

## Assuring Network Security

Today's IT staff faces the daunting task of accurately controlling network traffic. Network Geographic's tools enable

- Improved understanding of security device operation
- Tighter binding between security policy and security implementation
- Multi-vendor and -version support
- Integration into existing your existing operations



## Understand the Issues

As computers proliferate and connectivity options explode, simply making the desired traffic flow properly is difficult. Ensuring that hostile traffic is blocked is even harder. In a world of constant change you can depend on your users to tell you about problems, but

[ The bad guys don't file bug reports. ]

The many changes that occur during the life cycle of the network lead to many security issues you need to be concerned about.

- **Policy stagnation.** The person who added the rule to allow HTTP traffic from a particular subnetwork is long gone. Do you still need that rule? Could any packets ever trigger the rule?
- **Policy comprehension.** You are a new employee inheriting filtering rules sets of 100's or 1000's of rules. How do you quickly understand the implications of the existing security stance?
- **Change scope and integrity.** You've been told to allow access from additional partners, and your colleague has a proposed solution. Does it solve the problem? Does it have unintended consequences?
- **Uniform enforcement.** Your enterprise deploys security devices from multiple vendors as a matter of policy. Do all the vendors apply AAA rules in the same way? Do you interpret the rules in the same way in your reviews?
- **Proof of compliance and adherence.** The external auditor asked for proof that your security configurations accurately enforce the company's stated security policy. What do you provide?

## Solve the Problems

Network Geographic's Information Security Dissector, **InfoSector**, provides a suite of tools to help you solve these problems. The InfoSector Engine interprets the configuration file to gather information about how packets will be processed and performs analysis to reorganize this information to be more relevant to policy and easier for you to understand. The Engine stores the results in an XML file for easy integration with your existing workflow. The InfoSector Visualizer displays the results and enables you to interactively understand your configuration: how well it implements your policy and which particular elements of the configuration impact the bottom line.

InfoSector operates on security device configurations, so this analysis can be performed before configuration changes are deployed, enabling you to catch potential security errors earlier and reducing the window of vulnerability on the production network.

## Analyze the Security Posture

The InfoSector Engine can perform the following operations.

**Cross configuration functional changes** – Identify the functional differences between an initial configuration and a changed version of that configuration. Sometimes changes to one configuration line may have unintended consequences elsewhere in the configuration. Consider the following example:

Initial Configuration	Proposed Configuration
Rule 10 – permit ip 192.168.1.0/24 any	Rule 10 – permit ip 192.168.1.0/25 any
Rule 11 – deny ip any any	Rule 11 – deny ip any any

InfoSector will report a conflict for the source addresses 192.168.1.128 to 192.168.1.255 to any destination. The initial configuration allows IP traffic to these ranges, but the proposed configuration denies it. By isolating the changes, you can more confidently decide whether all the functional changes are desirable.

Cross configuration functional analysis can also be beneficial for comparing configurations between different devices that should be performing equivalent tasks. These devices may well be produced by different vendors, e.g. Cisco vs Netscreen.

**Tiling** – Remove the ambiguities in a network configuration. Each potential packet will match one and exactly one line in the tiled view. That line summarizes all actions that will be applied to the packet by the network security device. By setting filters for particular sets of packets or actions, you can rapidly drill down to find the parts of the configuration that are of current interest. You will gain a deeper understanding of how the network security implementation will work on the network and how well it matches guiding security policy.

**Policy Constraints** – Given a set of precise policy constraints, identify any violations of the constraints and how the targeted configuration will enforce the security posture. For example, if the security policy states that partner networks should only have HTTP access to a particular internal server, the policy may be expressed as

```
Source Address ^ 10.10.0.0/16 &
(Destination Address ^192.168.1.15 &
 Destination Service ^ TCP:80 & Action = permit) |
(!(Destination Address ^ 192.168.1.15) |
!(Destination Service ^ TCP:80))& action = deny)
```

You could automatically apply this standing policy constraint to each proposed changed configuration before it is deployed to ensure that all higher level policy requirements are continually enforced. Alternatively, the policy constraints could be run each night to ensure that no out-of-policy changes were inserted during the day.

Policy constraints can also be contributed from all groups affected by the network security device not just the group directly responsible for its configuration. This enables distributed organizational intelligence to work together to keep the network infrastructure working within security policy specifications.

**Policy Query** – Similar to policy constraints, specify the traffic of interest. Perhaps the traffic is not flowing as expected, or you are concerned that traffic is not being adequately secured. By specifying the subset of packets of interest, InfoSector can create a report of configuration rules that affect the packets in question. The report includes links back to the original configuration to help the user rectify any problems.

