

Pictorial Representation of Enterprise Firewall Ruleset Engine - PREFiRE

When reviewing firewall rulesets, it is often difficult to visualize the overall effect that firewall rules have on traffic flows through a firewall or group of firewalls. One of the most effective methods to visualize such activity is to produce a pictorial representation of the firewall rules. **PREFiRE** (Pictorial Representation of Enterprise Firewall Ruleset Engine) is an IRM in-house tool that takes as input firewall rulesets in their native output and produces pictorial representations of these text-based rules.

The aim of the output is to aid firewall ruleset reviews. The output illustrations provide a much improved view of a firewall ruleset configuration, allowing for better identification of erroneous configurations and rules that could compromise the security of the firewall and the enterprise that it seeks to protect.

Additionally, the resulting diagrams can be used to effectively communicate any issues found at a high level to a non-technical audience, which would otherwise be difficult through use of the text-based ruleset alone.

Supported Firewalls

PREFiRE currently supports two of the main firewall vendor ruleset configurations:

- CheckPoint Firewall-1
- Cisco PIX/ASA/IOS ACLs

Support for NetScreen firewalls is currently in development. Owing to the modular way in which **PREFiRE** has been developed, additional modules to support additional ruleset configurations from different firewall vendors can be created.

PREFiRE Architecture

PREFiRE is capable of producing its graphical output of large rulesets (in excess of 200 rules) within 5-10 minutes, depending on the overall ruleset complexity. **PREFiRE** first draws the 'All' graph, which shows all permitted connectivity through a firewall. An example 'All' graph generated by **PREFiRE** on a small ruleset can be found in Figure 1 below:

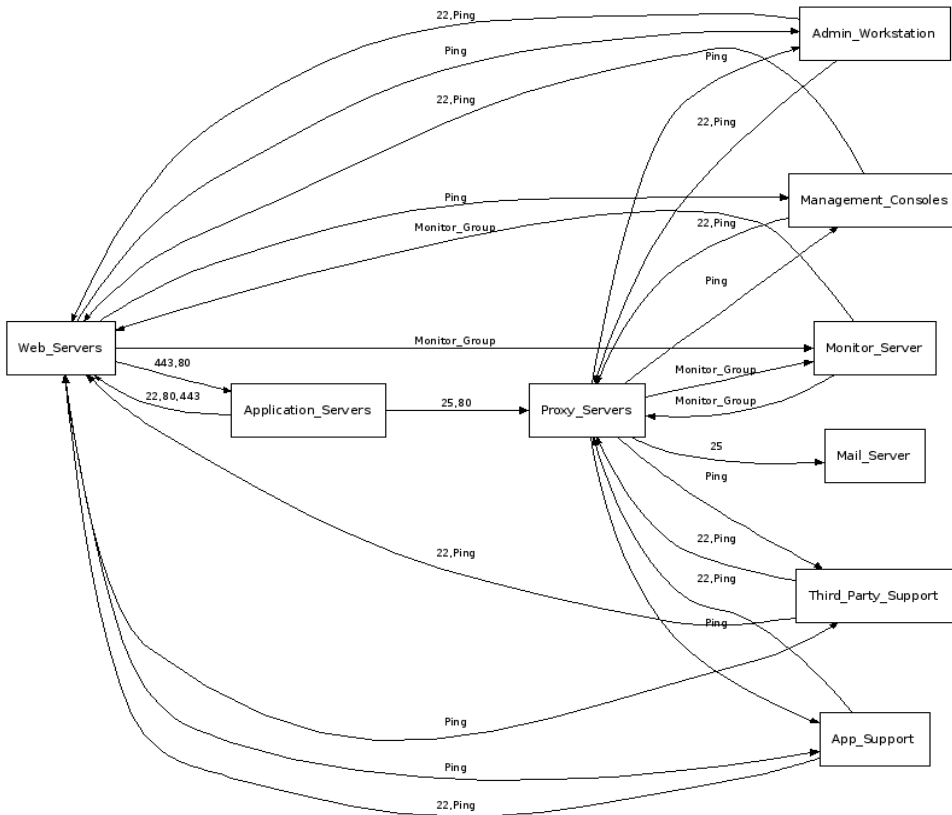


Figure 1. An example of the 'All' graph generated by **PREFiRE**

For each object within the firewall, **PREFiRE** then generates a connected graph showing the permitted traffic flows both *from* and *to* that object, as shown in Figure 2 below:

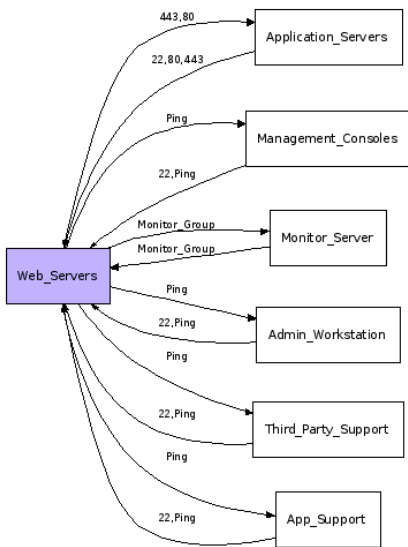


Figure 2. Individual object graphs show traffic allowed *from* and *to* each firewall object

The output clearly shows the allowed connectivity and services between objects. The benefits of visualising firewall rulesets in this way non-exhaustively include:

- **Firewall change control** – By running **PREFiRE** periodically on the same ruleset, the generated graphs can be used to quickly identify any changes in the rules. E.g. firewall administrators may wish to run **PREFiRE** on a ruleset every quarter to identify changes or even following each individual ruleset change to observe the effects on overall permitted connectivity.
- **Comparison of Firewall Types** – Because **PREFiRE** defines all firewall types within the same object definitions, the graphs of say a Checkpoint FW-1 and Cisco ASA firewall that should perhaps be running the same rule configuration can be compared. If identical, confidence can be gained that the two different technologies are actually running the same configuration.
- **Ruleset Change Effects** – **PREFiRE** takes as input text-based and offline firewall configurations. Firewall administrators can edit these configuration files with additional or removed rules, and use **PREFiRE** to graph the new connectivity. The graphs can be used as a sanity check to ensure that the desired connectivity is achieved, before committing the ruleset changes to production systems.
- **Compliance** – **PREFiRE** can be used as a tool to assist in various audits related to compliance and standards across a number of different sectors.

Facilitating PCI DSS Compliance

PREFiRE can be used to assist in many aspects of the Payment Card Industry (PCI) Data Security Standard (DSS). Section 1.1 requires that firewall configuration standards are established, and the following sub sections are immediately applicable to **PREFiRE** and its usage:

- **1.1.2** A current network diagram with all connections to cardholder data, including any wireless networks
- **1.1.5** Documented list of services and ports necessary for business
- **1.1.6** Justification and documentation for any available protocols besides hypertext transfer protocol (HTTP), and secure sockets layer (SSL), secure shell (SSH), and virtual private network (VPN)
- **1.1.8** Quarterly review of firewall and router rules sets

PREFiRE is part of IRM's ongoing research efforts. It is not a commercially available tool and is in a constant state of refinement. However, the tool is accessible through IRM for clients, and where applicable, **PREFiRE** is used as part of IRM's standard firewall ruleset review service offering, and is also capable of being extended for client-specific needs within the firewall domain. Contact IRM for further information on **PREFiRE** and its potential usage for your firewall security and auditing needs.

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.