Firewall rules and logging

Good Practice

All firewalls work on the premise of rules configured to implement the site security policy. Rules are so critical to the operation of the firewall that it is vital they are fully understood before a firewall implementation is deployed.

The most important thing to remember is that firewall rules are processed in sequence. When a packet is analysed it is checked against each rule in turn until it finds a match or reaches the end. If the firewall finds a match the action defined is executed: this could be allow or deny with the option to log. If no match is found then the default action of the firewall is executed. The default action is, again, allow or deny, depending on the firewall configuration. It is good practice to define an explicit allow or deny at the end of each rule set.

It is important to optimise the rules so that as few rules as possible are checked before a hit is made. However, exceptions need to be placed before explicit deny rules. For example, to block all outgoing HTTP traffic except that from the web caches, a rule would be written to drop all outgoing HTTP. This would, initally, block all traffic including that from the web caches. An additional rule would need to be added before the default deny to ensure traffic from the IP addresses assigned to the web caches is allowed.

IP addresses should be used instead of DNS hostnames, as it is easy to subvert DNS queries to undermine the firewall rules. It is important to ensure that when the firewall rules have been changed they are completely reloaded to ensure there is no conflict with previous rules.

It is critical that rules are as specific as possible to ensure that correct packets are matched and the number of false positives is kept to a minimum. The best advice is to block everything at first and then open holes to increase functionality one step at a time.

Regulations and Guidelines

The Data Protection Act

There are two elements of firewall implementation where the DPA 1998 [1] specifically applies:

- If an IP address can identify an end user then the storage of logs is subject to the DPA.
- It is possible that content of communications may be revealed with Layer 7 inspection.

This is regarded by the law as well as by users as more of an intrusion and will therefore require a stronger justification.

If the content of packets may be revealed or recorded, laws governing interception are also likely to apply, in particular the Regulation of Investigatory Powers Act 2000 [2].

The implementation of a firewall as part of a complete IT security policy will go some way to ensuring that the seventh principal of the DPA is addressed:

> ‘Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data’.

At present there is very little case law to determine ‘appropriate measures’. However, taking steps to provide an effective firewall is a good move forward.

ISO/IEC standards

The standards ISO/IEC 17799:2005 and ISO/IEC 27001:2005 provide a comprehensive collection of information security good practice advice.

Previously known as BS7799, the standards have been updated and revised. BS 7799 Part 1 was updated in June 2005 to become ISO/IEC 17799:2005. Seventeen controls were added while others were deleted and merged to give a total of 133 information security controls. This document will be re-released in April 2007 as ISO/IEC 27002:2007.

BS7799 Part 2 was revised in 2005 as ISO/IEC 27001:2005 and defines a framework for an Information Security Management System. This can be used to design, monitor and control security policies and rules within an organisation.

BS ISO/IEC 27001:2005 does not specifically refer to firewalls, but to a number of controls concern policies that would affect the operation of a firewall system. These include controls relating to the isolation of networks and systems which would be difficult to implement without the use of VLAN technology, router ACLs or firewalls. The purchase and installation of a firewall will not cover all the suggested controls in BS ISO/IEC 27001:2005. However, it can be used as a tool in the organisational information security policy to mitigate risk.

Blocking Common Threats

There are many Internet-based threats to network security, but there are some that every organisation should be blocking. Examples of possible rules are given in the NetFilter/ IPTables format (see 2.4.2).

With a default deny firewall, it is less critical to ensure all malicious attack vectors are protected against as they will be blocked inherently. However, if there is not a default deny rule in place, the rules necessary to implement the organisation’s security policy will need to be considered carefully.

Stealth TCP Scans

Port scanning activity is common, with many different methods used in attempts to subvert firewalls, IDS and IPS. Blocking undesirable combinations of TCP flags can counteract this:

iptables -A FORWARD -p tcp --tcp-flags ALL NONE -j DROP

iptables -A FORWARD -p tcp --tcp-flags SYN,FIN SYN,FIN -j DROP

iptables -A FORWARD -p tcp --tcp-flags SYN,RST SYN,RST -j DROP

iptables -A FORWARD -p tcp --tcp-flags FIN,RST FIN,RST -j DROP

iptables -A FORWARD -p tcp --tcp-flags ACK,FIN FIN -j DROP

iptables -A FORWARD -p tcp --tcp-flags ACK,PSH PSH -j DROP

iptables -A FORWARD -p tcp --tcp-flags ACK,URG URG -j DROP

OS Fingerprinting

Crackers using port 0 fingerprinting can be prevented from identifying hosts on the inside network using the following code:

iptables -A FORWARD -p tcp --dport 0 -j DROP

iptables -A FORWARD -p udp --dport 0 -j DROP

iptables -A FORWARD -p tcp --sport 0 -j DROP

iptables -A FORWARD -p udp --sport 0 -j DROP

Protocols

There are a number of protocols that are unlikely to be used across the Internet and therefore can be blocked at the organisational firewall:

