



CNIE

Hardware based Network IPS

**Computer Networks and
Internet Engineering (CNIE)
Division**

C-DAC, Electronics City

and

C-DAC Mumbai

Background



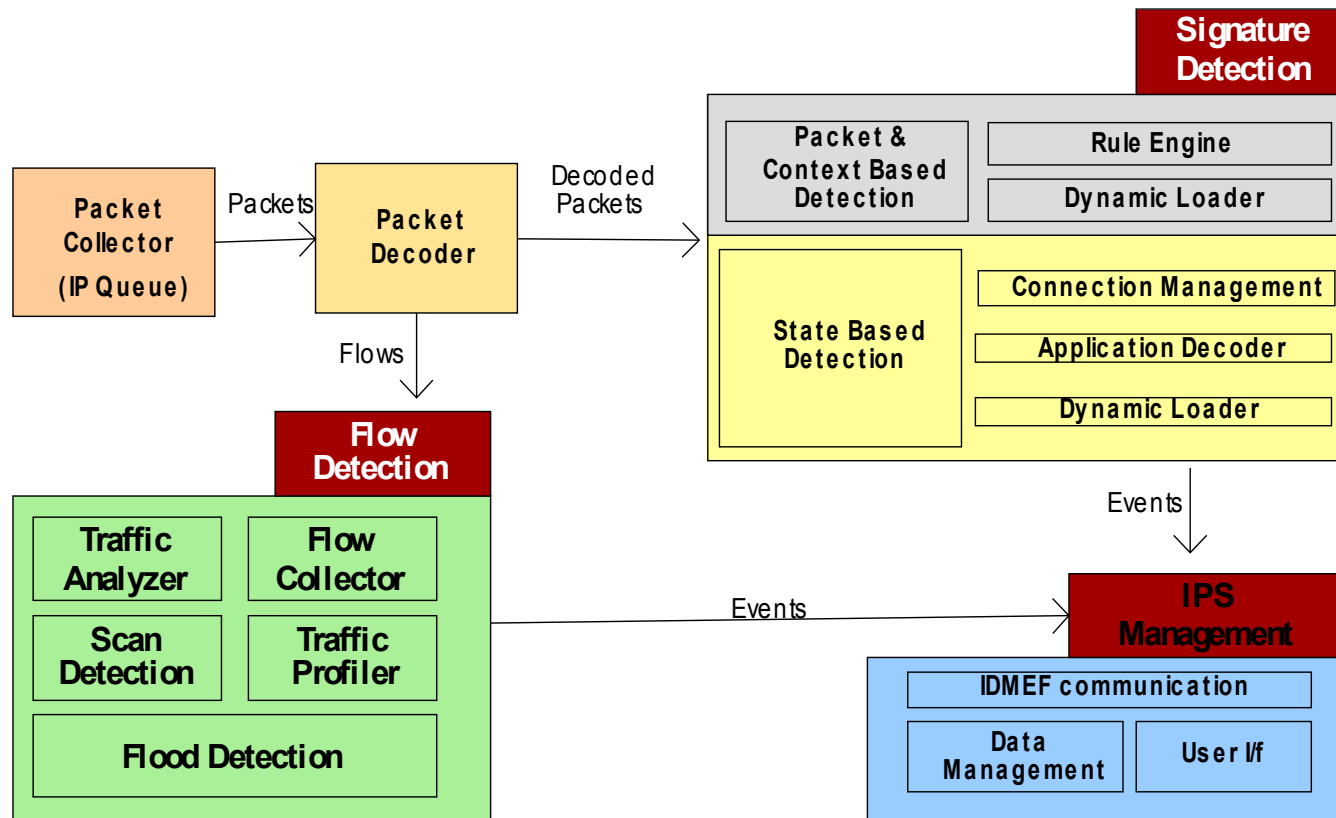
- Objective: To carry out research in intrusion prevention & content analysis to design and develop high-performance hardware based network intrusion prevention system.
- Duration: 18 months (from Feb. 2008)
- Expected Outcome:
 - Hardware based Network Intrusion Prevention System

Target Specifications



- **Functional**
 - Signature Protections
 - Server crack protection
 - Reconnaissance Detection
 - Stateful Inspection
 - Traffic Anomaly Detection
 - Flow Detection
 - Access control
 - In-line Operation mode
 - Alerting
 - Management
 - Comprehensive Threat Protection
- **Performance**
 - Maximum Through put (1-Gbps)
 - Latencies (< 250 micro Sec)
 - 10,00,000 Sessions