For example, you might be helping a user who is not seeing traffic pass from his work station (in the 10.20.0.0/16 network) to the engineering file server (192.168.1.21). You pass the following query to InfoSector

```
Source Address ^10.20.0.0/16 &  
Destination Address ^192.168.1.21 &  
Protocol ^ TCP
```

The query returns a report of all rules in the security appliance that affect the queried packets. The packet region that includes your user is affected by a rule that explicitly blocks SMB traffic from a subset of the 10.20.0.0/16 network which includes your user's machine. A note on the rule indicates there had been a malfunctioning machine in that range. Perhaps this was a temporary rule that had been forgotten. With the query, you focus on the subset of the configuration that affects your current problem. In a large configuration this reduces clutter and potentially identifies rules you didn't think were relevant.

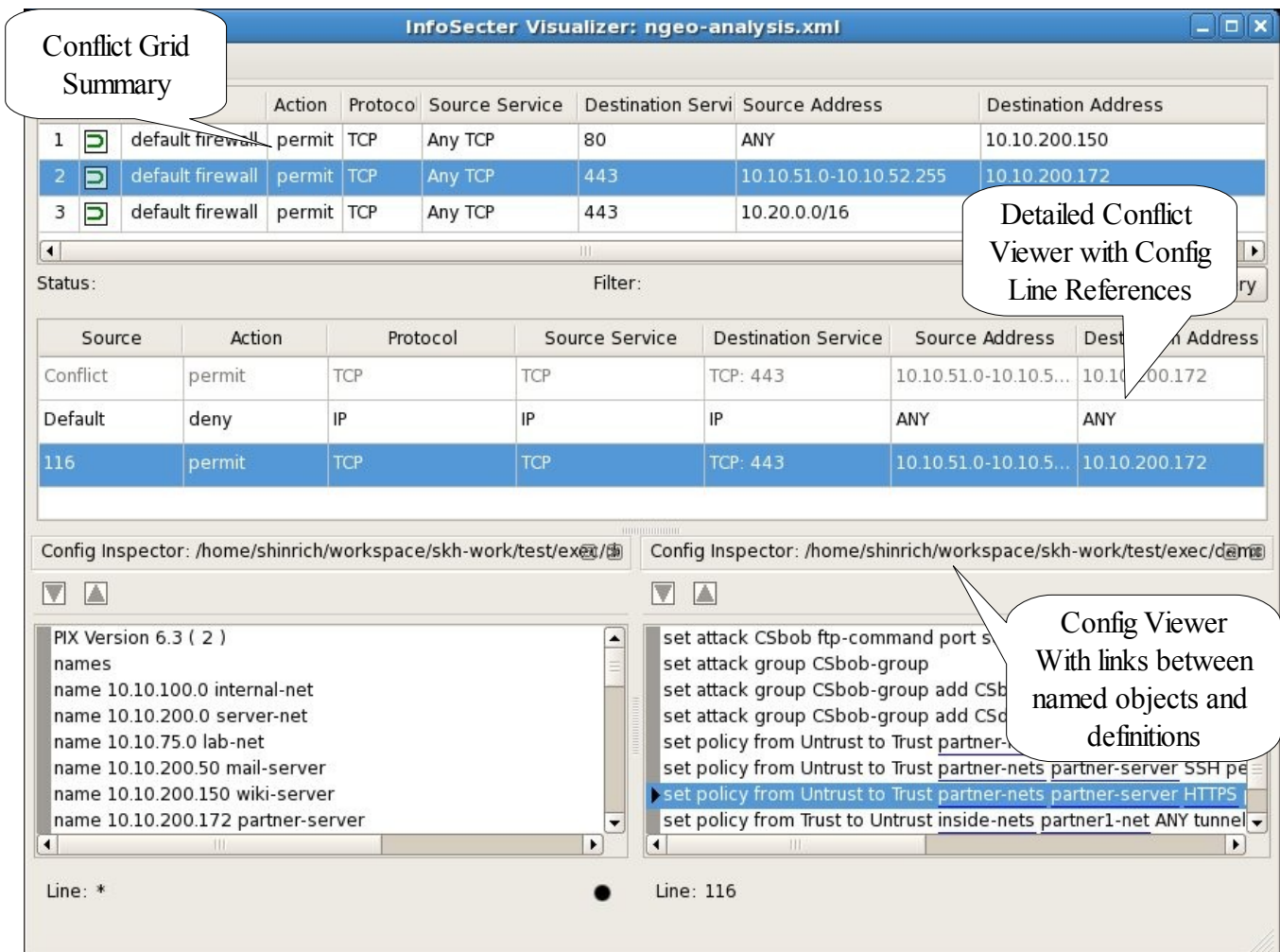
**Self analysis** – Identify the rules within the same configuration that overlap one another. Some conflicts are to be expected in a ordered access control list, but other conflicts may be unintentional and merit deeper investigation.

## Visualize the Results

Network Geographic's InfoSector Visualizer displays the results of all Engine operations. With it you can interpret the analysis results against the configurations. InfoSector Visualizer features:

- Links between conflicting lines in the new and initial configuration files.
- A structured view of the configuration with hyperlinks between uses and definitions in the configuration.
- The ability to sort and filter on various columns to focus on particular aspects of the results which enables rapid interpretation of potentially large conflict sets.

