



NISCC

NATIONAL INFRASTRUCTURE SECURITY CO-ORDINATION CENTRE

**NISCC Viewpoint 02/2006
Issued 31 March 2006**

Firewalls

A firewall separates two regions of an IT system, restricting the traffic that can pass between them. This Viewpoint describes the different types of firewall and provides a brief overview of the scope and limitations of a firewall.

NISCC Viewpoint papers are intended to provide an overview of emerging technologies and other issues facing the IT sector. A Viewpoint will not necessarily offer mitigation advice; other NISCC products do this. Although this Viewpoint is intended as a basic guide for non-technical decision makers, it does contain some technical content. Additional information for specialists is available in NISCC technical note 10/04, "Understanding Firewalls".

**National Infrastructure
Security Co-ordination Centre**
PO Box 832
London, SW1P 1BG

Tel: 0870 487 0748
Fax: 0870 487 0749
Email: enquiries@nisc.gov.uk
Web: www.nisc.gov.uk

Firewalls

1. If asked to name a device used for computer security, the most popular answer would undoubtedly be 'a firewall'. But what can we expect from a firewall? What can a firewall do, and – just as important – what can't it do? What types of firewall are available, and what makes some of them expensive? This NISCC Viewpoint briefly covers all of these questions. The most important message it contains is 'a firewall is only as good as its configuration'.

2. Network traffic can be described at the lowest level by the IP addresses of the two endpoints, the ports of the two endpoints, and the packet type (e.g. UDP, TCP). Higher level protocols are layered on top of these basics; for example DNS is built on top of UDP, while HTTP is TCP based. In some cases there are several layers in the protocol stack; for example the Simple Object Access Protocol (SOAP) is usually implemented using HTTP as the transport.

3. Encrypted protocols are particularly difficult to control adequately, as the firewall is not able to check the content of the data stream. It is sometimes possible to enforce tight controls on the identities of the parties in encrypted transactions by using authentication, but these controls must be enforced at the endpoints, and the firewall is little help.

4. Any firewall is potentially vulnerable to denial of service attacks caused by simple volume of traffic; this may result in the effective isolation of the two networks. In some cases the impact of this can be reduced by implementing additional filtering rules upstream, so as to reduce the hostile traffic at the earliest possible points. More sophisticated denial of service attacks exploit features of the protocols (or defects in implementation) to disrupt service using modest amounts of bandwidth.

5. Most firewalls can generate logs of traffic in greater or lesser amounts of detail. Everybody would agree in principle that these should be routinely inspected, but this rarely happens. Sadly, the commonest practical use of firewall logs is as part of a forensic investigation after an incident has occurred.

6. There are two broad classes of firewall – hardware and software.

Hardware firewalls

7. A hardware firewall is an appliance that connects to two (or sometimes more) network segments, and restricts traffic flow between the networks. The simplest type is called a packet filter, and allows rules that specify which packets can travel between specific endpoints, based on the packet type and the source and destination addresses and ports. This sort of rule can be implemented by any modern router, but it has the limitation that each packet is considered in isolation, and there is no concept of a protocol with state (ie the possible continuations to a

sequence of packets are not modelled). Despite this limitation, packet filtering at routing devices is still valuable, as it can reduce the volume of traffic that more sophisticated devices need to handle.

8. More sophisticated firewalls have a deeper understanding of the protocols, so that they can apply stricter tests on the incoming and outgoing data. Even if the data is well formed, it may be unwanted; perhaps because it carries a virus or other malware, or is spam e-mail. Some firewalls integrate additional protocol specific payload checking, such as virus or spam checking. Many of these tests depend, to a greater or lesser extent, on the use of signatures to detect known types of threat. These signatures need to be kept up to date, and cannot offer protection against newly discovered threats until an appropriate signature can be created and circulated.

9. An alternative architecture moves some of the protocol specific checking to servers inside the firewall; for example virus and spam-filtering may be performed on the mail server. It is important to understand what a given firewall can check, and add supplemental filtering elsewhere in the system when needed.

10. In general, there is a three way trade-off between the strength of the filtering, the speed of the device and its cost. Devices which have been certified to a high level in the [Common Criteria](#)¹ scheme tend to command a price premium.

Software firewalls

11. Software firewalls are installed on the computer to be protected, and limit the connections that are allowed between applications running on the computer, and the network (or networks) the computer is connected to. It is possible for a software firewall to identify which application wishes to make a connection, to send data or to receive data. This means that rules can be formulated that specifically permit certain applications to connect to particular ports, while excluding all unregistered ones. For example, access to the local mail server could be restricted to an approved e-mail client.

12. A major drawback of software firewalls is that they run on the same hardware as the applications they seek to control and protect. This means that even a denial of service attack that is entirely blocked by the firewall consumes resources on the same platform as the applications to be protected, and may render them unacceptably slow.

13. Software firewalls are highly privileged components, and often form part of the operating system kernel, where there are no effective access controls. This means that exploitable defects in the firewall itself will generally lead to complete system compromise.

