

An introduction to client firewalls

A Sophos white paper

March 2006

Increased connectivity in and out of the office has radically changed the task of securing an organization's systems and data. Client firewalls – often referred to as “personal” firewalls – are now an essential part of corporate endpoint security. This paper describes what a personal firewall is, why it is important, and how it differs from a gateway firewall.

Today's business environment is no longer one of office-bound workers using desktop computers permanently attached to a network with well-defined parameters. In that environment a diligent network administrator could keep the company's network more or less effectively protected through a combination of good practice, a gateway firewall and up-to-date anti-virus software. Today, common laptop use and ubiquitous internet connections (through hotel broadband connections, wireless hotspots, internet cafés and so on) have changed all that. Corporate laptops and remote desktops are routinely connected directly to the internet to browse the web, to send and receive email and to access the office network.

The increased vulnerability that this connectivity brings to an organization is matched by the changing nature of the threats themselves. The speed with which new threats are created and spread through the internet makes end users' computers more vulnerable than ever to a range of new and old threats. Not only are they still under threat from “traditional” viruses, they are also subjected to intrusion from hackers, can have Trojans and spyware downloaded on to them, and can be infected by internet worms. They can also be hijacked and used, for example, as spam or porn servers or to carry out denial of service attacks on other company's websites and email servers. In short, personal firewalls have become an important and necessary component of endpoint security.

What is a personal firewall?

In general terms, a firewall is software or a hardware device which controls the flow of traffic between two networks or entities. In the case of a personal firewall, it controls the network traffic between a computer on one side, and the internet or corporate network on the other side.

Gateway firewalls have been around for many years, but personal firewalls are a relatively recent development. Although at the highest level their roles are similar – to provide a layer of defense against the internet – there are clear distinctions between them.

A **gateway firewall** normally runs on a dedicated network device or computer positioned on the boundary of the corporate network. It is primarily used to deny unauthorized access to or from a corporate network.

A **personal firewall** runs on individual computers and while the primary role is still simply to deny unauthorized access to that computer, a good personal firewall also generally monitors

A personal firewall controls the network traffic between a computer on one side, and the internet or corporate network on the other side.

which programs attempt to initiate outbound network or internet communications. It can then either alert the user or block the traffic when suspicious or unauthorized activity occurs. This is particularly useful in preventing worms from infecting computers via unused network ports, and in preventing spyware or other types of malware from sending any information over the internet.

Why enterprise laptops and desktops need a personal firewall

Remember that, in talking about firewalls, we are talking about internet and network connections – and, to communicate over a network, applications' need for open “ports” on the computer. These open ports make the computer vulnerable to hackers, internet worms and so on. A port represents a potential access point to the computer from the network, and the port number typically (but not always) identifies what type of port it is, i.e. what it is used for. For example, port 80 is the standard port used for inbound HTTP (web) traffic.

Ports can be open or closed. An open port means there is a service that sends information to or accepts input from the

network, like browsing, Windows file sharing, FTP, etc. Closed ports do not accept any communication. When a computer is connected to the network it can be probed or scanned to see what services it “offers”, i.e. which ports are open. Open ports can be exploited not just by a worm accessing a service on the computer to install itself, but also through hackers trying to get access to the computer. They can also be used by applications such as Trojan horses or adware/spyware to send information to third parties over the internet. In the same way that unlocked windows in a building provide an easy way for intruders to get in and out, unsecured ports on a computer can act as an open invitation to spammers, hackers and the like.

Today's personal firewalls don't just block access to specific ports – they can also allow or restrict access to the internet by particular applications.

So this is how the worms, hackers etc manage to get on to the individual computers. But why does the gateway firewall or anti-virus and anti-spam software on the email server not stop the threats before they get on to the network? If anything does get past the gateway, why doesn't anti-virus software on the desktop or laptop block the threat? Why is a personal firewall needed? The reasons are:

- 1 Internet worms like Blaster or Slammer spread by exploiting vulnerabilities in operating systems or applications. They can spread globally within a matter of minutes, making it possible for them to infect a network either before the operating system vulnerabilities can be patched or before specific anti-virus detection is available and deployed across the enterprise. In blocking all unauthorized access to the computer from the internet, a personal firewall blocks attempts by a new internet worm to infect a computer before new virus signatures are available to detect and remove it. A personal firewall also helps in situations where a worm is memory resident and never writes to a file (where anti-virus software usually operates).
- 2 Today's mobile business computers are not always protected by the gateway firewall because they are connected to the internet through hotel or internet café facilities, making local protection essential.

How a personal firewall works

Overview

A personal firewall protects individual computers – and by extension the whole corporate network – by blocking access to

the computer from the internet and by limiting which applications can communicate with the internet (and the network).

It does this in two ways:

- 1 It blocks access to specific ports, specific protocols, or port and protocol combinations, hiding the computer from view from other network and internet users (i.e. preventing hackers from gaining access to a computer).
- 2 It controls which applications are allowed to communicate to or from the computer (i.e. preventing worms from infecting/spreading over the network).

Early versions of personal firewalls did only the first of these, i.e. they simply blocked all access to particular ports. Today's personal firewalls are much more flexible and can allow or restrict access to the internet by particular applications. Algorithms within the software can also be used to check that an application really is what it purports to be, thus preventing substituted programs from communicating from the computer.