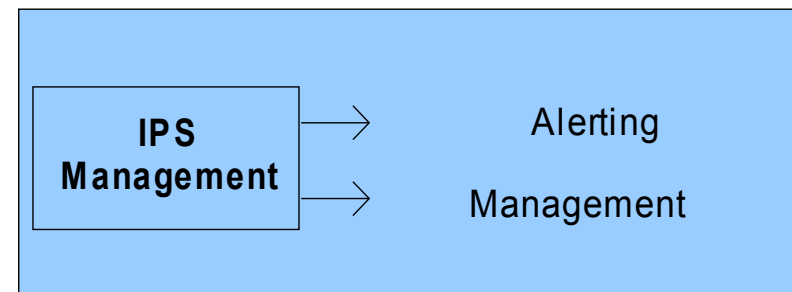
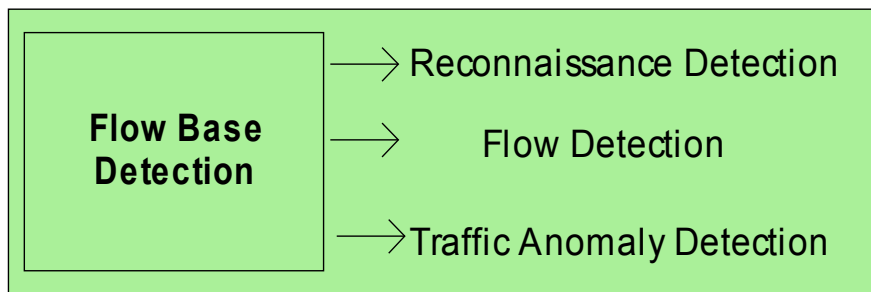
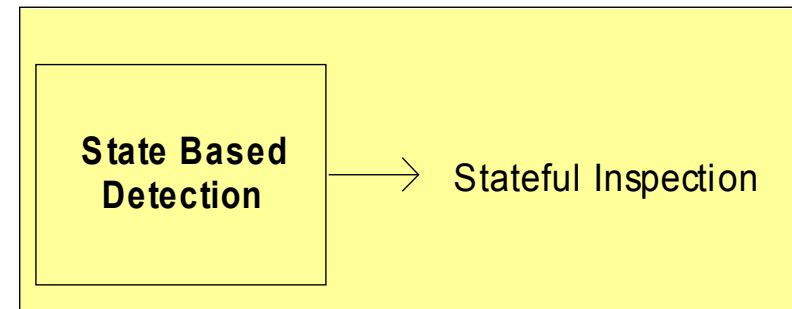
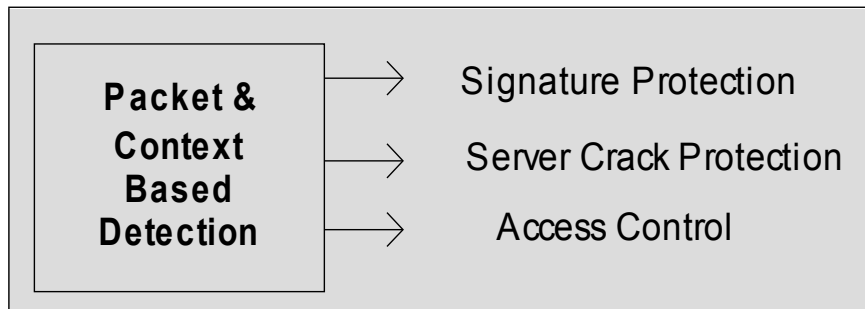
IPS Components



