



[www.gpcg.org](http://www.gpcg.org)

# **GPCG Computer Security**

## Firewall Guideline



# Table of Contents

<b>Acknowledgements</b>	<b>2</b>
<b>Introduction</b>	<b>3</b>
<b>Why do we need firewalls?</b>	<b>3</b>
What is a firewall?	4
What other computer security is needed?	5
What if your ISP already provides a firewall?	5
Firewall implementation issues	6
<b>Firewall Checklist</b>	<b>8</b>
<b>Firewall Selection Chart</b>	<b>10</b>
<b>Glossary</b>	<b>14</b>

## Acknowledgements

The General Practice Computing Group would like to thank the following people for contributing to *GPCG Computer Security – Firewall Guideline*. Dr Horst Herb conceived and formulated the original LAN Firewalls document with subsequent input from Dr Ian Cheong, Dr Rob Hosking and Dr David Guest. Further technical expertise was received from the Broadband for Health Section of the Department of Health and Ageing. Additional feedback has been provided by state-based officers of the Australian Divisions of General Practice.

*GPCG Computer Security – Firewall Guideline* was jointly funded by the Australian Government and General Practice Computing Group.

This resource has been designed as a companion document to the *GPCG Computer Security Self-Assessment Guideline and Checklist for General Practitioners* (the Security Guidelines).

Additional copies of these resources are available from the GPCG Secretariat or download from [www.gpcg.org.au](http://www.gpcg.org.au)

General Practice Computing Group  
C/- Royal Australian College of General Practitioners  
1 Palmerston Crescent  
South Melbourne, Vic 3205  
Tel: (03) 8699 0414

© June 2005

## Introduction

The aim of this booklet and associated web-based Tutorial at [www.gpcg.org.au](http://www.gpcg.org.au) is to enhance awareness and understanding about firewalls. It will assist your medical practice to:

- ] make an informed choice regarding firewall products and/or services
- ] install a firewall product best suited to your practice
- ] configure the firewall so that all desired Internet services will work without placing your practice network at unnecessary risk
- ] maintain the effectiveness of the firewall.

The information has been developed by the General Practice Computing Group (GPCG) in consultation with the Broadband for Health Section of the Australian Department of Health and Ageing. Additional input has been provided by state-based officers of the Australian Divisions of General Practice.

This booklet provides an introduction to the Tutorial. It includes a firewall selection table to help you select the appropriate type of connectivity for your practice. It also includes an implementation, configuration and management policy checklist.

While the Guideline and Tutorial can help you understand firewalls, you will require technical expertise to follow through and properly protect your computer system.

Setting up a firewall requires networking and network security knowledge. If your practice does not have a skilled IT person on staff, the Tutorial may still act as a guideline for hiring professional IT staff and/or services, and as a checklist for specifying the work that needs to be done.

## Why do we need firewalls?

Australian privacy legislation requires medical practices take reasonable steps to protect confidential patient data. If your practice computer system/s connects to the Internet, the GPCG recommends you protect that connection with a properly configured firewall.

According to the 2004 Australian Computer Crime and Security Survey by the Australian Computer Emergency Response Team (AUSCERT), the key computer security trends in Australia are:

- ] 95% of respondents reported experiencing computer security incidents in the past 12 months, with the majority of organisations experiencing between one and five incidents
- ] the number of respondents experiencing attacks that harmed the confidentiality, integrity and availability of networks, data or systems increased from 42% in 2003 to 49% in 2004

- ] the average financial loss per incident was \$116,212
- ] 88% of attacks originate from external sources
- ] 13% of respondents reported that hackers had penetrated their systems.

The full survey results can be found at [www.auscert.org.au](http://www.auscert.org.au).

One of the most reputable network security institutions, SANS (the SysAdmin, Audit, Network, Security Institute), regularly publishes lists of the worst mistakes people make that lead to security breaches – see [www.sans.org/resources/mistakes.php](http://www.sans.org/resources/mistakes.php). The most common mistakes made by IT people are ‘Connecting systems to the Internet before hardening them’. Establishing a firewall forms part of this hardening process. Patching known software vulnerabilities and removing services that are not required are the other ways of hardening systems.

Recently, SANS added a ‘bonus’ number 11: ‘Allowing untrained, uncertified people to take responsibility for securing important systems’. It is critical that you involve someone with adequate security experience when purchasing and setting up security for your practice computer system/s.