The personal firewall uses a set of configurable rules to determine whether or not it will allow an application to communicate with the internet. It detects which applications are trying to communicate, compares these with its rule set, and stops prohibited applications from communicating. Therefore, most personal firewalls – although not the Windows Firewall (see note at end of paper) – also prevent the computer from sending out malware over the network, stopping Trojans and similar applications from spreading or generating network traffic. The more flexible personal firewalls can allow a trusted zone for more relaxed network access, e.g. they can be configured to ban access to suspect internet sites.

It is important to note that the firewall detects and controls the **communications mechanisms** which might open the computer to the vulnerabilities of viruses, Trojans, worms, spam, spyware, and so on, i.e. it offers generic protection: it is not responsible for the specific detection of particular threats. A useful way of thinking about it is that anti-virus software blocks threats based upon **what** is transmitted, whereas a firewall blocks threats based upon **how** they are transmitted.

Technical detail

Packet filtering

The process by which personal firewalls monitor the traffic going in and out of the computer is known as “packet filtering”. Data travelling on a network is split into packets which use the TCP/IP (Transmission Control Protocol/Internet Protocol) network architecture. Each packet has a header which contains the source address (the IP address of the source computer and the relevant port number) and the destination address (the IP address of the destination computer and the relevant port number). The rest of the packet contains the actual data. The

TCP/IP protocol is used to establish the connection between the source and destination.

Static packet filtering

In “static” packet filtering, a personal firewall controls access to a network by analyzing the incoming and outgoing packets and letting them pass or blocking them based on the IP addresses of the source and destination. Static packet filtering uses the information in the header, applying the firewall’s set of rules, in order, until a packet matches one of the rules. Each packet is filtered independently and in both directions, but each direction has its own set of rules.

The successful implementation of personal firewalls is now essential to administrators’ ability to achieve complete endpoint security.

Typical inbound filtering checks:

- The source address to ensure that it has not been spoofed or is not unauthorized, and will limit incoming traffic to selected remote hosts
- The destination port to defeat probes and scans.

Typical outbound filtering checks:

- The source address to verify the source IP address and port number
- The destination address and port checking to restrict access to unauthorized addresses.

Note that Windows Firewall does not perform outbound filtering.

Dynamic packet filtering/stateful inspection

Nowadays most personal firewalls go further than this static packet filtering, using what is known as “dynamic” packet filtering or “stateful inspection”, a term coined by Check Point Software in the use of its FireWall-1 in 1993. A stateful firewall examines not just a packet’s header information but also its contents in order to determine more than its source and destination. It also monitors and maintains information about the state of the TCP/IP connection and compiles the information in a state table. This “optimization” allows administrator-defined rules to be bypassed if the context is recognized as part of an ongoing, previously allowed exchange. As an added security measure against port scanning, stateful inspection firewalls close off ports until connection to the specific port is requested.

Summary

The easy access to the internet, which has opened up many benefits to corporations and end users, has also created a number of vulnerabilities, requiring a multi-tier approach to security. The complicated nature of today’s IT infrastructure and the complexity of rapidly evolving new threats have increased that vulnerability. The need for anti-virus software to provide protection against many of these threats has never been greater, but the speed at which operating system vulnerabilities are discovered and exploited, the speed at which new viruses and worms spread, and the ever-increasing threat from hackers, has made the use of personal firewalls on desktop and laptops extremely important. Personal firewalls have become an essential component in the network administrator’s armoury in achieving complete endpoint security.

Note: The Windows XP Firewall

Windows XP contains an integrated personal firewall. Until Service Pack 2 (SP2), however, the firewall was not enabled by default and left several ports open and exposed to the internet.

Windows XP Service Pack 2, which was released by Microsoft in late 2004, addresses some of the security vulnerabilities in Windows XP, but the need for a more robust third-party personal firewall remains. If XP SP2 detects that a third-party firewall exists, it will turn off its own firewall. The problem with the Windows Firewall is that, while it provides a defense against threats coming in from outside, it does nothing about infections already on the computer, or that manage to get through and install themselves despite the user’s best efforts. So if, for example, the computer became infected by a worm, that computer could become a base for flooding the internet, and the local network, with worm traffic. Third-party personal firewalls, including Sophos Client Firewall, would block the outgoing threat as well as any incoming threats.

About Sophos

Sophos is the world leader in integrated threat management solutions purpose-built for business, education and government. Our reliably engineered, easy-to-operate products protect over 35 million users in over 150 countries. Through 20 years' experience, combined in-house anti-virus and anti-spam expertise, and a global network of threat analysis centers, we respond rapidly to emerging threats – no matter how complex – and achieve the highest levels of customer satisfaction in the industry.

Boston, USA • Mainz, Germany • Milan, Italy • Oxford, UK • Paris, France
Singapore • Sydney, Australia • Vancouver, Canada • Yokohama, Japan

© Copyright 2006. Sophos Plc.

*All registered trademarks and copyrights are understood and recognized by Sophos.
No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form
or by any means without the prior written permission of the publishers.*

SOPHOS
WWW.SOPHOS.COM