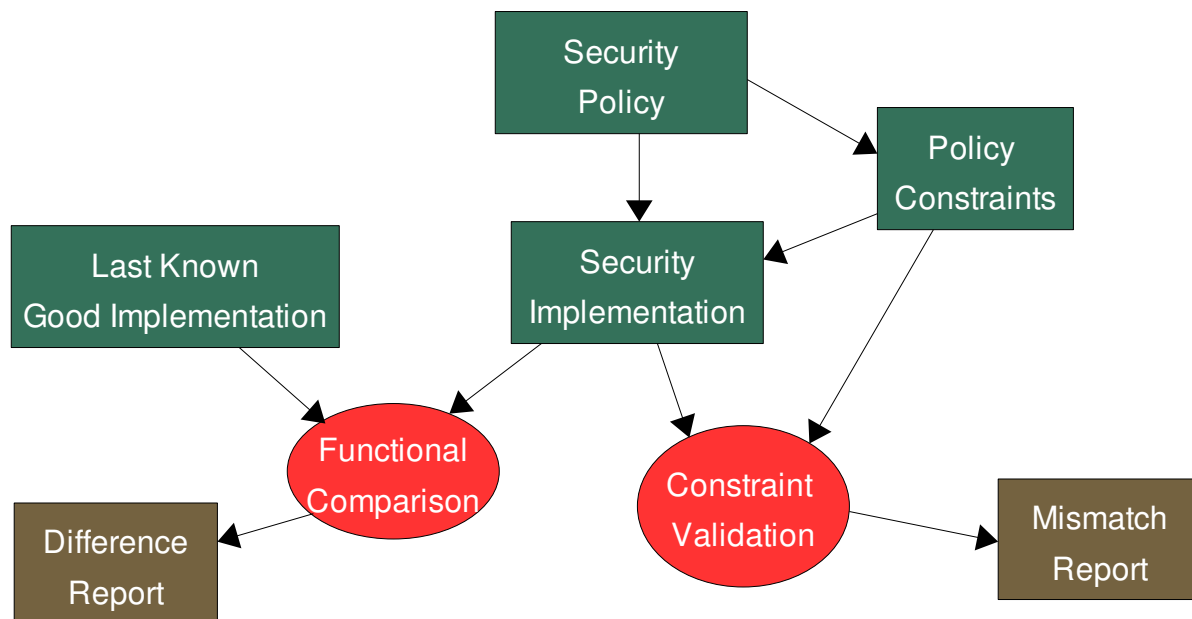


## New Product Announcement: InfoSector, the Information Security Dissector

A critical ingredient for successfully managing modern network security is finding relevant information in a maze of configuration data. The InfoSector toolset is designed to map configuration data in a way that makes finding the relevant information faster and more reliable. Quickly discover what your firewall is doing and why with InfoSector.

- **Improve security device operation understanding:** Browse and interrogate a flow model of how the configured security device will operate on sets of packets.
- **Detect configuration flaws before deployment:** Identify conflicting rules or unexpected functional differences between configurations.
- **Support multiple vendors and versions:** Understand the operation of your Cisco and Juniper devices in a common model.
- **Integrate with existing operation flow:** Use InfoSector tools at key points in your existing configuration management and review processes.
- **Tighten binding between security policy and implementation** As changes are made to the security implementation, errors may be introduced that violate the guiding policy. As shown in the flow chart below, InfoSector operations automatically catch such implementation drift.





## Operations

- **Self Conflict Analysis** – Identify entries in the same rule lists that operate on the same packets.
- **Disambiguation/Dissection** – Create an unambiguous listing of packet sets to operations. This describes all possible packets and what the configured device will do those packets. The Visualizer allows the user to filter and sort this data to rapidly find what the configuration would do and why.
- **Functional Comparison** – Perform a functional difference between two configurations, two versions of a configuration from the same device or configurations from different devices performing the same role (even between devices of different vendors). Find the important functional changes without the clutter of textual differences.
- **Constraint Validation** – Create an expression to indicate how sets of packets should be processed. Find where the configuration does not match the constraint.

## Components

- **Analyzer** – Employs efficient algorithms to enable rapid analysis of even the most complex configurations. Can be invoked from the other tools or from scripts. Generates XML reports as output.
- **Visualizer** – Displays the results of the analyzer. Supports the user in browsing, sorting, and filtering the results. Displays the analysis results in conjunction with the original configurations.
- **Querent** – Creates and displays policy constraints. Can invoke Analyzer and Visualizer on user selected constraints.

## Details

Install Platforms	Windows XP, Server, Vista; Linux available on demand
Analyzed Platforms	PIX/ASA 5.x-8.x, FWSM, IOS 12.3, Netscreen 5.x, Checkpoint
Required Hardware	Intel/AMD 1 GHz, 1 GB memory, 50 MB free disk
Actions modeled	Firewall filtering, URL filtering, Inspect/proxying, IPSec, AAA, NAT

## Interested?

Official product release date, April 7, 2008. Contact us for evaluation copies and pricing information. [info@network-geographics.com](mailto:info@network-geographics.com) 888.276.2027