



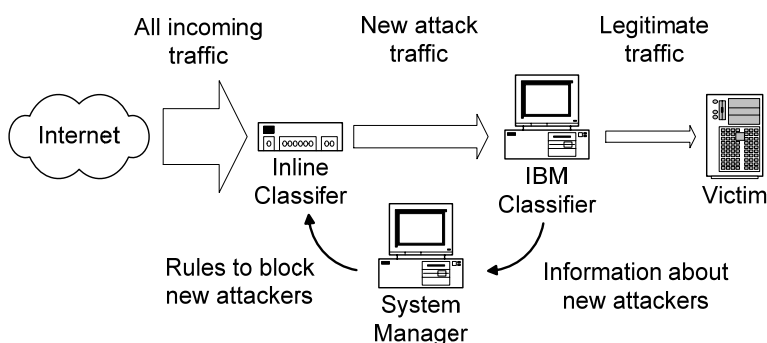
Motivation

- Diadem distributed firewall
 - ▶ Detects distributed attacks on networks
 - ▶ Determines appropriate reaction to attack
 - ▶ Applies reaction function on closest network node
- Diadem requirements for ingress firewalls
 - ▶ Update rules quickly in response to attacks
 - ▶ Need unconventional rules for new attacks
 - ▶ Filtering must occur at full line-speed
 - ▶ Cheap enough to deploy everywhere
- Proposed solution
 - ▶ Low-cost FPGA based firewall

Capabilities

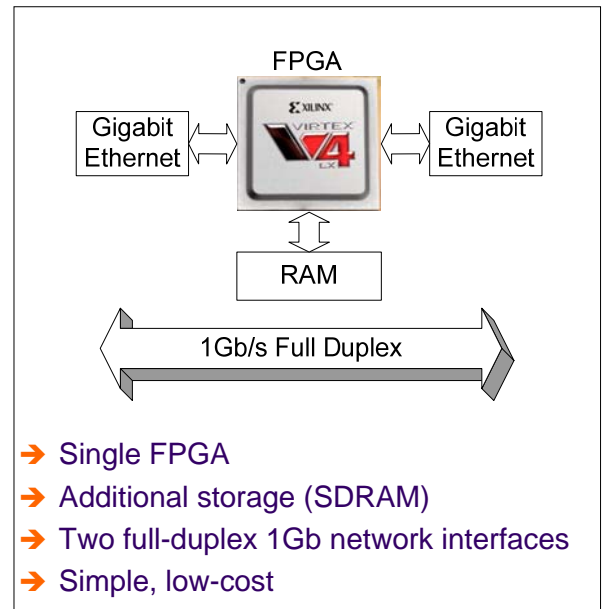
- Functionality of firewall changed through reconfiguration
 - ▶ Adjust firewall capabilities to react to attacks
 - ▶ Upgrade capabilities to mitigate new attacks
 - ▶ Switch configurations in less than 1 second
- Configuration 1: Standard firewall
 - ▶ 512 arbitrary rules
 - ▶ Actions: accept, drop, layer 2 redirect, rate-limit
- Configuration 2: DDoS firewall
 - ▶ 32 enhanced rules to block specific attackers
 - ▶ Each rule specifies over 2 million distinct addresses
 - ▶ Add over 1000 new attackers to rules per second

Operation



- Inline Classifier and IBM Classifier co-operate in attacks
 - ▶ Inline classifier removes traffic from known attackers
 - ▶ IBM classifier filters new attackers at lower line-rate
- Feedback through Diadem System Manager
 - ▶ New attack addresses propagated to Inline Classifier

Platform



- Single FPGA
- Additional storage (SDRAM)
- Two full-duplex 1Gb network interfaces
- Simple, low-cost

Performance

- Support worst-case traffic
- 1 Gb/s guaranteed throughput
- Full line-rate even for 64 byte packets

Integration

- Integrated into Diadem firewall
 - ▶ Acts as Standard Firewall Element
 - ▶ Managed over SSL connection
- Controlled remotely by System Manager
- Diadem API exposes firewall capabilities
 - ▶ Attack reaction optimised for firewall
 - ▶ Response split across multiple firewalls with different functionality

Summary

- High performance FPGA firewall
 - ▶ Runs at line speed
- Cheap, simple and flexible
 - ▶ Off-the-shelf components
- Reconfigurable for different scenarios
 - ▶ Adaptable and upgradeable