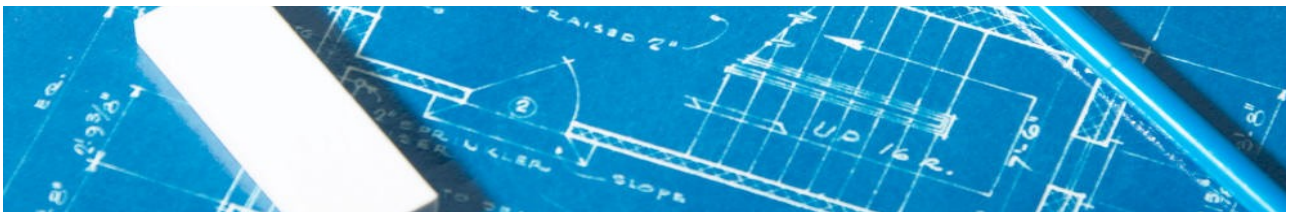
360-FAAR Firewall Analysis, Audit, Repair

Un-Stirring the Jam



Purpose of 360-FAAR

Organisations require security for their networks. A firewall is one of the most effective defences a network can have, if configured correctly. Many organisations are required to use two different firewall brands by law, adding to the complexity of their configurations. A firewalls “policy” is its list of instructions to carry out; rules.

Firewall policies evolve over time (usually configured manually by an engineer), and once built are hard or even a security risk to remove or replace. Many policies have been growing for ten or more years and need serious restructuring to cope with emerging connectivity models, or to remove security concerns.

360-FAAR's purpose is to establish, from known information (log files and configuration) which of the existing policies parts are needed and then build a new, easy to understand, **secure**, policy from those components and to write a file to configure it on the firewall. Configurations are tailored for each firewall automatically.

Commercial Policy Analysis Tools

My current market competition (Firemon, Skybox, Tufen etc) are pursuing a question and answer model with the answers being provided by a person on a per rule basis, with extra information being provided by the program via a multiple choice menu system, to help the engineer decide what to do with the rule.

For large and complex firewalls this process is costly in time and money, so much so (1-2 years per project) that often the firewall in question has changed enough that the project is unrecognisable by the end and it inevitably fails. Project creep is costly and ineffective in the new fast moving network we have today!

360-FAAR - Un-Stirring The Jam from the Peanut Butter – We Only Want the Jam

360-FAAR processes policies in the same way as firewalls do internally, doing the hard work for you, and produces MS Excel readable spreadsheets of the new policies it suggests, including all relevant information from the original configuration. No information is lost!! Unused configuration information and debug output about the process in an easy to understand format provides visibility to check the new policies are correct.

The the new policies can be tweaked by the interested parties, in spreadsheet form before sign off, after which the policy spreadsheet is read again by the program and the code to update the firewall is automatically generated. It is in the firewalls command language so can be checked by engineers.

The process is completely off line and needs no live access to firewalls or a network. It simply reads copies of the firewall configurations and log files. There is no better security for your data than off line.

The speed, accuracy and transparency of this process allowed multi-nations such as Diageo Ltd. Verison, BT Design, BT Openreach, Party Gaming Ltd. Aviva Investment, Cap Gemini and others, to achieve the signoff needed from their many connectivity partners to resolve the security considerations they had. It was possible to do this within the same project as the audit its self, and often more effectively than the commercial products available.

360-FAAR has even been used in collaboration with other commercial products, to create new clean understandable policies that can then be monitored effectively by the commercial tools.