¹ See www.commoncriteriaportal.org

14. The use of software firewalls by themselves on important machines is not usually recommended but they are very useful as a supplement to hardware firewalls, as they can implement additional controls at the level of individual applications, and provide an additional level of protection to give defence in depth. Software firewalls can be configured to restrict which other computers within a network can be accessed, which would otherwise require an impractical number of a hardware firewalls.

Limitations of all Firewalls

15. Firewalls are not perfect. Bugs inevitably exist in anything as complex as a firewall, and some of these bugs will be exploitable vulnerabilities. If defects are discovered, you will need to upgrade your firewall. With firewall devices, this often means upgrading the firmware.

16. **A firewall is only as good as its configuration.** The rules should allow those protocols through that are needed, and no more. One common problem is that special rules to allow additional access get added temporarily as a work-around or for a short term project, and are then never removed. When services or machines are no longer needed, the configuration is not always tightened to remove the now redundant access. The defect is not apparent, as permitted services still continue. This is the basic difficulty in firewall maintenance – when things fail open, nobody notices. Good processes for configuration control can help reduce these problems.

17. Strict configuration control should be enforced on firewalls because they are one of the key defences of a system. When significant changes are made to the configuration, the new settings should be tested. Ideally, this testing should take the form of penetration testing by an independent team, who will be able to see if they can reach systems or services that are not intended to be accessible. The configuration data should be stored and protected like any other business continuity data, as it may be necessary to recreate the same configuration after hardware failure or some bigger incident.

18. Even if a firewall has been configured correctly, and works as intended, it cannot offer complete protection. All it can hope to do is restrict the nature of the threat to those protocols that are actually needed. Threats that are carried by well formed traffic in the permitted protocols will pass through the firewall. A common example is e-mail; a firewall may indeed restrict connections so that only legitimate e-mail traffic enters the network, but will not be able to stop a harmful payload being carried by an attachment unless it examines attachments and can distinguish good and bad.

19. A common mistake in configuring firewalls is to concentrate exclusively on the threat from outside, and to assume that traffic originating inside the firewall is automatically legitimate. This is not a safe assumption anymore, as viruses, trojans, key-loggers and other malware may attempt to send valuable data out through the firewall, often by using mainstream protocols. Common examples include e-mail

viruses that send well-formed mail messages, and various remote control payloads that use Internet Relay Chat (IRC) to establish a control link with a remote machine, making the compromised machine into a “zombie”. Firewall rules should certainly constrain outgoing protocols to those that are actually needed from specific machines.

20. Protocols that allow Remote Procedure Calls (RPC) need to be very tightly controlled if they are allowed at all. Examples of such protocols include DCE RPC, Java RMI, DCOM, CORBA and SOAP. SOAP is particularly worrying, as it uses HTTP as a transport, and many firewalls need to allow HTTP traffic through for legitimate business reasons. Simple HTTP filtering rules, such as those used by a packet filter which allows connections on port 80, will allow SOAP through as well. More sophisticated firewalls can detect SOAP traffic (there are some SOAP specific headers, and it has a distinct Mime-Type), and apply specific rules to it, or even block it entirely if it is not needed. There are also now a variety of SOAP specific firewall products which make it possible to enforce fine grained application level rules. There are a much smaller number of firewall products for the other RPC protocols, and system architects should think long and hard about the wisdom of exposing such protocols outside the protected part of the system.

21. Firewall administrators, like any security administrators, have to be trusted absolutely. Their technical competence must be trusted, and their loyalty to the organisation must be beyond question. For highly critical systems, it may be worthwhile to set up procedural controls, where two administrators routinely check one another’s work.

22. A correctly configured firewall forms part, but only one part, of the defences of a system. The best that can be hoped for is to reduce the avenues of attack to the minimum consistent with delivering necessary services. Firewalls can never be a panacea, and their presence can induce complacency that leads to neglect of other vital measures, or toleration of risky behaviours by system users. System administrators, users and policy makers all need to understand the residual risks in a system with even the best maintained and configured firewall and behave responsibly in the face of those risks.

This paper was produced for NISCC by QinetiQ

About NISCC

The role of NISCC is to minimise the risk to the Critical National Infrastructure from electronic attack. NISCC was set up in 1999 and is an inter-departmental centre drawing on contributions from across government. Defence, Central Government Policy, Trade, the Intelligence Agencies and Law Enforcement all contribute expertise and effort. Further information can be found at www.niscc.gov.uk



National Infrastructure Security Co-ordination Centre

PO Box 832

London, SW1P 1BG

Tel: 0870 487 0748

Fax: 0870 487 0749

Email: enquiries@niscc.gov.uk

Web: www.niscc.gov.uk

About QinetiQ

QinetiQ is one of the world's leading defence technology and security companies.

For further information please call us on 08700 100 942 or refer to our website: www.QinetiQ.com