Specifications and Corresponding Components



CNIE



Current Status



CNIE

**Packet &
Context
Based
Detection**

Implemented,
tested,
interacted with user

**State Based
Detection**

Implemented,
tested for
HTTP

**Flow Base
Detection**

Implemented,
tested,
interacted with user

**IPS
Management**

Implemented,
tested

Additional Functionalities



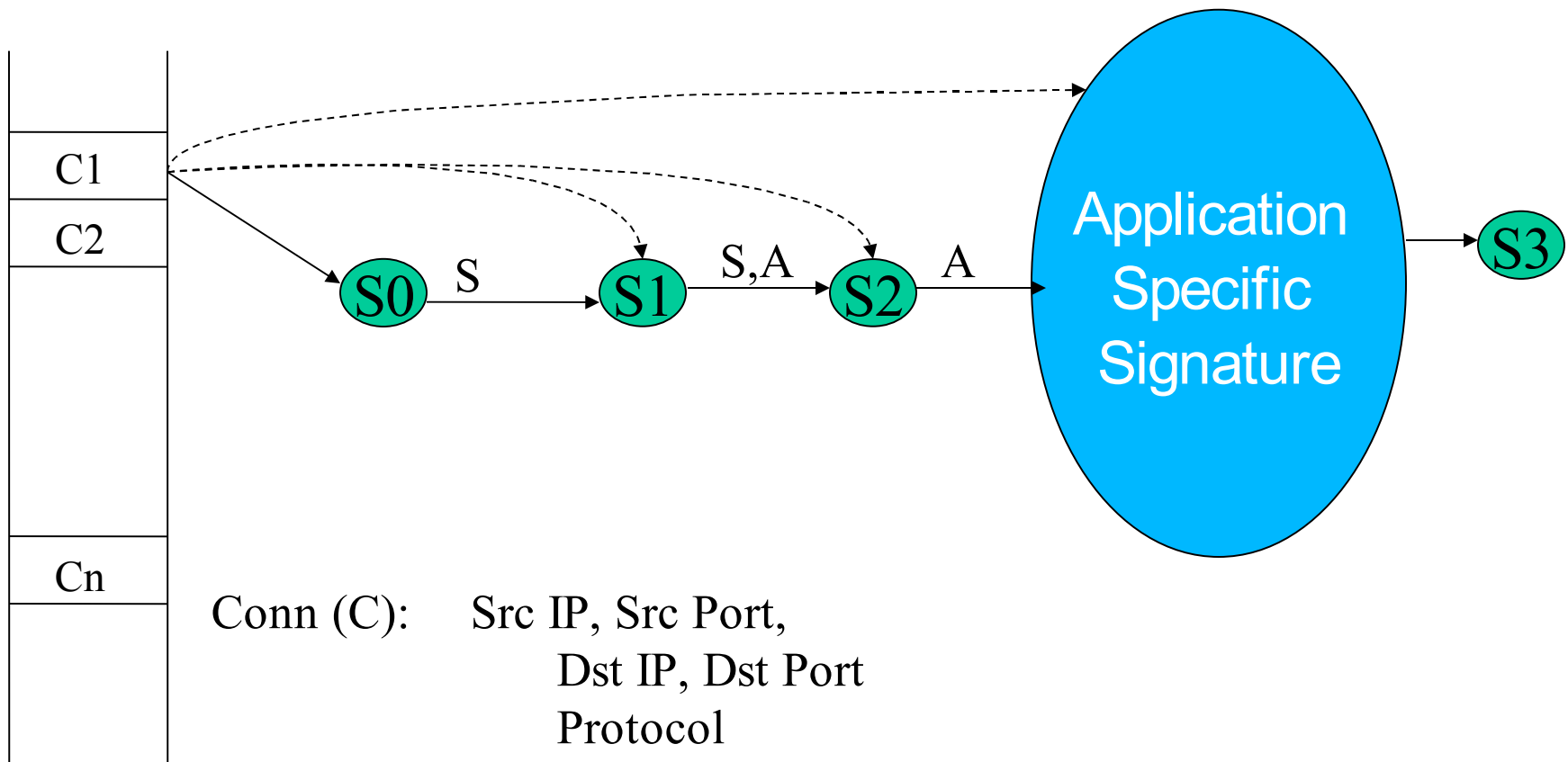
- Certain specifications mentioned below that are not the part of target specifications were also considered in development:
 1. Encrypted Traffic (SSL based attacks)
 2. Compressed HTTP Traffic
 3. Bandwidth analysis for security

Packet and Context based Signature Detection



- Packet and Context based signature detection engine completed
- Incorporated SNORT signatures (Jan 09 set)
- Carried out Signature validation (by crafting attacks, confirming the criticality of signatures)
- Currently, 296 IPS signatures (web & active-x (50%), smtp, ftp, rpc, scan)
- More SNORT IPS signatures to be validated and added
- System functional and Testing on-going

