Firewall implementation at Janet-connected organisations

Matthew Cook, Loughborough University

Authors and Contributors

This document was put together by Loughborough University to share knowledge, experience and current trends surrounding firewall implementation with the JANET community. This Technical Guide is complemented by the JANET Training programme which provides courses covering multiple facets of firewall implementation as part of their extensive portfolio.

The primary author is Matthew Cook who has been a member of the Computing Services department at Loughborough University since 1999. He has an extensive knowledge of a wide range of operating systems and networking technologies and has spoken at many conferences on various security matters. These presentations, papers and lectures are available at: http://escarpment.net/ [1].

Other contributions and editing came from Gill Chester, Andrew Cormack and Katharine Iles of JANET.

Readers are assumed to have a basic knowledge of networking concepts and preventive security awareness. A companion *Security Matters* [2] guide is available.

References to particular products do not imply any recommendation.

Scope and Audience

The Internet is a double-edged sword: it is an excellent technology for communication and collaboration, but at the same time threats are created by this connectivity. Tools to protect against malicious and otherwise unwanted network traffic began to be developed very early in the history of the Internet. Firewalls to filter traffic are now a key part of any modern day network infrastructure and the concept has extended from a system administration term into everyday vocabulary.

Firewalls can be employed at different locations on the network, and in different configurations. Understanding what each of these can (and cannot) achieve is essential to procuring and managing the right firewall system(s) to address a particular set of requirements. This Technical Guide surveys the theory and technology behind the implementation of firewalls on campus LANs of JANET-connected organisations. This Guide is aimed at the staff responsible for the implementation of an IT security policy in these organisations, of which a firewall is a single, but critical, part. Understanding the detailed functions of any firewall system is essential to its successful operation and continued

maintenance. A firewall is a long term investment, with most solutions installed for approximately three to five years. Moreover, in addition to the technical issues, consideration needs to be given to customer support, documentation and training.

The Threat of the Internet

The Internet is growing at an exponential rate: the number of people connected to the Internet was recorded as 1,086 million by the Internet World Statistics organisation on 18 September 2006 (http://www.internetworldstats.com [3]**)**.Of course, it is difficult to ascertain the accuracy of such a number, but it gives an idea of the sheer volume. Moreover, this estimate was based on the number of IP addresses in use, so may have been distorted by the use of NAT and PAT technologies which can conceal many computers and people behind one or a small pool of real-world IP addresses.

With the increasing number of people and computers connected to the Internet, the danger from Internet-based threats also rises, for a number of reasons. The Internet becomes a more attractive arena for malicious activity because there is a higher target population, with an increased dependency on the technology and greater variety of connected devices, but less specialist knowledge of how to deal with the risks. In addition, there are far more people actively working on malicious code for personal or financial gain.

It is easy to see why it is essential that threats to a local IT infrastructure are managed effectively. It is a serious incident if a computer is compromised and backdoors installed, but this also creates the possibility of theft of credit card details and access to Building Management Systems, remote IP surveillance cameras and a whole host of information stored on local information systems. Apart from the potential harm to staff and property, the obvious public relations issues and media reporting of the issue, there will be significant staff time involved executing disaster recovery plans.

A simple DoS attack which prevents users reading their e-mail may be manageable for a few hours, but prolonged outage will become mission-critical very quickly.

With the increased dependency on information systems in a culture of online learning and 24/7 access, it is critical that a well-implemented firewall is part of any organisation’s overall IT security policy.

What Does a Firewall Protect Against?

A firewall provides a level of protection from network-based attacks by allowing good traffic and denying bad traffic as defined by a security policy.

In normal operation the firewall allows a user to carry out usual IT activities (sending and receiving e-mail, web browsing, file transfer) but also prevents unauthorised access to these systems, DoS attacks and sometimes Peer to Peer file sharing. What services users can and cannot access depends on the local IT policy.

Any machines connected to the Internet will be vulnerable to repeated attacks; recent research has shown that attacks can happen as frequently as every minute. Scanning attempts to establish what weaknesses exist in computer systems. Malicious network worms

and malware popups are just some threats a firewall can protect against.

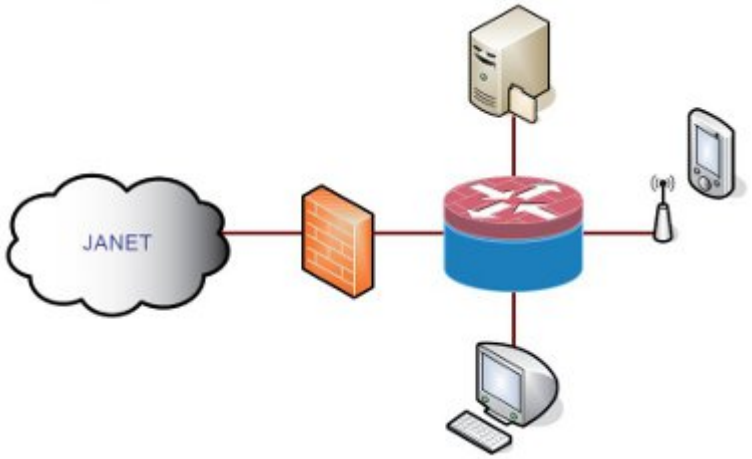
Firewall rules are commonly based upon the TCP/IP suite of protocols. The security policy to be implemented is written as a set of rules which apply restrictions to a block of network addresses (a netblock) and to a protocol and transport. The rules could be very generic (no FTP), or very specific (no FTP inbound from host 192.168.1.10). One small error in the firewall rules could leave systems without protection or, alternatively, block all access to an essential service.

