Terminus:
Towards a Network-Level Deployable Architecture Against Distributed Denial-of-Service Attacks

Felipe Huici and Mark Handley
Networks Research Group
Department of Computer Science

Overview

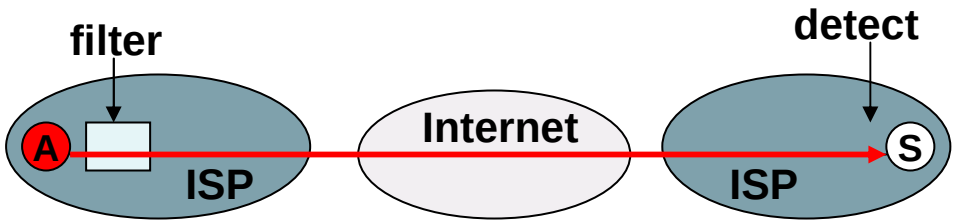
- Terminus architecture
- Protecting the architecture
- Performance results

Terminus Architecture

No Magic Bullet

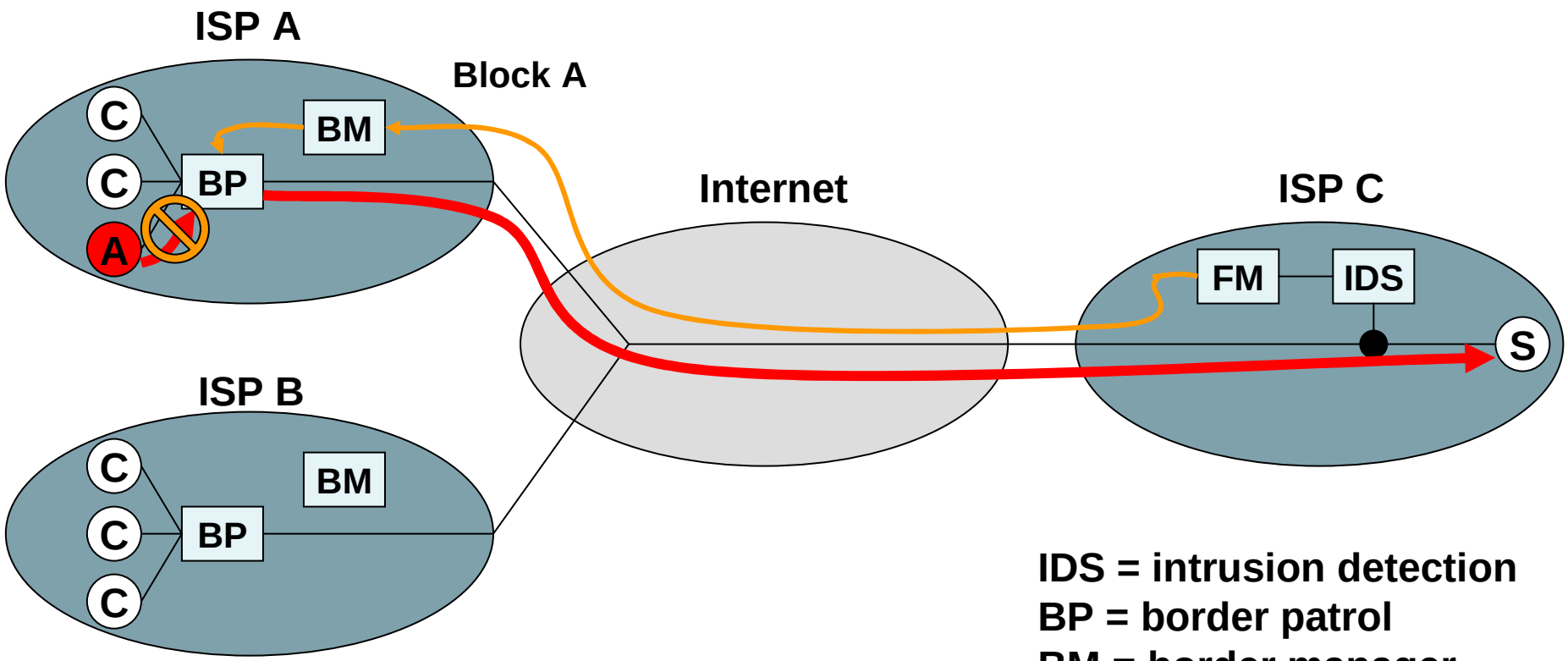
- Need minimal IP-level changes that can raise the bar for the attacker
- Difficult deployment issues:
  - Can’t change the hosts
  - Too expensive to change network core
- These point towards reactive solutions at edge ISPs

