360-FAAR Firewall Analysis, Audit, Repair

360-FAAR Open Source Release vs 360-FAAR Enhanced Release Feature Comparison

General Feature	360-FAAR Open Source	360-FAAR Enhanced
NETWORK AND SERVICE OBJECT AND GROUP ANALYSIS:		
Configuration Syntax Checking	Yes	Yes
Object Consistency Checking	Yes	Yes
Duplicate Identification and Reporting	Yes	Yes
Infinitely Deep Nested Circular Group Checking	No	Yes
Translation Between Manufacturers	Yes	Yes
Fast / Robust Translation Between Manufacturers	No	Yes
RULE ANALYSIS:		
Configuration Syntax Checking	Yes	Yes
Object and Type Consistency Checking	Yes	Yes
Accept Rule Matching and Translation Between Manufacturers	Yes	Yes
Drop, Reject, Deny and Encrypt Rule Output and Translation Between Manufacturers	No	Yes
FILTERS AND FUZZY LOGIC:		
CIDR Filtering, Matching and Resolution	Yes	Yes
Service and Port Filtering	No	Yes
Fuzzy Group Matching	No	Yes

Feature Analysis	360-FAAR Open Source	360-FAAR Enhanced
CONFIGURATION CHECKING DURING INPUT:		
Object, group, IP address, rule and NAT definition checking during configuration read	Yes	Yes
Circular group detection and nested circular group detection	Yes	Yes
Deep circular group detection and nested circular group detection within infinitely deep nested groups	No	Yes
CONFIGURATION CHECKING DURING PROCESSING:		
Network and service object consistency checking	Yes	Yes
Network and service group consistency checking	Yes	Yes
Deep network and service group consistency checking	No	Yes
PRINT MODES:		
Modes: print (Print Object Analysis)	Yes	Yes
Modes: fltprint (Filtered Object Analysis)	Yes	Yes
Modes: srvcprint (Print Service Object Analysis)	No	Yes
Modes: fsrvcprint (Filtered Service Object Analysis)	No	Yes
Print Mode Filters: CIDR include and exclude filters	Yes	Yes
Print Mode Filters: Text String include and exclude filters	Yes	Yes
Print Mode Filters: Service name and/or port range include and exclude filters	No	Yes
Print Mode Output: Output network object information from configuration and log files	Yes	Yes
Print Mode Output: Output network object group information – network objects, super-groups, subgroups	No	Yes
Service Print Mode Filters: CIDR include and exclude filters	No	Yes
Service Print Mode Filters: Text String include and exclude filters	No	Yes
Service Print Mode Filters: Service name and/or port range include and exclude filters	No	Yes
Service Print Mode Output: Output service object information from configuration and log files	Yes	Yes
Service Print Mode Output: Output service object group information – service objects, super-groups, subgroups	No	Yes

Feature Analysis	360-FAAR Open Source	360-FAAR Enhanced
RR MODE:		
Mode: rr mode (Rationalise Rules Processing)	Yes	Yes
RR Mode Filters: CIDR include and exclude filters	Yes	Yes
RR Mode Filters: Text String include and exclude filters	Yes	Yes
RR Mode Filters: Service name and/or port range include and exclude filters	No	Yes
RR Mode Options: Default option sets: SIMPLE, NAT TRANSLATION, LOG FILTER, HIGH RESOLUTION	Yes	Yes
RR Mode Options: Default option sets: COMPLEX, COMPLEX LOG FILTER	No	Yes
RR Mode Options: INCLUDE objects from the SUBNETS of the CIDR FILTERS in the new rulebase	Yes	Yes
RR Mode Options: Choose FILTER TYPE and FILTER rules based on CONNECTIONS FOUND in the LOG?	Yes	Yes
RR Mode Options: Filter Type: yes, no, loose loosen, none	Yes	Yes
RR Mode Options: Filter Type: complex, complexn	No	Yes
RR Mode Options: INCLUDE objects that CONNECT to the OBJECTS RESOLVED, by the filters	Yes	Yes
RR Mode Options: TRANSLATE log connections IP's using NATS while FILTERING for IN EX CIDRs	Yes	Yes
RR Mode Options: Resolve NETWORK OBJECT "Any" to the most specific netobejcts SEEN IN THE LOG FILES	Yes	Yes
RR Mode Options: Resolve SERVICE OBJECT "Any" to the speciffic services SEEN IN THE LOG FILES	Yes	Yes
RR Mode Options: Match rules and supernets aginst PREVIOUSLY EXPANDED rules	Yes	Yes
RR Mode Options: Match ACCEPT rules against ENCRTPYION rules FROM EARLIER in the MERGE FROM rulebase	Yes	Yes
RR Mode Options: Include ENCRYPTION rules from the MERGE TO rulebase in the filter match rulebase	Yes	Yes
RR Mode Options: Use FUZZY logic for NETWORK GROUP MATCH. Smallest size groups to match	No	Yes
RR Mode Options: Use FUZZY logic for NETWORK GROUP LOOSE MATCH. Number of missing objects per group	No	Yes
RR Mode Options: Use FUZZY logic for SERVICE GROUP MATCH. Choose smallest size groups to match	No	Yes
RR Mode Options: Use FUZZY logic for SERVICE GROUP LOOSE MATCH. Choose number of missing objects per group	No	Yes
RR Mode Options: MATCH the MOST SPECIFFIC NETWORK groups possible? Use the largest, smallest or random groups	No	Yes

