Global/Firewall Settings).

TB: To make changes to the default configuration, use the **configure** command and change the keywords in the **[Dynamic Firewall Globals]** section.

Logging Settings

The logging settings define the level at which specific events are logged. The IntraGuard's default logging configuration is shown below.

```
[ Dynamic Firewall Logging ]
Rejects                  = Warning
TCP_EST_Reject           = Error
Sessions                 = Error
TearDown                 = Warning
IP_Timeouts              = Warning
TCP_Timeouts             = Alert
TCP_Resets               = Notice
ICMP_Resets              = Notice
TCP_SYN                  = Critical
TCP_FIN                  = Critical
Redirects                = Critical
General                  = Critical
```

The seven possible log levels are listed below in descending order of importance.

- 0/Emergency
- 1/Alert
- 2/Critical
- 3/Error
- 4/Warning
- 5/Notice
- 6/Info
- 7/Debug

Off may also be selected, and will disable log messages for the event.

The IntraGuard "tags" the log messages associated with each type of event with the specified log level. The event log messages will appear in the log buffer (or wherever log messages are being sent), only if the global log level is at the same level or a lower level of importance. This allows you to closely monitor certain events while excluding events you do not wish to closely monitor from the log. Logging parameters for the device, including the global log level, are set in the **[Logging]** section.

Using the default configuration as an example, if you wish to see log messages for **TCP_Resets**, which have a default setting of Notice, you would need to set the **Level** keyword in the **[Logging]** section to Notice, Info or Debug. Any other setting would mean that **TCP_Resets** would not appear in the log.

CV: To make changes to the IntraGuard's event logging parameters, use the Firewall Logging Dialog Box (under Global/Firewall Logging).

TB: To make changes to the IntraGuard's event logging parameters, use the **configure** command and change the keywords in the **[Dynamic Firewall Logging]** section.

Setting Up NAT (Network Address Translation)

In order to set up NAT on the IntraGuard, it is necessary to assign an IP address to the interface which will serve as the NAT internal interface (usually Ethernet 0). The Bridge interface, which should already have an IP address, will serve as the NAT external interface.

IP Setup for NAT

These parameters set the basic IP configuration necessary for NAT.

- IP Address
- IP Subnet Mask
- IP Broadcast Address
- RIP 1 (Routing Information Protocol version 1) or RIP 2 (version 2)
- NAT Mapping On

CV: Use the TCP/IP Routing: Ethernet Dialog Box.

TB: Use the **configure** command and the **IPAddress**, **SubnetMask**, **IPBroadcast** and **RIPVersion** keywords in the **[IP Ethernet 0]** section. Set the **RIPVersion** and the **NatMap** keywords in the **[IP Bridge]** sections.

❖ **Note:** *The IP address for Ethernet 0 must be part of the same network as the NAT InternalRange, which is set using the* **NAT Global** *section (see the Nat Global Settings below). Likewise, the Bridge IP address must be part of the same network as the NAT ExternalRange.*

Firewall Path Settings for NAT

Ethernet 0 should be removed as an Internal Interface from the paths to which it belongs.

CV: Use the Settings: FirewallPath Dialog Box

TB: Use the **config** command and the **[Dynamic Firewall Path Green-Yellow]** and the **[Dynamic Firewall Path Green-Red]** section, then use the **delete** command to delete the **InsideInterface** keywords for Ethernet 0 *only.*

NAT Global Settings

There are only a few required global NAT settings.

- Enabled
- Internal Range
- External Range

CV: Use the NAT Configuration Dialog Box (under Global/NAT).

TB: Use the **configure** command and set the **Enabled**, **InternalRange**, and **ExternalRange** keywords in the **[NAT Global]** section.

❖ **Note:** *In order to use NAT on the IntraGuard with a DMZ network, you must have enough "official" IP addresses to be assigned to each device on the DMZ.*

NAT Mapping Settings

These optional parameters can only be set using text-based configuration. To set up one-to-one translation pairs between the internal and external networks, use the **edit config** command and the **[NAT Mapping]** section.

Saving a Configuration File to Flash ROM

Once a configuration is complete, you can save it to the firewall's Flash ROM. Until saved, all changes are made in a separate buffer and the firewall's interfaces continue to run as before the changes were made.

CV: Use the Save to/Device option from the File menu.

TB: Use the **save** command.