Architecture Introduction



- General idea
  - Identify attack traffic at destination
  - Request that traffic be filtered
  - Block attack traffic at source ISP's filtering box
- Pretty obvious…
  - Architecture's novelty lies in meeting these criteria robustly and with minimum mechanism.

Terminus Architecture



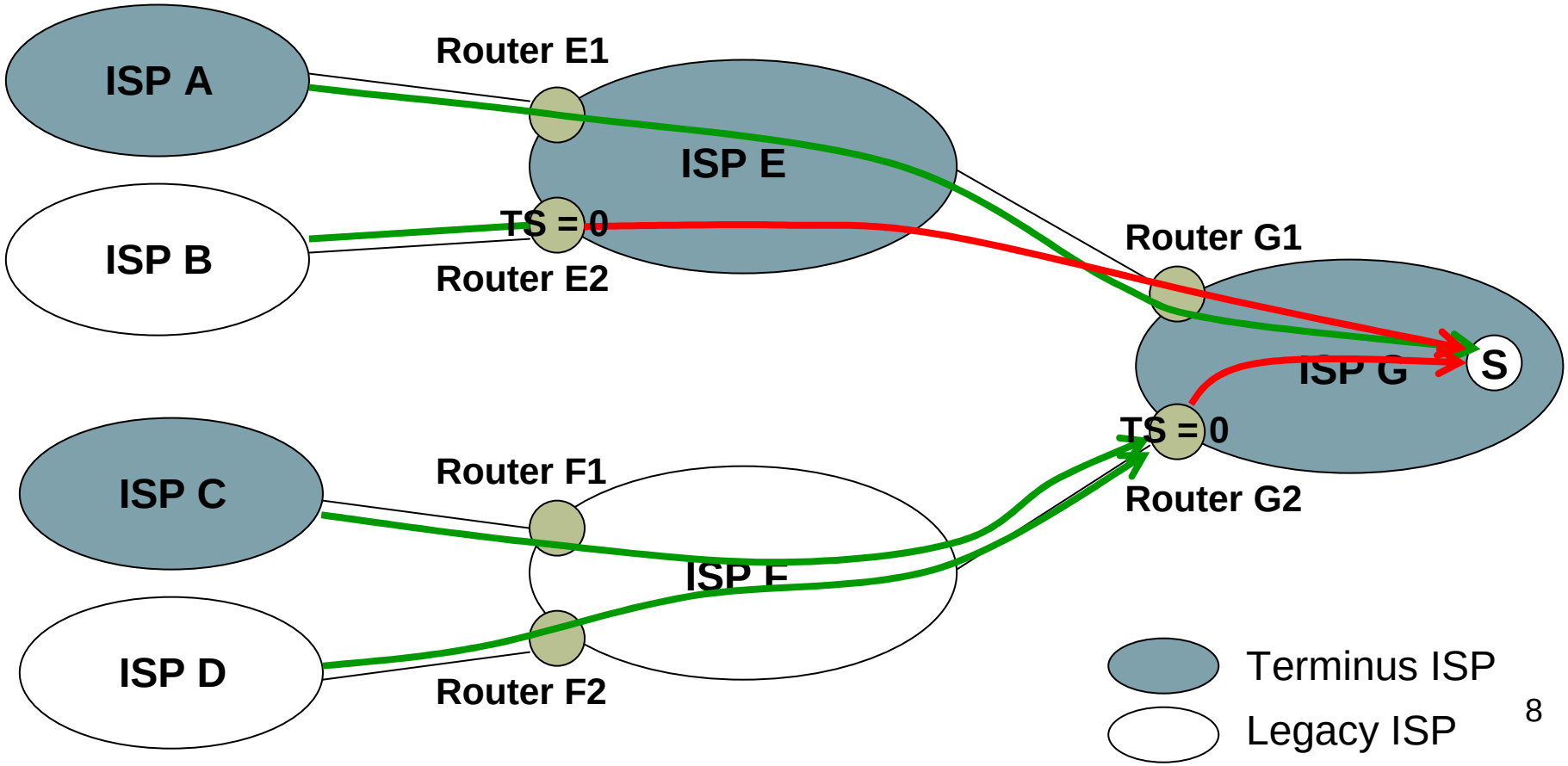
IDS = intrusion detection
BP = border patrol
BM = border manager
FM = filter manager