Here the Visualizer shows the results of a functional comparison between supposedly equivalent PIX and Netscreen configurations.



The screenshot displays the InfoSector Visualizer interface with several key components:

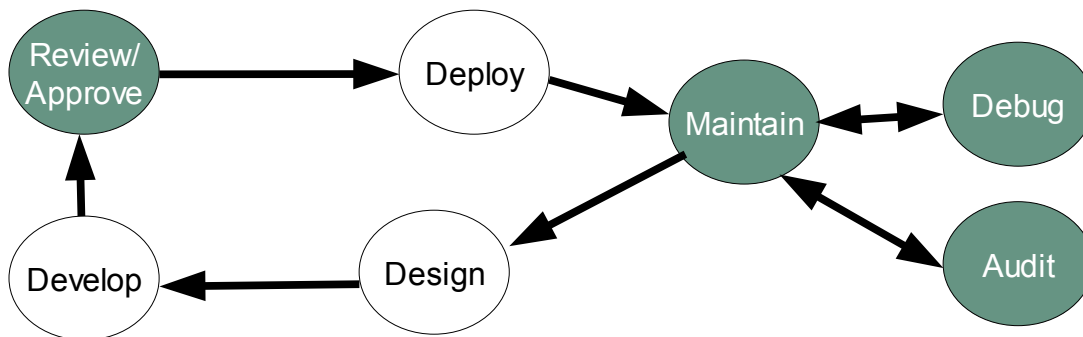
- Conflict Grid Summary:** A table showing the results of a comparison between configurations.
 

	Action	Protocol	Source Service	Destination Service	Source Address	Destination Address
1	default firewall	permit	TCP	Any TCP	80	ANY
2	default firewall	permit	TCP	Any TCP	10.10.51.0-10.10.52.255	10.10.200.172
3	default firewall	permit	TCP	Any TCP	10.20.0.0/16	
- Detailed Conflict Viewer with Config Line References:** A table providing more detail on the conflicts.
 

Source	Action	Protocol	Source Service	Destination Service	Source Address	Destination Address
Conflict	permit	TCP	TCP	TCP: 443	10.10.51.0-10.10.5...	10.10.200.172
Default	deny	IP	IP	IP	ANY	ANY
116	permit	TCP	TCP	TCP: 443	10.10.51.0-10.10.5...	10.10.200.172
- Config Inspector:** Two panes showing configuration files. The left pane shows PIX configuration (PIX Version 6.3) with network definitions. The right pane shows configuration commands for attack groups and policies.
- Config Viewer:** A pane at the bottom showing configuration lines with hyperlinks between named objects and definitions.

## Extend Your Processes

Many enterprises require standardized processes to impose the reproducibility in their operations. A standard workflow for network security design and implementation is depicted below.



Rather than forcing a new workflow onto your enterprise, use the InfoSector tools to make your existing processes faster and more accurate. In the workflow above, we recommend using InfoSector tools in the phases that are marked in green.

**Review/approve:** Augment your existing configuration review process to include an InfoSector policy constraint test against the proposed configuration to ensure that the new changes do not violate any organizational security policy assertions. The policy constraints can encode policy intelligence from different groups within the organization that are affected by the device in question. InfoSector can also be used to highlight functional changes between the new and original configurations. This functional change report can be used by the reviewer to detect unanticipated changes in packet processing.

**Maintain/Debug:** The IT staff is asked to debug network access problems and perform, or assist in, regular audits of security stance. While enhancing analysis in the review phase reduces the number of problems to debug, some problems will remain. The current process might use ad hoc network probe or a systematic scanning tool, such as nmap, to determine what packets are allowed from various points in the network. In addition to using this runtime information, query and tiling clarify how the currently configured devices should be processing packets. If SMTP traffic is traversing a security device unexpectedly, filtering for SMTP in the tiled view can reveal whether an early rule is broad and permits the SMTP traffic before a later rule denies it.

**Maintain/Audit:** The InfoSector Engine generates reports about devices through the network to create a trail of evidence. If you encode your desired network security stance as a set of filters and expected actions, the tiling analysis generates a report to highlight what rules apply to each filter set. By removing unrelated rules, you simplify the process of ensuring that the security policy implementation matches the security

policy requirements. Policy queries and constraints can also be used to automatically ensure that the configurations continue to meet security policy requirements. If the queries or constraints are performed periodically or at key points in the device life cycle, you can give the resulting reports to the external auditor as proof of security policy enforcement across your network.

## Contact Us

For more information on InfoSector and other tools and services from Network Geographics contact us at:

Network Geographics, Inc.  
60 Hazelwood Dr.  
Champaign, IL 61820  
888.276.2027

<http://www.network-geographics.com>

[contact@network-geographics.com](mailto:contact@network-geographics.com)