Appendix A - Shipping Defaults

Default Password

- letmein

Ethernet Interfaces

IP Routing Defaults

- Off, all interfaces

IP Bridging Defaults

- On, all interfaces
- Address: 198.41.12.1
- Subnet mask: 255.255.255.0
- Broadcast address: 198.41.12.255
- Mode: Routed

Appendix B - Connector and Cable Pin Outs

Pin Outs for DB-25 Male to DB-25 Female RS-232 Data & Console Cable

The cable supplied with the IntraGuard Firewall is twenty-five conductors connected straight through. Connections on the Console interface follow the standard RS-232 pin outs.

Appendix C - LED Patterns and Test Switch Settings

IntraGuard Firewall LED Patterns

Ethernet Back Panel Indicators LEDs

The IntraGuard Firewall features three sets of lights on the back panel to indicate the hardware status of each of the three Ethernet ports.

Link: The Link light indicates that there is a good connection to the hub.

Activity: The Activity light indicates that there is activity across the link.

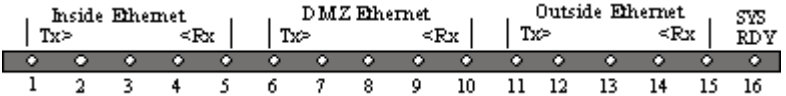
Front Panel LEDs

The IntraGuard Firewall uses a number of light patterns on the front LED bars to indicate various operating conditions.

- **Sys Ready -** The firewall booted properly without detecting any failures.
- **Power On, No Traffic -** The firewall will scan through the LED bar, from left to right, illuminating one element at a time.
- **Ethernet Traffic Indicators -** Each Ethernet interface has its own set of five LED lights.
    - TX: Ethernet transmit packet
    - RX: Ethernet receive packet

IntraGuard Special Indicators

To understand the special indicator lights on the IntraGuard, it is helpful to assign them numbers 1-16, from left to right.



IntraGuard Front Panel LED Bars

ETHERNET LIGHTS	INDICATION
4&5 and 12&13 flashing	Firewall stacks starting up.
2&3, 6&7, 10&11, 14&15 flashing	No OS loaded. Running from ROM.
1,4&5, and 12,13&16 flashing	Erasing OS or config in Flash ROM.
Scanning from the outside toward the center	Flash ROM erase due to switch setting five or six is complete. Set switch to zero and cycle power.

IntraGuard Firewall Switch Settings

0 Normal Operation
1 Unused*
2 Unused*
3 Run Boot ROM Downloader
4 Unused*
5 Erase Flash ROM (OS and Configuration)
6 Erase Flash ROM (Configuration Only)
7 Unused*
8 Unused*
9 **Allow *letmein* password for 5 minutes after powerup**

❖ **Note:** *Settings marked with an asterisk may erase your Flash ROM. Please do not use these settings without first contacting Compatible Systems Technical Support.*

Appendix D - Downloading Software From Compatible Systems

We make the latest versions of operating software for all Compatible Systems products available at our Web site. The latest version of CompatiView management software is also available.

To download software, follow the instructions below.

1. Use your browser to access http://www.compatible.com/, and find the link on our home page to "Software Downloads."
2. Select the product and software version you want, and click on the appropriate file to download it.

❖ **Note:** *Uncompressed downloads (suitable for TFTP and CompatiView Windows downloading) are stored as .DLD files. Self-extracting Windows compatible style files (and CompatiView for Windows itself) are stored as .EXE files. Self-extracting Macintosh style files are stored as .sea.bin (MacBinary format) and/or .sea.hqx files.*

❖ **Note:** *These files are also accessible directly via Anonymous FTP at* **ftp.compatible.com/files/**.

Appendix E - Terms and Conditions

Compatible Systems Corporation (Compatible Systems) offers to sell only on the condition that Customer's acceptance is expressly limited to Compatible Systems' terms and conditions of sale. Compatible Systems' acceptance of any order from Customer is expressly made conditional on assent to these terms and conditions of sale unless otherwise specifically agreed to in writing by Compatible Systems. In the absence of such agreement, commencement of performance or delivery shall be for Customer's convenience only and shall not be construed as an acceptance of Compatible Systems' terms and conditions. If a contract is not earlier formed by mutual agreement in writing, Customer's acceptance of any goods or services shall be deemed acceptance of the terms and conditions stated herein.

1. Warranty. Compatible Systems warrants to the Customer and to all persons who purchase Products from the Customer during the Warranty terms ("subsequent purchasers"), that, for an unlimited period from the date (the "shipping date") on which Compatible Systems ships the Products to the Customer: (a) the Product meets, in all material respects, all specifications published by Compatible Systems for such Products as of the shipping date; (b) the Products are free from all material defects in materials and workmanship under normal use and service; and (c) that as a result of the purchase of the Products from Compatible Systems, the Customer will have good title to the Products, free and clear of all liens and encumbrances.