State Based Design



Modules of State Based Detection

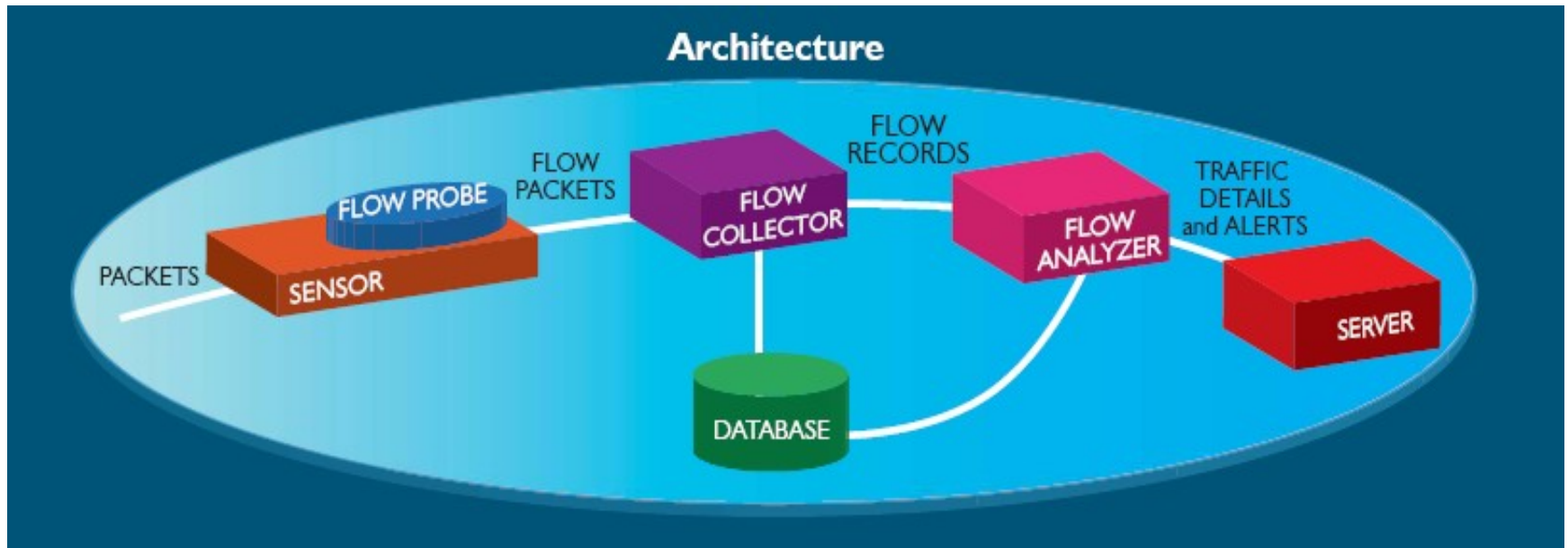


- Connection Management
 - Maintaining the connection table
- Application State Analysis (HTTP, SMTP and DNS)
 - Expansion of IPS Signatures with state knowledge
 - Application protocol parsing (keyword extraction)
- Implementation done for HTTP

