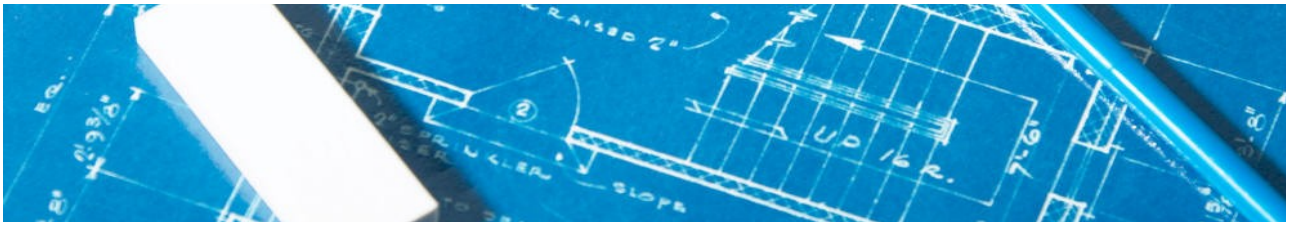
360-FAAR Executive Summary

Scenarios For Use



Purpose of This Document

This document presents bullet points for each of the twenty scenarios and solutions detailed in the 360-FAAR Scenarios For Use documentation.

Intended Audience

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 in large high-tech environments.

Table of Contents

1. The Firewall Rulebase Cleanup

- Remove all unused connectivity from a firewall's policy.
- Tag and keep DR rules using firewall specific tags.
- Simplify the connectivity in use and automatically build new rulebases.
- Reduce rule numbers by up to 70% (stat from real life implementations).

2. Moving Networks or Routes Within Network Infrastructure

- Automatically identify all connectivity to or from CIDR network ranges.
- Translate rules and objects between firewall manufacturers.
- Remove unneeded connectivity after route move.
- Add only the connectivity that is not already permitted by the 'move to' firewalls.

3. Network Object Translation to Newly Assigned IPv4 or IPv6 Addresses

- Translate network objects to new IP addresses using a choice of methodologies.
- Translate IPv4 to IPv6 addresses.
- Match existing objects during translation.

4. Change Object Naming Conventions

- Rename objects and remove duplicates throughout all specified configurations.

5. Firewall Policy / Group Reassignment and Restructuring

- Regroup all objects and rename groups throughout all specified configurations.

6. Close Open Rules

- Identify all connectivity permitted by open rules and automatically build replacement rules.
- Identify rules permitting large areas of connectivity and build replacement rules.

7. Security Policy Enforcement

- Identify security policy violations in firewalls with or without zone methodologies.

8. Split Large Policies Into Smaller Policies for Virtualisation

- Filter, translate and subdivide existing rulebases within the core functionality.

9. Merge Firewall Configurations Together Seamlessly

- Filter, translate and merge many existing rulebases within the core functionality.

10. Translating Between Firewalls and Manufacturers

- Filter only the connectivity you require and then translate this to another firewall.
- Remove all duplicate connectivity or object definitions from the new rules.

11. NAT Rule optimisation and Simplification

- Identify NAT rules in use and automatically build simplified rules from these.
- Tag and keep NAT rules using firewall specific tags.
- Identify all objects and addresses using specific NAT rules.

12. VPN Rule Optimisation and Simplification

- Identify VPN rules in use and automatically build simplified rules from these.
- Tag and keep VPN rules using firewall specific tags.
- Identify all objects and addresses using specific VPN rules.

13. Security Policy Optimisation and Simplification

- Filter the connectivity you require or select a complete rulebase to optimise.
- Organise the new rulebases using hit counts (object hits or rule hits)
- Organise the new rulebases using addresses (names or IP addresses)
- Organise the new rulebases using services (names, protocols or ports)

14. Removing or Decommissioning Networks

- Safely remove connectivity to networks from all rules requested.
- Re-optimise rules after networks are removed.

15. Build New Policies From Log Files, Objects and Groups (not pre-existing rules)

- Specify new groups and objects and build firewall specific policies from pre existing logs.
- Replace router hardware with firewall hardware and build a policy for the firewall from the routers log files!

16. Antispoofing Group / Routing Table Cross Referencing

- Allocate all objects to routes to establish each objects direction from the firewall.
- Safely re-enable firewall antispoofing capabilities without risking network outages.

17. Custom Analysis and Rebuild Projects Using 360-FAAR

- Design customised procedures for organisation wide policy consolidation.
- Add custom modules to the 360-FAAR Policy Engine's modular structure.

18. Automating 360-FAAR Within Your Infrastructure (A Future Project)

- Implement 360-FAARs full functionality within your network.
- Automatically remove old rules and organise firewall policies using any of the aforementioned methods throughout your complete infrastructure.

19. Has a Network Audit Identified Rules that Violate Your Security Policy?

- See point 1-5, then see point 6 and 7 - and repeat the process

20. Document Your Firewalls Configuration Automatically (A Future Project)

- Automatically document all or part of your firewalls configuration (e.g to a wiki)

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 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