

Case Study: Configuration Review – Firewalls & Routers
Industry Sector: Media and Telecommunications

Firewalls aim to provide organisations with reliable security at the network perimeter; however each firewall must be properly configured in order to allow and disallow network traffic accordingly, in a manner sensitive to business needs.

Poorly configured firewalls can be overwhelmingly damaging to the security of an organisation – lax ingress rules may provide multiple vectors to attackers on the Internet, while lax egress rules may provide avenues for unauthorised command and control connections from the Internet and exfiltration of intellectual property and confidential data.

Other factors must also be considered as part of a firewall configuration review, i.e.

- The software/firmware versions need to be identified in order to correlate with any publicly known issues or exploits with the specific device and version
- The network services available on the firewall also demand investigation and review against documented business requirements, including the number of registered users on the firewall and the password policies governing access to the device.

IRM's firewall configuration review provides an unbiased assessment of an organisation's firewall deployments and the traffic that is currently permitted and denied through the organisation's networks. The firewall configuration is validated against best practices in order to identify any misconfiguration that could lead to unauthorised and undesired access.

Case #1

IRM was asked to perform a firewall configuration review against a number of key perimeter firewalls of a global media corporation. The corporation had extended rapidly over a short time across multiple sites, which had led to firewall configurations having in excess of 1000 rules.

The client requested a full review to identify any extraneous rules that could be removed to improve the overall security posture of their firewalls and to streamline future management of the devices.

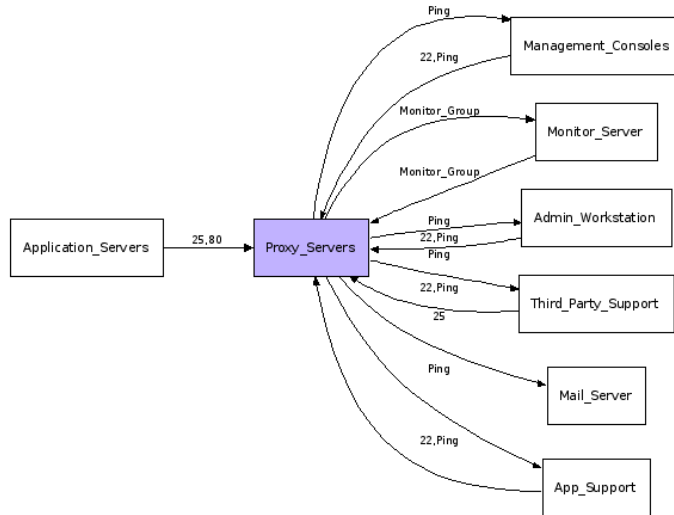
IRM employed its in-house tool PREFiRE[†] in order to assist in this domain. Visualisation of firewall rule sets in excess of hundreds of rules can be arduous and often impossible due to time constraints. PREFiRE imports firewall rule sets in their native form and produces pictorial representations of the rules and permitted connectivity through a firewall.

IRM was able to use the PREFiRE output to quickly identify the permitted traffic flows through the firewalls under investigation. This enabled rapid identification of duplicate rules, insecure protocols and protocols whose use was not documented as being a valid business requirement.

As a consequence of these core findings, the client was able to significantly reduce the number of firewall rules in operation and remove a number of permitted connections that might have been providing undesired access between networks. Furthermore it presented the client with the opportunity to update the necessary documentation sets and reduce the ongoing maintenance effort.

[†] PREFiRE - the *Pictorial Representation of Enterprise Firewall Ruleset Engine* – an IRM in-house developed tool which graphically represents the rule base of a number of firewall technologies.

An example of the output for rules governing connections between groups of servers is shown in the following image:



Case #2

IRM was asked to review the VPN parameters and tunnelling configurations between two router endpoints of a global telecommunications organisation.

A full review of the router configurations was conducted which highlighted a number of concerns. The pre-shared key was found to relate to the client name and organisation, rendering it vulnerable to password guessing attacks.

Similarly, the configuration change passwords on the routers were found to be stored using weak encryption which is readily reversed by various publicly-available tools. This issue was compounded by the observation that the routers were running with remote administration services such as telnet available on Internet-facing interfaces, providing avenues for brute force attacks against the user accounts on the routers.

IRM was able to present these issues and provide appropriate remedial advice inline with recommended best practices in a comprehensive report; this ultimately allowed the client to implement the changes and gain the necessary confidence in the security of their site-to-site VPN connections.

About IRM

Information Risk Management Plc (IRM) is a vendor-independent information security consultancy. Founded in 1998 to work alongside global enterprises in understanding the security risks inherent in an increasingly interconnected business environment, IRM has become a leader in penetration testing, risk assessment and security auditing.