Feature Analysis	360-FAAR Open Source	360-FAAR Enhanced
RR Mode Options: MATCH the MOST SPECIFFIC SERVICE groups possible? Use the largest, smallest or random groups	No	Yes
RR Mode Options: Use 'fast' and 'robust' object and group matching between configurations and manufacturers	No	Yes
RR Mode Options: Output VERBOSE information during Rule Rationalization	Yes	Yes
RR Mode Build Rules Options: ds (Destination/Source Priority)	Yes	Yes
RR Mode Build Rules Options: sr (Service Priority)	Yes	Yes
RR Mode Build Rules Options: hc (Hit Count Priority)	Yes	Yes
RR Mode Build Rules Options: cl (Clean Original Rules)	Yes	Yes
RR Mode Build Rules Options: COMPLEX rulebase rule order preservation: ds (Destination/Source Priority)	No	Yes
RR Mode Build Rules Options: COMPLEX rulebase rule order preservation: sr (Service Priority)	No	Yes
RR Mode Build Rules Options: COMPLEX rulebase rule order preservation: hc (Hit Count Priority)	No	Yes
RR Mode Output Rules: Checkpoint, Cisco, Netscreen Rule Actions: Accept, Permit	Yes	Yes
RR Mode Output Rules: Checkpoint, Cisco, Netscreen Rule Actions: Drop, Reject, Deny	No	Yes
RR Mode Output Rules: Checkpoint, Cisco, Netscreen Rule Actions: Encrypt, Tunnel – IKE and ESP needs manual config	No	Yes
BLDOBJ MODE:		
Mode: bldobj (Build Objects For Rules Mode)	Yes	Yes
BLDOBJ Mode Input Format: odumper/ofiller rules and numberrules.pl output	Yes	Yes
BLDOBJ Mode Object Locations: Pull network and service objects from 3 loaded configurations	Yes	Yes
BLDOBJ Mode Object Locations: Pull network and service objects from 3 or more loaded configurations	No	Yes
BLDOBJ Mode Object Output Translations: Translate objects to output configuration names and type	Yes	Yes
BLDOBJ Mode Object Output Robust and Fast Translations: Translate objects using 'robust' and 'fast' methods	No	Yes
BLDOBJ Mode Output Rules: Checkpoint, Cisco, Netscreen Rule Actions: Accept, Permit	Yes	Yes
BLDOBJ Mode Output Rules: Checkpoint, Cisco, Netscreen Rule Actions: Drop, Reject, Deny	No	Yes
BLDOBJ Mode Output Rules: Checkpoint, Cisco, Netscreen Rule Actions: Encrypt, – IKE / ESP needs manual configuration	No	Yes

Feature Analysis	360-FAAR Open Source	360-FAAR Enhanced
LOAD MODE:		
MODE: load (Load Configuration Bundles Into Running Instance of 360-FAAR)	Yes	Yes
COPYLOG MODE:		
MODE: copylog (Copy Binary Logs Between Config Bundles)	Yes	Yes
MERGELOG MODE:		
MODE: mergelog (Merge Binary Logs Between Config Bundles and Report Matches)	Yes	Yes
HELP MODE:		
MODE: help (Output Help Information)	Yes	Yes