It is surprisingly easy for skilled people to gain full control over unprotected computers that are connected to the Internet. An intruders primary goal may not be the data you have stored on your computer. They may want to use your system to deliver spam mail for example. However, your data is still at risk of being compromised. Most computers in a medical practice store confidential patient data. Even if a compromised computer doesn’t store confidential data, it can potentially be used to access the rest of the practice network or even other health networks that your practice is connected to. Attacks are often an automated process and the attacker will only become personally involved when a weakness has been found, a malicious code (i.e. a Trojan Horse) has been successfully inserted, or something of interest has been located.

If a computer is connected to the Internet, even temporarily, a firewall is essential. It is possible for an attack to occur in very short time and at any hour of the day. Such attacks may not be obvious to the user.

## What is a firewall?

A firewall is a system designed to prevent unauthorised access to or from a private network (e.g. between your practice network and the Internet). Firewalls can be implemented in both hardware and software, or a combination of the two. All messages entering or leaving the private network must pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

There are several types of firewall techniques:

- ] **Packet filter** – a packet filter examines each packet (message) entering or leaving the network and accepts or rejects it based on the packet type or source/destination address, according to user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing, i.e. using a legitimate IP address or packet to gain unauthorised access to a computer.
- ] **Stateful inspection** – a stateful inspector monitors the state of network connections that pass through the firewall. It inspects incoming and outgoing packets to determine if they correspond to an authorised connection.
- ] **Application proxy** – an application proxy only permits packets related to specific applications to pass through the firewall. For example, SMTP packets for email and HTTP for web browsing. This is very effective, but can reduce the computers performance.

In practice, many firewalls use two or all of these techniques.

## What other computer security is needed?

According to SANS, one of the worst mistakes that lead to security breaches is to rely primarily on a firewall.

A firewall is considered a first line of defence in protecting private information against network attacks. While firewalls can be configured to filter certain types of traffic, that does not necessarily mean they stop all threats. For instance, firewalls may let email through irrespective of who sent the email and whether or not it contains a virus.

There are trade-offs between the level of filtering and the need to allow application services to pass through. An attacker may still be able to compromise your internal systems using application traffic which you allow to pass through the firewall. For example, some worm programs can infect your computer via HTTP, which is the communications protocol used for Internet browsing and web-based applications. Even with a firewall in place, you still need to take other security measures to protect your internal computer systems, including:

- ] arrangements to control people's access to the computer system and the types of information they access
- ] a means for uniquely identifying and authenticating each authorised user of the computer system, such as a user ID and password, a smart card and PIN, or biometrics
- ] audit and monitoring tools to detect intrusion and other forms of misuse
- ] regular off-site backup of the system data for disaster recovery
- ] physical security to prevent after-hours access to facilities that house the computer system and associated data storage media (CD, disks, etc)

- ] arrangements for the proper erasure of patient data prior to disposing of obsolete computer hardware and data storage media (i.e. complete data removal procedures)
- ] virus scanning and SPAM filtering of incoming email
- ] encryption services, such as a Virtual Private Network (VPN), to protect communications with other health systems and to allow GPs to securely access their practice systems from home, when visiting patients, or when working from other health facilities.

For more information on practice computer security refer to the *GPCG Computer Security Guidelines and Checklist* at [www.gpcg.org.au](http://www.gpcg.org.au)

## What if your ISP already provides a firewall?

The quality and effectiveness of Internet Service Provider (ISP) firewall services varies from provider to provider. If you are uncertain about the capabilities of your ISP's firewall service, consider switching your service to a provider that specialises in secure services. Some ISPs offer a Defence Signals Directorate (DSD) approved firewall service that meets government standards, albeit at a higher cost.

For more information on Australian Government firewall standards refer to [www.dsd.gov.au/infosec/index.html](http://www.dsd.gov.au/infosec/index.html).

Some ISPs offer firewall capabilities at their network gateway, which sits between the Internet and your access service (referred to as a network firewall). Others offer firewall capabilities in the network access device (router or modem) that is connected to your LAN (referred to as a LAN firewall). In the case of network firewalls, some ISPs may provide the same service, or 'single ruleset', for all customers. While this may provide adequate network security it may also restrict your business if the ISP is inflexible about modifying its rulebase to allow you to use non-standard application services. Other ISPs may have a very 'open rule' policy to accommodate all customer requirements, resulting in a lower network security regime which may not be adequate for your business.

In line with the 'defence in depth' security principle, it is good practice to have multiple layers of firewall capability at different points in your network. For example, you may wish to use the network firewall service at your ISP gateway together with a local LAN firewall, as well as installing firewall software on each computer connected to your LAN (personal firewalls). Personal firewalls should always be considered for computers that are used away from the practice (e.g. laptops), particularly if those computers have remote access into your LAN via wireless or dialup Internet services.



