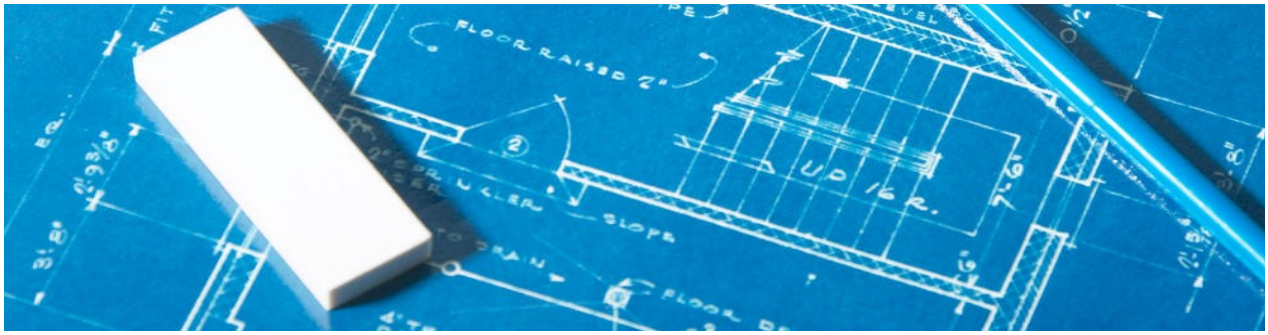
360-FAAR Executive Overview

Scenarios For Use

Overview of Proposed Scenarios

General Principals



Purpose of This Document

This document presents a generalised overview of the scenarios and solutions presented in the 360-FAAR Scenarios For Use documentation.

Intended Audience

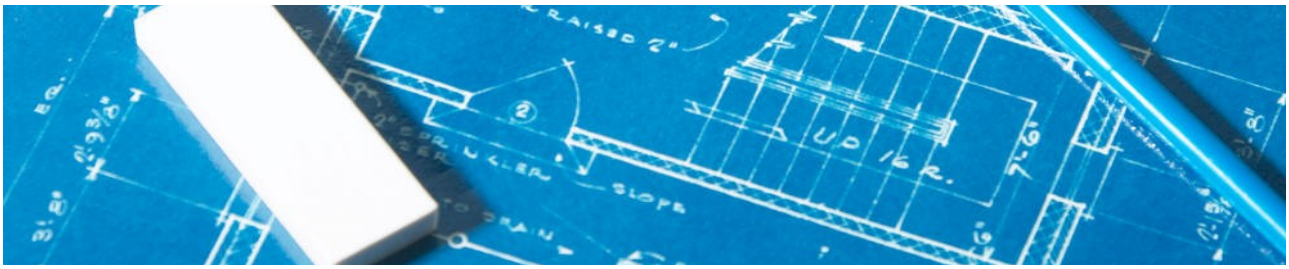
This documents intended audience are technical professionals, technical managers, operations teams, and company directors interested in technologies that offer a distinct advantage over competitors solutions.

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. Overview of Methodologies Examined in the 360-FAAR Scenarios For Use Document

1.1 What Does 360-FAAR Do And Where Can I Use it?

360-FAAR solves many common issues found in large networks and in firewall configurations, and automates the process of correcting the problems identified.

360-FAAR can merge multiple configurations together and split single (or multiple) configs into smaller subdivisions using any of the filters, matching engine's or policy cleanup routines provided.

Custom modules can be added with ease due to the modular nature of the 360-FAAR Policy Engine.

The 360-FAAR Policy Engine operates in a repeatable and predictable way that is easily understandable, is familiar to technicians, is (if required) highly configurable and is consistent across many hardware manufacturers equipment.

It can be used in any situations that routing, or firewall policy decisions relating to traffic or types of connectivity used, are made.

In short, 360-FAAR can be used almost anywhere you are experiencing issues with connectivity, management and visibility, or security concerns; a firewall policy cleanup is a good example.