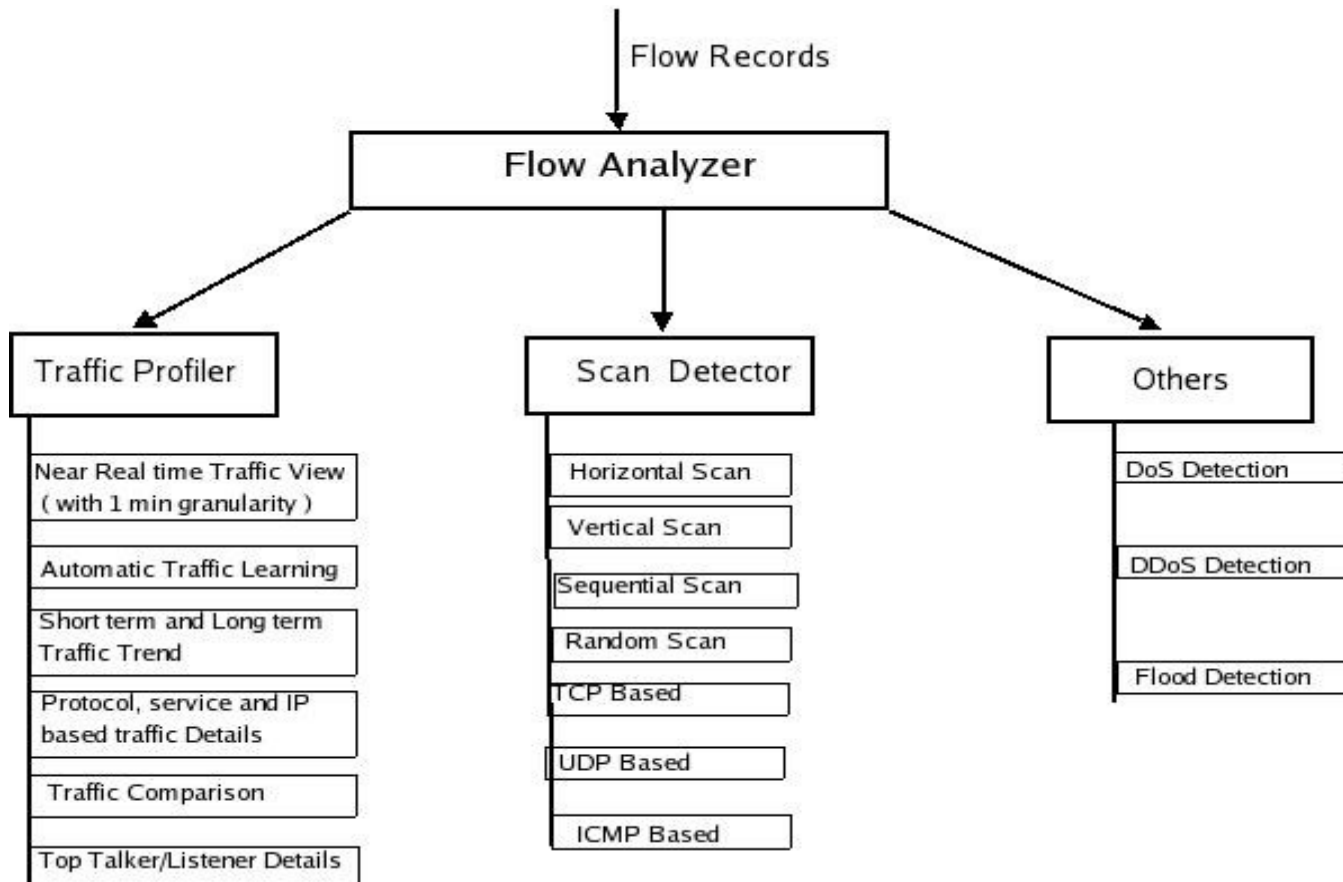
Flow Analyzer



CNIE



Flow Analyser



Flow Analyser



- Learning Phase
 - Configurable (hours/days/weeks)
 - Key parameters such as Flow aggregation, single packet counts, Avg Flow Duration, Avg Bytes per Packet
- Detection Phase
 - Scan detection, flood detection, traffic anomalies

Flow Analyser



- Capabilities
 - TCP, UDP and ICMP scan Detection
 - Vertical, Horizontal, Sequential and Random scan
- TCP Scan
 - TCP connect() scan
 - TCP SYN (Half-open) scan
 - Stealthy scan like inverse TCP flag scanning (FIN, NULL and Xmas tree scan)
 - ACK flag probe scanning and Window Scan
 - Scanning using non-standard packet size ('-- data_length' option in nmap)
- Flooding (TCP, UDP and ICMP)
- Limitations

Flow Analyzer



- IPFIX based implementation can reduce latencies – 50 seconds (under testing)
- Continuous learning model using moving average (under testing)
- Deployed different networks