Many ISPs offer fully managed multi-tier firewall services. However, while you may rely on your ISP to provide a network firewall service, you may choose to provide your own LAN and personal firewalls. If you are planning to rely solely on your own firewall/s, you need to be confident that you have chosen the right firewall product and that you know how to properly configure and manage the firewall. You should also be aware that some applications, such as video conferencing and Voice Over Internet Protocol (VOIP), may not work 'out of the box' through your firewall.

Be prepared to continually manage your firewall configuration, making changes to the filtering rules to accommodate new applications as necessary, upgrading software and firmware with vendor patches to address any vulnerability in the firewall, and monitoring log files for signs of attacks.

## Firewall implementation issues

Implementation and secure configuration of a firewall may impact on the delivery of some applications services. While a firewall will not limit your ability to allow any services into your network, some services may implement less than secure protocols. By allowing these to pass through the firewall you may greatly diminish its effectiveness. Typically, applications that deliver file transfers such as Pathology may use less than secure protocols like FTP (File Transfer Protocol). Configuring your firewall to enable such applications may open up your network to attack through these protocol services.

If your secure firewall configuration is not enabling applications to pass through, you can seek support from the application supplier and a network security expert. Firewall configuration rules may be modified to allow the required application protocols to be accepted, or accepted from an authorised address, or in a particular network direction, so as not to compromise your network.

Alternatively, the application may require an insecure configuration of your firewall. The best advice in this case is to either work with the application vendor to modify the application to provide a secure firewall friendly transfer mechanism, or change to an application that does not require insecure configuration.

## Firewall checklist

This is a checklist of activities for ensuring secure connections to the Internet or other insecure public networks. It covers implementation and ongoing management requirements:

- ☐ Ensure firewall is installed between internal network and insecure public network such as the Internet.
- ☐ Ensure no other 'un-firewalled' connections to insecure networks are creating an unprotected backdoor into your LAN. All communications traffic to and from the internal network must be routed through the firewall as the only route.
- ☐ Ensure the firewall type selected is 'fit for purpose', i.e. the type recommended that will adequately protect against the security risks facing your practice. This comprises the IT environment type (size, complexity and applications) and the potential for network access to confidential patient data.
- ☐ Use firewall equipment that carries a valid certification or is recommended by an authorised body. These products provide a level of assurance having passed testing processes that certify fitness for use. The firewall selection chart in this booklet suggests products that have been informally assessed by General Practice experts. Other guidance can be found through Government Security Organisations including the DSD certified products program.
- ☐ Ensure firewall is correctly configured:
  - ☐ Turn off all ports not required. Only required ports to be activated in rules. The default rule is to deny all connections to and from the internal network and authorise specific connection via firewall rules.
  - ☐ Change passwords from factory defaults using non-weak passwords, i.e. not guessable or easily cracked by automated tools that try every possible password.
  - ☐ Limit physical access to the firewall.
  - ☐ Refine rules as desired to restrict inbound and outbound ports and restrict services to identified network addresses for services. Refer to configuration guidance on the site and vendor configuration guides.

- ☐ Ensure firewall software is kept up-to-date with patches as soon as possible after release. Put in place processes to monitor update releases. In some cases vendors may provide a notification or online update services.
- ☐ Ensure alerts are highlighted to firewall management person/s for key attack events and an accompanying response process.
- ☐ Where possible ensure network equipment, and in particular your firewall, is physically secured from unauthorised access. This may be in a lockable room.
- ☐ Check firewall rulebase each month to ensure it is current and applicable. Audit or engage an IT security specialist to confirm firewall is protecting against known computer hacking scenarios.
- ☐ Ensure firewall can only be managed via a trusted path, i.e. local log on or secure remote access.
- ☐ Ensure firewall is configured and managed by an appropriately skilled person. If this cannot be done internally get external support.

Remember firewalls are not the panacea of all computer security. Ensure other computer security measures are implemented including, but not limited to, installing antivirus software, applying security patches to operating and systems software as soon as possible after release, and physically securing computer equipment.

# Firewall selection chart

The GPCG recommends the following minimum firewall functionality for the uses or applications described. The applications and minimum functionality are listed from simple through to more complex solutions. You can find explanations of the types of firewalls mentioned at [www.gpcg.org.au](http://www.gpcg.org.au). Unless you have high level IT skills you should seek expert advice. This information will help you understand and question the advice you are given. Don't wait until you have a security breach. You will be liable for this as you would any breach of confidentiality from your practice. You may also be vulnerable to malicious damage to your system that could be costly to repair. If your computer/s are not connected to the Internet, you do not require a firewall.

