



The challenges of providing an open, available and secure education network.

Kelvin Rundle, CISSP
krundle@sourcefire.com

SOURCEfire



Agenda

- Challenges & opportunities for network security infrastructure refresh?
- Requirements for change
- Identifying potential solutions
- Example solution
- Lessons learnt



Challenges & Opportunities for Refresh

- Increasing diversity of network traffic
- 10 Gbps network speeds
- Cloud computing
- Resistant to change user base
- Increased risk in being seen as the instigator of network attacks
- Internal attacks/ network misuse impacting on service availability
- Constrained resources - operational staff
- Lack of centralised funding pool

3

SOURCEfire

Defining the Requirements for Change

- Providing an open, available and secure education network
- Increased need for bandwidth
- IP infringement management
- Improved control without degrading access
- Operational efficiency

4

SOURCEfire



Potential Solutions

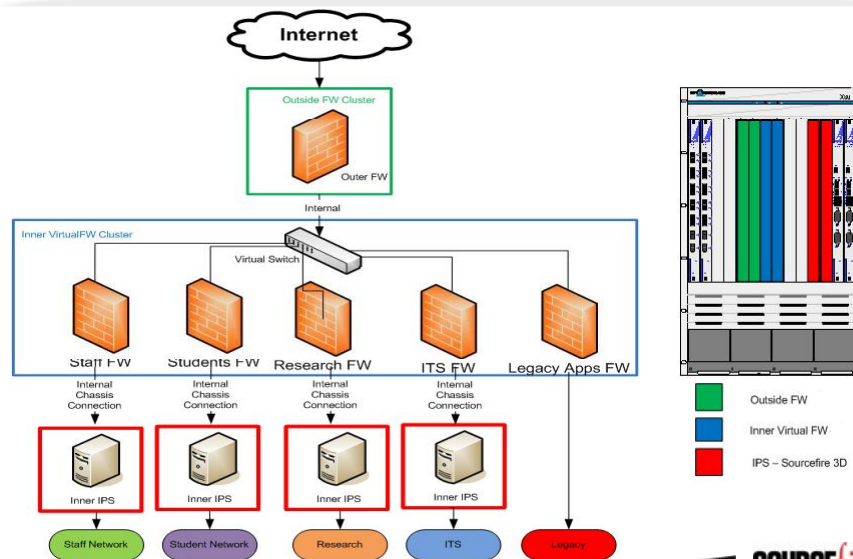


5

SOURCEfire



Example Solution



6

SOURCEfire



Why Sourcefire

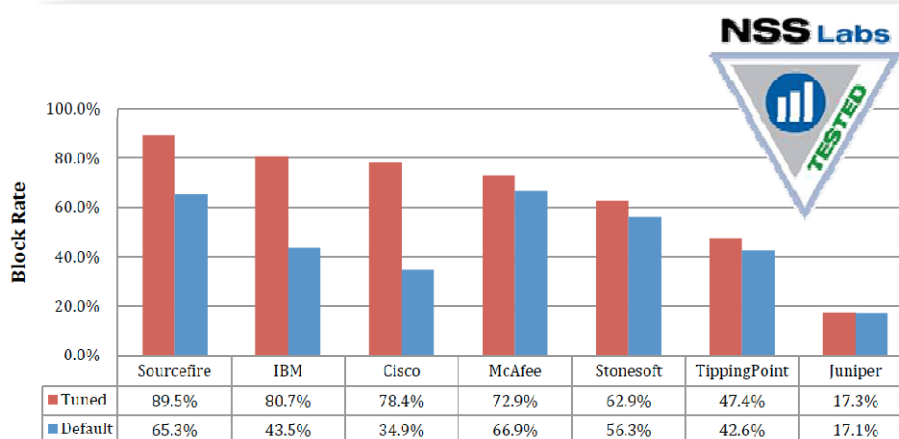
- Support for Chassis, Appliance and Virtual IPS
 - Same version, same functions centrally managed
- Drives operational efficiency through RNA/ RUA
 - Passive, real time, 24/7 network discovery of hosts and network applications (services) using protocol analysis
 - 99.9% event reduction – focus on what matters
 - Adds user identity to reduce investigation time
 - Full network visibility including protocol based P2P detection
- Owns Snort – 3.7 million downloads, 270,000 active users

7

SOURCEfire



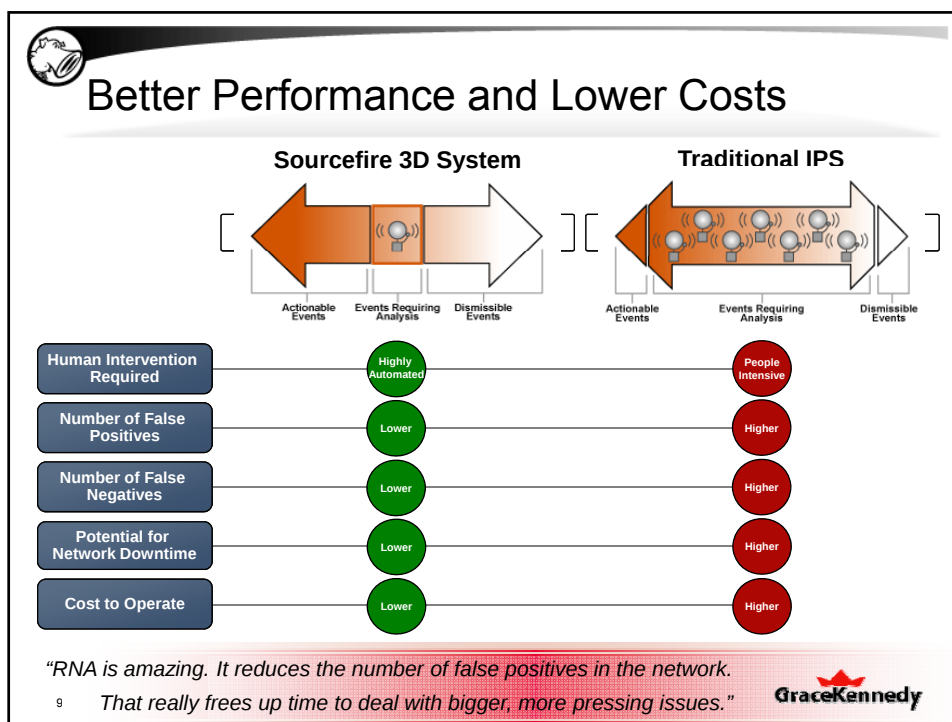
NSS Labs Group IPS Test - Block Rate Comparison



Source: Graphic used with permission by NSS Labs. "Network Intrusion Prevention Systems Comparative Test Results," December 2009.

8

SOURCEfire



Lessons Learnt

- 10 Gbps is expensive
- Increase visibility without having to control
- Increased visibility is key to security – cannot defend what you don't know
- Next gen firewalls are not there yet
- Operational efficiencies can be achieved

10