Compatible Systems' obligations pursuant to this Warranty, and the sole remedies of the Customer and of any subsequent purchaser, shall be limited to the repair or replacement, in Compatible Systems' sole discretion, of any of the Products that do not conform to this Warranty.

This Warranty shall be invalidated if the Products (a) have not been installed, handled, or used in accordance with Compatible Systems recommended procedures; (b) have been damaged through the negligence or abuse of the Customer or of any subsequent purchasers; (c) are damaged by causes external to the Products, including (without limitation) shipping damage, power or air conditioning failure, or accident or catastrophe of any nature; and (d) have been subjected to repairs or attempted repairs by any person other than Compatible Systems (or an authorized Compatible Systems service technician).

To obtain service under this Warranty, the Customer (or subsequent purchaser, if applicable) must follow the procedures outlined below, under "Product Return Policy."

THE WARRANTIES SET FORTH IN THESE TERMS AND CONDITIONS ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED. WITHOUT LIMITATION ON THE GENERALITY OF THE FOREGOING SENTENCE, COMPATIBLE SYSTEMS EXPRESSLY DISCLAIMS AND EXCLUDES ALL IMPLIED WARRANTIES OF MERCHANTIBILITY AND OF FITNESS (GENERALLY OR FOR A PARTICULAR PURPOSE).

2. Shipments. All delivery indications are estimated and are dependent in part upon prompt receipt of all necessary information to service an order. Compatible Systems shall not be liable for any premium transportation or other costs or losses incurred by Customer as a result of Compatible Systems inability to deliver Product in accordance with Customer's requested delivery dates. All shipments by Compatible Systems are made F.O.B. factory (Boulder, Colorado); risk of loss shall pass to Customer at point of shipment. Unless specified by the Customer, Compatible Systems will select the mode of transportation for each order. Compatible Systems reserves the right to make deliveries in installments. Partial shipments are subject to the terms of payment noted below. Compatible Systems reserves the right to allocate inventory and production if such allocation becomes necessary.

3. Payment Terms. Payment shall be made prior to shipment or upon delivery, unless otherwise agreed to in writing. Payment shall not constitute acceptance of the goods.

4. Force Majeure. All orders accepted by Compatible Systems are subject to postponement or cancellation for any cause beyond the reasonable control of Compatible Systems, including without limitation: inability to obtain necessary materials and components; strikes, labor disturbances, and other unavailability of workers; fire, flood, and other acts of God; war, riot, civil insurrection, and other disturbances; production or engineering difficulties; and governmental regulations, orders, directives, and restrictions.

5. Product Return Policy. Prior to shipping any Product to Compatible Systems, the Customer must contact Compatible Systems Technical Support (by letter or telephone) with the following information: (a) reason for return; (b) quantity, description, and model number, and (if applicable) serial number of each item being returned; (c) original Compatible Systems Sales Agreement number; and (d) any special instructions. Upon receipt of this information, Compatible Systems will issue an RMA ("Return Material Authorization") number and any required U.S. Customs identification to assure correct identification of the Customer and to insure prompt and accurate processing.

6. Limitation of Remedies. Compatible Systems' liability for all claims brought pursuant to or in connection with this agreement, including the purported breach hereof, shall be limited: (a) in the case of claims for breach of warranty, to compliance with the repair or replacement provisions of the warranty, and (b) in all other cases (including any claim that the warranty

failed of its essential purpose), to actual damages of the Customer (or, if appropriate, of the subsequent purchaser). IN NO EVENT SHALL COMPATIBLE SYSTEMS BE LIABLE FOR ANY SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES ARISING OUT OF THE SALE, USE, INSTALLATION OR OPERATION OF THE PRODUCTS, WHETHER A CLAIM IS BASED ON STRICT LIABILITY, BREACH OF WARRANTY, NEGLIGENCE, OR ANY OTHER CAUSE WHATSOEVER, WHETHER OR NOT SIMILAR. This limitation on remedies shall apply even if Compatible Systems is advised of the possibility and nature of any special, consequential, or incidental damages.

7. Governing Law; Merger. This agreement and all Terms and Conditions hereof shall be governed by, and construed in accordance with the internal laws of the State of Colorado. Except as superseded by a separate written contract signed by both Compatible Systems and the Customer, superseding all prior negotiations or offers, written or oral, this agreement may be amended only in writing, signed by an authorized officer of Compatible Systems.