APPLICATION	MINIMUM FIREWALL	HARDWARE COST	NETWORK TOPOLOGY	FIREWALL CONFIGURATION	RISKS NOT MANAGED BY FIREWALL	ADDITIONAL MEASURES REQUIRED	MAINTENANCE	COMMENTS
Web browsing and email Pathology downloading using encrypted data attached to email Internet banking	Dedicated stateful packet inspecting firewall	\$200 – \$600	All traffic to internal network must pass through firewall	All ports blocked (other than those few required for the services)  Remote administrative access to router barred	Malware – including viruses  Spyware  Unencrypted email  Access controls	Up-to-date antivirus software  Avoid sending confidential information over unencrypted email or encrypt all internal and external email traffic  Secure web browser  Training to ensure confidential information only supplied to trusted providers using secure connections  Confidential data access controls	Periodic updates of firewall firmware as released  <b>Beware:</b> if cables are not plugged into the correct ports on the firewall, the network could be open to the outside world	Pathology downloading by direct modem dialup to standalone PC is still safe and secure

APPLICATION	MINIMUM FIREWALL	HARDWARE COST	NETWORK TOPOLOGY	FIREWALL CONFIGURATION	RISKS NOT MANAGED BY FIREWALL	ADDITIONAL MEASURES REQUIRED	MAINTENANCE	COMMENTS
Pathology downloading using direct network connection requiring open ports HIC online	Dedicated stateful packet inspecting firewall	\$200 – \$600	All traffic to internal network must pass through firewall	Block all connections initiated by remote sites Initiate connections from practice Must use secure communication tunnels end to end Must authenticate endpoints securely Remote administrative access to firewall barred	Malware – including viruses Spyware Unencrypted email Access controls	Up-to-date antivirus software Avoid sending confidential information over unencrypted email Confidential data access controls	Periodic updates of firewall firmware as released <b>Beware:</b> if cables are not plugged into the correct ports on the firewall, the network could be open to the outside world	Many devices in this category have simple VPN capability Other connection mechanisms may be insecure and place internal network at risk Ensure mechanism is secure via secure firewall configuration and network design (e.g. DMZ for less secure protocols)
Connections between fixed locations (remote, practice or home) – permanent, or intermittent, with full network services available remotely	Dedicated stateful packet inspecting firewall with VPN (IPSEC) at each location Alternatively, dedicated stateful packet inspecting firewall with VPN pass through to VPN router	\$200 – \$800	All traffic to internal network must pass through firewall and VPN router if separate	Should only be used for point-to-point connections between known locations Must authenticate endpoints securely Remote administrative access to firewall barred	Malware – including viruses Spyware Unencrypted email Access controls	Up-to-date antivirus software Avoid sending confidential information over unencrypted email or encrypt all internal and external email traffic Secure web browser Training to ensure confidential information only supplied to trusted providers using secure connections Confidential data access controls	Periodic updates of firewall firmware as released <b>Beware:</b> if cables are not plugged into the correct ports on the firewall, the network could be open to the outside world	If access to external services required, refer to other sections for advice

APPLICATION	MINIMUM FIREWALL	HARDWARE COST	NETWORK TOPOLOGY	FIREWALL CONFIGURATION	RISKS NOT MANAGED BY FIREWALL	ADDITIONAL MEASURES REQUIRED	MAINTENANCE	COMMENTS
Practice website	External website hosting is strongly recommended  Firewall not specifically required if hosted by external provider  Dedicated stateful packet inspecting firewall with DMZ capability and load balancing over more than one connection	External hosting \$100 – \$300 per annum  Hardware firewall for internally hosted website \$1500 – \$3000	On-site web server for experts only  Web server must be in DMZ and not be hosting any other practice services, since it is potentially vulnerable	On-site web server for experts only  Permits web browsing (port 80) of web server in DMZ  All ports and traffic closed to internal network  Remote administrative access to firewall barred	Externally hosted website is still vulnerable to attack  Availability of website dependent on external hosting provider  On-site web server for experts only  Malware – including viruses  Spyware  Unencrypted email  Web server attacks  Access controls	On-site web server for experts only  Up-to-date antivirus software  Avoid sending confidential information over unencrypted email  Server intrusion detection with logging  Confidential data access controls	Externally hosted web site should be monitored for attack and data corruption  On-site web server for experts only  Periodic updates of firewall firmware as released  <b>Special Requirements</b> while conducting web server maintenance – disconnect from internet during maintenance procedures  Immediate action required in response to web server attacks	On-site web server for experts only  Maintaining a practice website is a potential risk and therefore easier if hosted externally
Public access to practice appointment systems	For experts only  Higher risk than practice website  Extremely technically challenging to set up and maintain in a secure fashion  Requires contracted specialised security expertise to oversee design/installation/ maintenance to ensure internal network is protected	\$1500 – \$3000	For experts only	For experts only	For experts only	For experts only	For experts only	For experts only



## Glossary

**Application services** - services that leverage bandwidth to deliver increased functionality and value to subscribers

**Biometrics** - the technique of studying physical characteristics of a person, such as finger prints, hand geometry, eye structure or voice pattern.