Traditionally, firewalls have been installed at the gateway to the organisational network. This methodology has been the standard for a long time, but is starting to become a minimum configuration. Threat propagation within the LAN is increasing, to which the UK Higher and Further Education communities are particularly vulnerable.

[4]

Figure 1: A typical organisational firewall implementation

To provide a more comprehensive protection policy, firewalls can be installed between different network segments or VLANs by adding hardware firewall cards to network switches a[illegible]t best thing is a set of router ACLs.



[5]

Figure 2: Protecting internal networks with multiple firewalls or firewall modules

One of the key problems facing network administrators is the growing population of mobile IT users. Laptop or Portable users can bring a computer that is infected with a network worm into the organisation, connect it to the LAN and bypass all the firewall defences installed at the perimeter. With the drive for increased provision for ubiquitous computing, this creates another IT security issue to consider.

Defence in Depth

Defence in depth was originally used to describe multiple levels of defensive lines, fortifications and barriers to attack which were employed in a military context. The term is now

synonymous with IT security theories. Providing multiple levels of protection can enhance the overall security of an organisation instead of relying simply on one system, such as a firewall.

Following the defence in depth principle would suggest the implementation of firewall technology at the ingress points to an organisation's network, such as the traditional Internet connection, wireless networks, backup routes, extranet mobile devices or anywhere that external Internet connectivity is possible. This defence can be further enhanced with the introduction of a cleaner feed from a first tier device or multiple firewalls. Moreover, firewalls should be employed alongside other security systems, including IDS, IPS and content filters, which should also provide warning information and feedback.

In addition, multiple vendor technology can be used to provide enhanced protection. If there are security issues with a product from a particular vendor, then this is an obvious risk until a patch or work-around is released. With protection from two different vendors, the defence is increased as the same issue will not usually be a vulnerability in both.

Servers and desktop computers also should adhere to the same security policy, and antivirus/ malware should be installed on all computers. Servers should have their operating systems hardened and should ideally run different anti-virus software to the desktop computers. Services installed on the servers should be sandboxed and configured to mitigate machine compromise.

Firewall or Router ACLs?

As many active network devices such as routers and switches include ACLs, it can seem at times that firewalls are redundant. However, firewall rules and router ACLs are not equal in functionality.

Network router ACLs are not a replacement for a firewall implementation, but can complement the security of the network. They can implement simple packet-blocking rules at high speeds and, depending on the hardware, can be applied in hardware ASICs for increased performance.

However, ACLs on network devices create additional load on the router or switch which will degrade performance. Another consideration is the limited logging space and flexibility available. In addition, they cannot provide packet inspection at higher levels.

History of Firewalls

Packet filters seem to be first mentioned in connection with the Xerox Alto operating system in 1976, followed by implementations on the UNIX® platform in the early 1980s.

A paper by J Mogul et al, *The Packet Filter: An Efficient Mechanism for User-level Network Code*, published in 1988, finally realised the usefulness of the firewall concept (http://www.hpl.hp.com/techreports/Compaq-DEC/WRL-87-2.pdf [6]).

Later that year, the Morris Worm created by Robert Morris of Cornell University is reputed to be the first Internet worm. It made use of the computer systems of MIT and was designed to gauge the size of the Internet. The academic merit of such an activity was questionable in the

first place, and the flawed architecture of the code created an even bigger problem. The code could install itself on a system multiple times and therefore render the system unusable — a primitive but effective DoS attack. The author had foreseen that checking if the code was already present on a system would provide an easy and effective mechanism for defence and therefore decided to design it to replicate regardless 14% of the time. With the worm exploiting known vulnerabilities in Sendmail, FingerD and RSH privileges, it spread at an alarming rate. This highlighted an issue with network security and led to the further development of firewalls as we know them today.

The early firewalls, although basic, still form the cornerstones of the technology as used today. Development by AT&T Laboratories and Gene Spafford of Purdue University created the second generation of circuit level and application layer firewalls.

The first reported commercial implementation of a firewall came out of the work of Marcus Ranum and was released by the Digital Equipment Corporation as the SEAL product. Later development focused on dynamic packet filtering which formed part of the first commercial offering from Check Poinr® in 1994.

Development of dedicated Kernel Proxy architecture firewalls resulted in the release of the Cisco Centri Firewall in 1997. The Kernel Proxy architecture uses the concept of network sessions to dynamically construct a stack for the session and its specific protocol. Firewall development is constantly evolving and incorporating more and more features. Firewalls including IPS and mitigation technology are becoming commonplace.

Links
[1] http://escarpment.net/
[2] http://community.ja.net/library/janet-services-documentation/security-matters-technical-guide
[3] http://www.internetworldstats.com/
[4] http://community.ja.net/system/files/images/firewalls-tg-01.jpg
[5] http://community.ja.net/system/files/images/firewalls-tg-02.jpg
[6] http://www.hpl.hp.com/techreports/Compaq-DEC/WRL-87-2.pdf