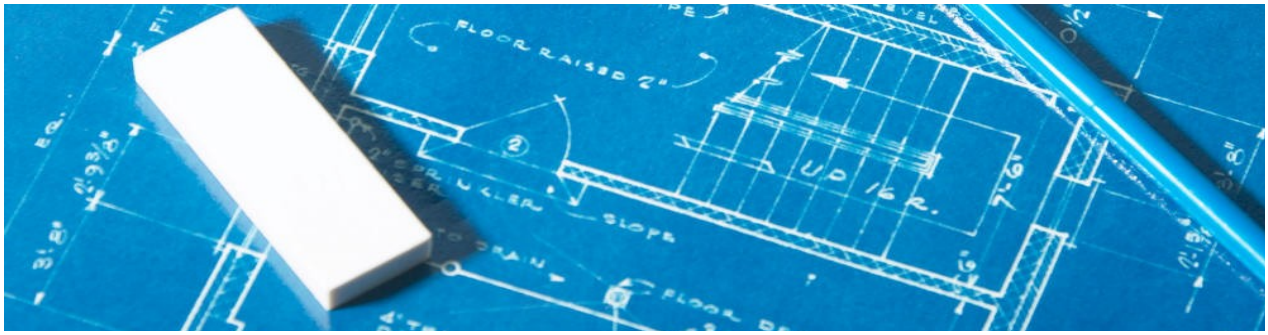
360-FAAR Design Goals

Overview of Design Goals and General Principals



Purpose of This Document

This document presents a generalised overview of the design goals of 360-FAAR.

It is hoped that the information presented here will provide insight into the way 360-FAAR has been constructed and how this relates to the methodologies described in the other material provided with this document.

Intended Audience

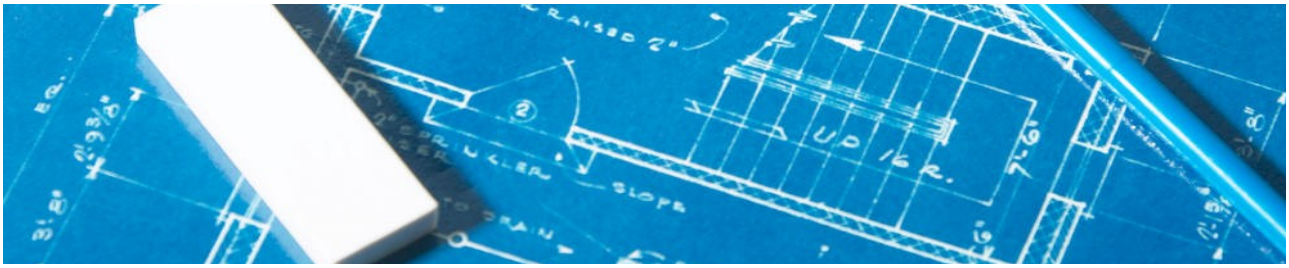
This documents intended audience are technical professionals, technical managers, operations teams, and company directors interested in technologies that offer a distinct advantage over competitors solutions.

About the Author

Dan Martin is the Director of 360-Analytics Ltd. Prior to this, he worked as a Network and Security Analyst/Engineer for fourteen years, employed by companies such as Intel, Nokia Internet Communications, Sun Microsystems, Qualcomm, Verison, Diageo Ltd, Party Gaming Ltd. and 'The Cloud' wifi network.

Table of Contents

End of Contents



1. Design Goals for 360-FAAR

1.1 Simplicity

The IPv4 and IPv6 protocols are the basis of all internet communication.

So fundamental are these protocols, that it is from them we take the name 'Internet' (from Internet Protocol, IP) for the large number of interconnected networks which make up our modern day Internet.

The address structure of IPv4 is 32 binary digits, yet from these 32 bits we are able to find any network or server located anywhere online.

We at 360 Analytics Ltd think that this simplicity of form and function is missing from the firewall analysis world and 360-FAAR was, in part, built to fill this gap.

1.2 Consistency

Firewall analysis tools come in many shapes and sizes, each of which has its own methodologies for firewall cleanup. Most commonly these tools present an engineer with conflicts within a rulebase and provide possible options for resolution of the conflict.

This methodology requires the engineer in question having 'Local Knowledge' with regard to the choices they are offered and in practice when an engineer does not have this they often choose to leave rules as they are and not to make any changes at all.

At the other end of the spectrum the engineer tasked with removing rulebase anomalies may choose to resolve all conflicts they are presented with but do not do this is any consistent way, leading to firewall policies that differ greatly across an organisation after cleanup operations, or worse yet broken connectivity for vital services!

360-FAAR resolves these issues by automating these processes. An engineer can use a firewalls log files to filter its rulebase and build known good configurations that permit all connectivity currently in use, removes all connectivity that was not in use, and builds full diagnostic reports.

Reports contain spreadsheets with rule definitions, the firewall commands to create them, all matches from the log files with the rulebase (including traffic that matched more than one rule) and the results of the various types of analysis requested.

The output of 360-FAAR uses the same format for all policy rebuild operations. It also presents all manufacturers rulebases in a common format to ease analysis and cross-referencing further.

360-FAAR uses an incredibly powerful filter section that permits inclusive and exclusive filters for CIDR addresses, text strings, section headers, comments, object names and groups to be used at once. This same filter section is used across the board and further aids consistency.

1.3 Granularity

360-FAAR is the most granule firewall analysis tool currently available.

It is capable of isolating connectivity based on any CIDR address, text string, range of addresses, object names, rule definitions and individual connectivity profiles from within many polices rules or a subset of an individual firewall rules.

360-FAAR can even isolate individual addresses or ranges from within objects within rules and build new connectivity from these providing a level of granularity not found in other programs.

1.4 Universality

With the advent of the internet, a huge number of technologies that are independent of their underlying hardware have been invented.

The Transmission Control Protocol and Internet Protocol (TCP/IP) were the first of these, allowing disparate systems to communicate with common rules.

This commonality has not transferred to firewall management tools. Policy editors are firewall manufacturer specific and often firewall specific, with different models using greatly differing approaches for management.

360-FAAR uses a common firewall rulebase format (very similar to checkpoints format, with extra fields for zone information if the firewall supports zones or area mappings) to display the rules it generated.

360-FAAR converts all firewall's configurations to this format internally, before processing, which means that its core functionality can be used in exactly the same way across all firewall manufacturers and models supported.

Once complete the process redefines these rules using the 360-FAAR Policy Engine to build rules from the objects and definitions currently available in firewall configs loaded, while also being able to create rational objects for connectivity that is not covered by the pre-existing configuration.

Contact and Company Details

360 Analytics Ltd.

LUTIDINE HOUSE
NEWARK LANE
RIPLEY, SURREY
UNITED KINGDOM
GU23 6BS
TEL: +447960 028 070
Company No. 07533060

- For General Information in the UK
  Please Visit: www.360analytics.co.uk
- For Further info please visit the blog: 36zeroanalytics.wordpress.com

- For General Queries Please Contact: info@360analytics.co.uk
- For Sales Requests Please Contact: sales@360analytics.co.uk

- For International Information Visit: www.360-analysis.com
- International Contact: info@360-analysis.com

- For Operations or Project Work Requiring Onsite Support
  Visit Our Sister Company Site: www.36ZeroNetworkAnalytics.com
- Contact 36ZeroNetworkAnalytic Ltd: info@36ZeroNetworkAnalytics.com