**DSD** – Defence Signals Directorate. The national authority for signals intelligence and information security.

**DMZ** – Demilitarised Zone. A firewall configuration for allowing visibility to a part of your local network.

**Encryption** - A procedure used to convert plaintext into ciphertext in order to prevent any but the intended recipient from reading that data. There are many types of data encryption, and they are the basis of network security.

**Firewall** – systems used to prevent unauthorised access. The firewall may be hardware, software or both.

**Firmware** - Software stored in the computers read only memory (ROM) and cannot be easily changed.

**FTP** - File Transfer Protocol. A protocol which allows a user on one host to access, and transfer files to and from, another host over a network.

**Hardware** - The physical equipment of a computer system, including the monitor, keyboard, central processing unit, and storage devices.

**HTTP** - Hyper Text Transfer Protocol; the WWW protocol that performs the request and retrieve functions of a server. Commonly seen as the first part of a website address.

**Internet** - An interconnected system of networks that connects computers around the world via the TCP/IP protocol.

**IP address** - Internet Protocol Address. It is a series of four numbers between one and three digits in length, numbers separated by periods. It is used to identify a computer connected to the Internet. For example, 212.6.125.76 is an IP address.

**IP spoofing** – using a legitimate IP address or packet to gain unauthorised access to a computer

**ISP** - Internet Service Provider. A company that provides an Internet connection.

**LAN** - A local area network (LAN) is a computer network covering a local area, like a home, general practice or small group of buildings such as a health centre. The topology of a network dictates its physical structure.

**Malware** - Malicious code in the form of viruses, worms, and Trojan Horses.

**Modem** - This is short for modulator-demodulator devices. Modems allow computers to transmit information to one another via an ordinary telephone line

**Network gateway** - A network gateway is an internet working system, a system that joins two networks together. A network gateway can be implemented completely in software, completely in hardware, or as a combination of the two.



**Packet** - A bundle of data organized for transmission, containing control information (destination, length, origin, etc.) the data itself and error detection and correction bits.

**Patches** - Upgrades for software supplied by manufacturers such as Microsoft usually over the Internet.

**Port** - In a communications network, a port is a point at which signals can enter or leave the network en route to or from another network.

**Protocol** - A formal description of message formats and the rules two computers must follow to exchange those messages.

**Router** - An electronic device that connects two or more networks and routes incoming data packets to the appropriate network.

**Rulebase** - Component of logic system that specifies the meanings of the well-formed expressions of the logical language.

**Ruleset** - A rule set contains an ordered group of configured rules which are sequentially tested.

**SMTP** - Simple Mail Transfer Protocol - the protocol used to transfer e-mail.

**Software** - A program or set of instructions that controls the operation of a computer. Distinguished from the actual hardware of the computer.

**Spam mail** - The Internet version of junk mail. Spamming is sending the same message to a large number of mailing lists or newsgroups usually to advertise something.

**Spyware** - Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes

**Stateful inspection** - Also known as dynamic packet filtering, stateful inspection is a firewall architecture that provides enhanced security by keeping track of and examining both incoming and outgoing packets.

**Trojan Horse** - A malicious non-replicationg program disguised as legitimate software.

**Virus** - In computer security technology, a virus is a self-replicating program that spreads by inserting copies of itself into other executable code or documents

**VOIP** - Voice Over Internet Protocol. Using the internet protocol to carry voice data. Depending on the scenario VOIP can facilitate cheap or even free phone calls.

**VPN** - Virtual Private Network. A private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunnelling protocol and security procedures

**VPN IPSEC** - Internet Protocol Security is an internationally recognised VPN protocol suite developed by the IETF (Internet Engineering Task Force).

**Worm** - A computer worm is a self-replicating computer program, similar to a computer virus. A virus attaches itself to, and becomes part of, another executable program; however, a worm is self-contained and does not need to be part of another program to propagate itself.

General Practice Computing Group  
C/- Royal Australian College of General Practitioners  
1 Palmerston Crescent  
South Melbourne, Vic 3205  
Tel: (03) 8699 0414

[www.gpcg.org.au](http://www.gpcg.org.au)