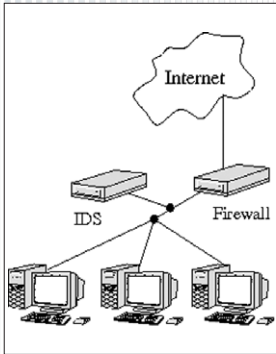


# Traffic Scanner

Dynamic growth of Internet traffic makes network security analysis increasingly difficult. Software-based network intrusion detection systems (IDS) have limited performance. CESNET started the development of hardware accelerated IDS using FPGA on COMBO6X card. This system is able to detect unauthorized access to computer systems and malicious network traffic such as viruses, Trojan horses and worms.



## Objectives

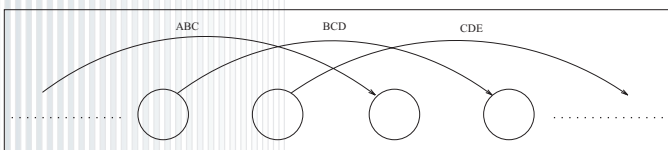
- Detecting unauthorized access to computer systems
- Detecting and blocking new viruses and worms
- Detecting and preventing piracy
- Preventing leaks of confidential data

## Architecture

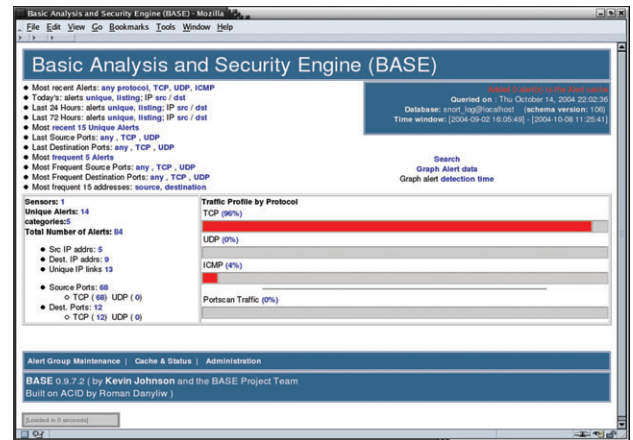
- **IBUF:** Network interfaces and input buffers
- **HFE:** Header Field Extractor - extraction of specified fields from the packet header
- **ROUND ROBIN:** Incoming packets are read from four input interfaces in a round robin manner
- **CLASSIFICATION UNIT:** Defines subset of patterns to be matched
- **PATTERN MATCH UNIT:** Search for specified patterns in packet payload
- **SWOBUF:** Send malicious packets to upper layers (Snort)

## Pattern Matching

- Improved NFA approach for pattern matching
- Multiple characters are processed within one clock cycle



- Prefix sharing for Snort strings - 50 % state space reduction
- Transition logic sharing
- Shared decoders implemented using BlockRAM
- Throughput up to 6.4 Gbps for the whole Snort database



## Features

- Passive monitoring of four Gigabit interfaces
- System throughput up to 3.2 Gbps
- Support for Snort rule set
- Exporting suspicious packets via PCI-X bus
- Substantially accelerated Snort