- Net BIOS/SMB/CIFS – TCP/UDP 135-139 and TCP 445
- Microsoft® RPC over HTTP – TCP/UDP 593
- BootP/DHCP – TCP/UDP 67 and 68
- SNMP – TCP/UDP 161and 162
- NFS – TCP/UDP 2049
- Microsoft® SQL – TCP 1433
- MySQL – TCP 3307
- LPD – TCP 515
- TFTP – UDP 69
- Simple UNIX Services (TIME, CHARGEN etc)

Blocking ICMP

ICMP is a straightforward method for transporting communication messages and errors. As with many of the Internet protocols, it has been abused over the years and the original

purpose subverted. ICMP is used regularly for DoS attacks, network scanning and tunnelling other communications.

Whether ICMP should be blocked is a hot topic of debate for network administrators. Some consider ICMP an essential part of network diagnostics and should therefore be allowed, while others believe it opens an undesirable security hole.

One compromise is to rate limit ICMP and only allow certain packet types. ICMP fragmentation is seldom seen outside a malicious attack, so it is recommended to block these packets explicitly, and allow only ICMP echo-reply, echo-request, time-exceeded and packet-too-big (these are required, respectively, for the **ping** command, traceroute and MTU discovery).

iptables -A FORWARD -p icmp --fragment -j DROP

iptables -A FORWARD -p icmp --icmp-type echo-reply -j ACCEPT

iptables -A FORWARD -p icmp --icmp-type echo-request -j

ACCEPT

iptables -A FORWARD -p icmp --icmp-type time-exceeded -j

ACCEPT

iptables -A FORWARD -p icmp --icmp-type fragmentation-needed

-j ACCEPT

iptables -A FORWARD -p ICMP -j DROP

access-list outside deny icmp any any fragments

access-list outside permit icmp any any echo-reply

access-list outside permit icmp any any time-exceeded

access-list outside permit icmp any any packet-too-big

access-list outside deny icmp any any

access-list inside deny icmp any any fragments

access-list inside permit icmp any any echo-request

access-list inside permit icmp any any time-exceeded

access-list inside permit icmp any any packet-too-big

access-list inside deny icmp any any

access-group outside in interface outside

access-group inside in interface inside

Logging

Log files are critical to the successful management of network devices. They can be taken from network hubs, switches, routers, firewalls and almost any other network device.

Most firewalls have limited local logging so the logs need to be extracted for analysis and examination. Logs can be the only indication an attack has occurred and can provide the only information about it. It is often easier to trace problems if logs are aggregated together in the same place. This also protects against crackers removing the traces of log files when they compromise a system.

SNMP monitoring of firewalls can be used to generate logs by sending requests or receiving traps. This information can be stored in logs, sent out as alerts or graphed. Logging may not only show security issues. For example, an exhausted DHCP scope where computers are using automatic Microsoft-generated addresses is shown in Cisco PIX logging output.

Network Time Protocol

The timestamp is critical to log files, especially on systems with a high level of transactions. Accurate time synchronisation is essential to the smooth running of any server, especially if running directory services. E-mail headers can sometimes give a clue to the timezone of the originating computer system or if the clock is not synchronised by NTP then it may be possible to guess the time difference fairly accurately.

When quoting or comparing timestamps, it is necessary to know whether the system's clock is synchronised to an external reference, and what timezone the times refer to.

Note: The JANET NTP service provides this level of accuracy. Time synchronisation can be completed with one of four JANET time servers. However, it is recommended that at least two local systems are used to distribute time around an organisation instead of all computers synchronising across JANET. For further information see:

http://community.ja.net/library/janet-services-documentation/network-time-service [3]

Links
[1] http://www.hmso.gov.uk/acts/acts1998/19980029.htm
[2] http://www.hmso.gov.uk/acts/acts2000/20000023.htm
[3] http://community.ja.net/library/janet-services-documentation/network-time-service