Comprehensive Threat Protection



CNIE

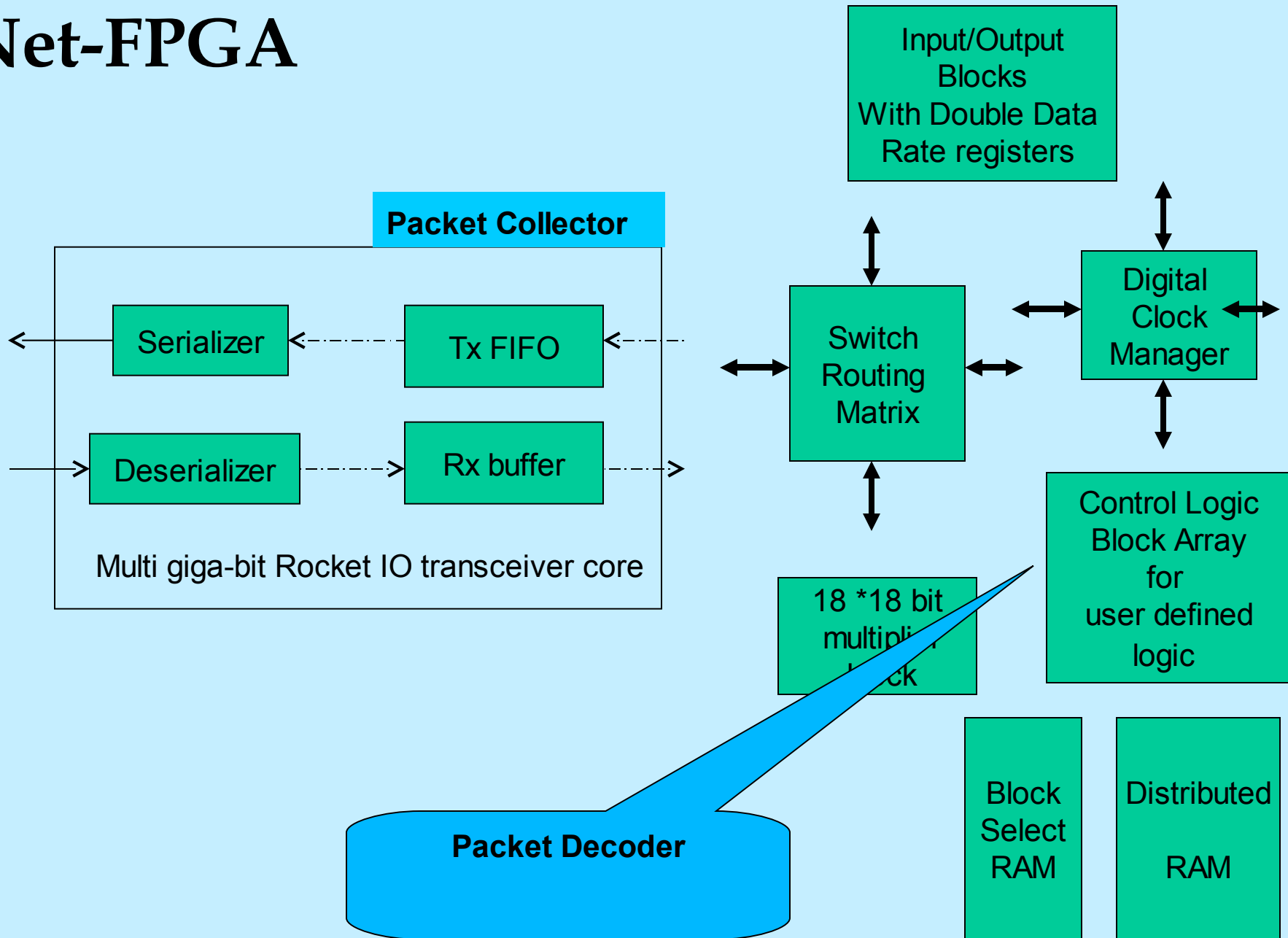
- Vulnerability Profile creation
- Validation of Intrusive events with respect to vulnerability profile and
- Generation of true IDS alerts

Hardware Approach



- Packet capture and decoding will be done in the NetFPGA board
- Host will carryout detection and prevention

Net-FPGA



IPS Management



- Data management
- Communication Interface
- Alerts and User Interface
- Work in progress:
 - Signature Update mechanism
 - Enhance of visualization & Query optimization
 - Signature Update mechanism

Other Challenges



- Handling SSL based Encrypted traffic..
- **Issue: Signatures can not be matched for the encrypted traffic**
- Studied Approaches followed by
 - Radware and
 - McAfee
- We are exploring Proxy based approach for our IPS

Other Challenges



- Handling compressed HTTP Traffic
- **Issue: Signatures can not be matched for the compressed traffic**
- Solution:
 - Identify compressed HTTP payloads and
 - Decompress to carryout signature detection

Test Cases



- Packet & Context based Signature Detection
 - 296 nemesis scripts used to generate attacks for 296 signatures
- State-based Signature Detection
 - 15 traffic dump of attacks against which HTTP based state detection is verified
 - Tested with traffic dump for compressed HTTP traffic
 - Stress testing carried out connection management

Test Cases



- Flow based detection
 - Test runs done using nmap, port-bunny and angry IP scanner for testing for various Scan detection
 - Test runs done using HPing for testing flood detection
 - Test cases for response time carried out (currently achieved 2 mts)

Testing Methodology



- Follow NSS guidelines for IPS evaluation
- Gigabit LAN testbed for performance evaluation
- Functionality testing along with user agencies based on intermediate milestones
- Third party testing

Acknowledgements



- Project Review and Steering Group Members
- Department of Information Technology, Ministry of Communications and Information Technology, Government of India, Delhi



CNIE

Thank You