1.2 The 360-FAAR Policy Engine

The 360-FAAR Policy Engine is at the heart of ALL the new methodologies put forward in the '360-FAAR Scenarios For Use' documentation.

The 360-FAAR Policy Engine provides the core functionality of the program.

It is a TCP/IP processing engine that is capable of matching CIDR ranges/addresses, protocols or services, group structures, text strings and many other cross platform methodologies for analysing a firewalls configuration, network traffic and other such information.

360-FAAR operates completely off-line and produces concise referenced documentation that can be edited in Microsoft Office software, by the interested parties, and then reprocessed before implementation in either a test or live environment.

The 360-FAAR Policy Engine can be run many times against any number of configurations, after the initial config, routing table and/or log file processing is complete.

1.3 Generalising The Scenarios and Solutions Presented

The commonality between the scenarios proposed in the 360-FAAR Scenarios For Use documentation, is the disparate nature of the network and firewall analysis methodologies in general use at the time of writing.

These require that an engineer perform a long manual processes to unify the disparate information he is presented with in order to produce concise and meaningful project plans, implementation plans and documentation of the changes required to fulfil these.

To manually produce a document, that holds its own integrity intrinsically, is such a way that its suggestions can be implemented in a large network with confidence, is very hard.

Meaning that the output of an automated process should, its self hold enough easily understandable information in rationalised sections to be able to cross reference the automated suggestions made.

360-FAAR combines all manufacturers configurations, routing tables and logs into a single format and uses this to establish 'ALL Known Information' that is related to the configs loaded, the traffic passed and the properties of all objects and rules.

After filtering or merging the sub sections of the firewalls policies in which you are interested, you can build many new configurations that are individually suited to each firewall in question and present these for editing in spreadsheet format to anyone who requires access to the changes proposed.

The types of new rues generated can be controlled by a system of priorities, or by definite rules or a combination of these. The process that creates the rules is repeatable and predictable for the types of outcomes you may require.

It is also general enough to cope with a large degree of 'special cases' and has many generalised structures that can be used as templates for new queries as required.

2. Why This Methodology Is Different

The 360-FAAR program is designed from the ground up as a periodic off-line analysis tool.

- Firewall state tables hold short term connection state.
- IDS/IDP hold longer term information.
- Log analysis holds the long term information.
- Provider independent tools that permit long term perspectives on current configurations, are few and far between. 360-FAAR is targeted to 'plug the hole' in this market segment.

360-FAAR's Policy Engine operates as a universal firewall, zone/CIDR filter and router internally.

It makes its comparisons in a way related directly to the current configuration in use, requiring no user intervention in the process of resolving the problem its configured to examine.

The process is highly configurable presenting at most hundreds of operations, although more commonly five or six will do.

Once the documentation has been created these spreadsheets them selves become modifiable representations of a firewall policy.

Changes made can be uploaded and the new rules generated. The same spreadsheet can be used to automatically generate new rules for many firewalls, ensuring the integrity of each of the changes built.

The automated generation of rules across multiple firewall vendors, based on a companies log information, its (dynamic) routing tables and current configurations lends it self easily to automation on larger scales.

The intention of a large scale implementation would be to ensure known good connectivity is retained while reorganising policies in ways that enable continuity across service providers, manufacturers and customers as well as during network changes.

Importantly, allowing safe removal of connectivity that is out of date or badly configured in an intrinsic part of a networks security procedures. 360-FAAR can automate this process.

A good analogy to use, would be to consider it a very slow DDNS for firewalls, looking at an infrastructure in any time frame, but most usefully, in three months to two year periods.

This allows sufficient time for the security department to cross check any proposed (automated) changes intrinsically within the documentation they are provided with, and to sign it off as safe before application to the infrastructure.

360-FAAR removes the element of human error while at the same time it protects against the automated poisoning of policies and other such attack vectors.

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