Traffic Marking

- Problem
  - Need to know origin of attack packets
    - Must send filter request to the right place
  - IP source address cannot be trusted
    - Can be spoofed
- Solve by adding a “true-source” bit to packets
  - Only Terminus ISPs with ingress filtering can set bit

Preventing True-Source Bit Spoofing

- Edge router at Terminus ISP connected to legacy ISP unsets this bit for all packets

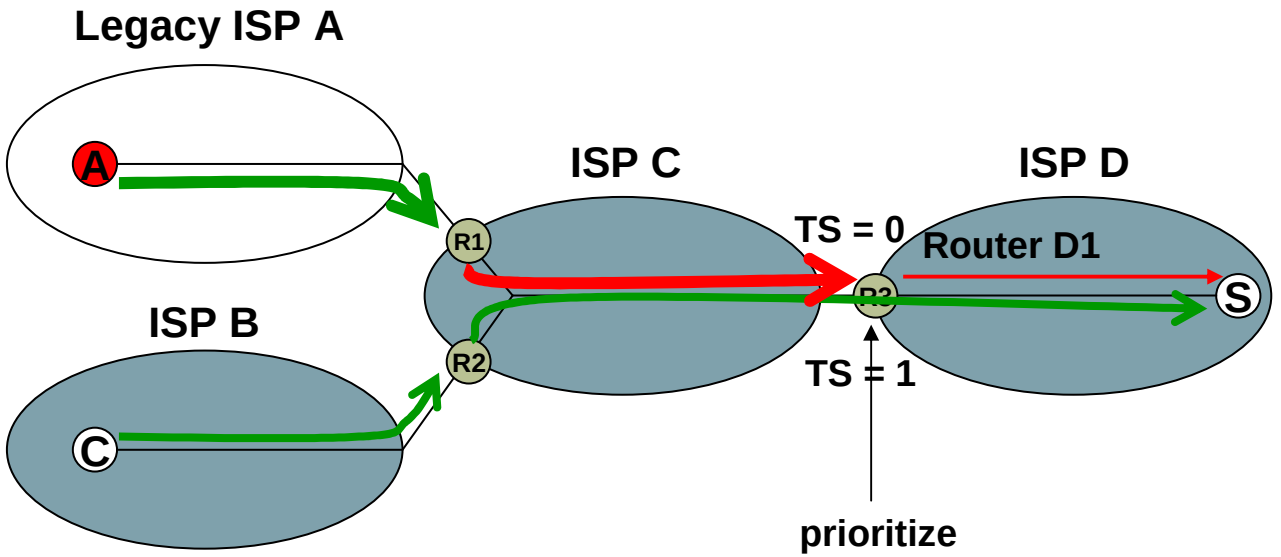


Protecting the Architecture

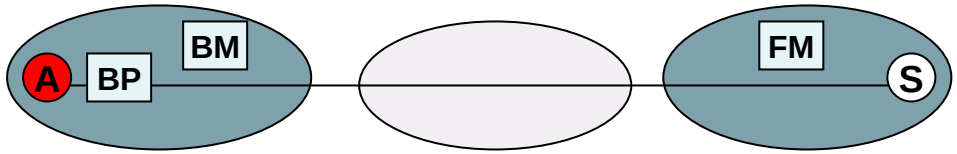
1. Attackers in legacy ISPs
2. Malicious filtering requests
3. Spoofed traffic triggering filtering requests
4. Reflection attacks

Problem 1: Defending Against Attackers at Legacy ISPs

- During initial stages, legacy ISPs will be the norm
- Use true-source bit to prioritize traffic at the destination ISP's peering routers
  - Implement true-source bit as a diffserv code point

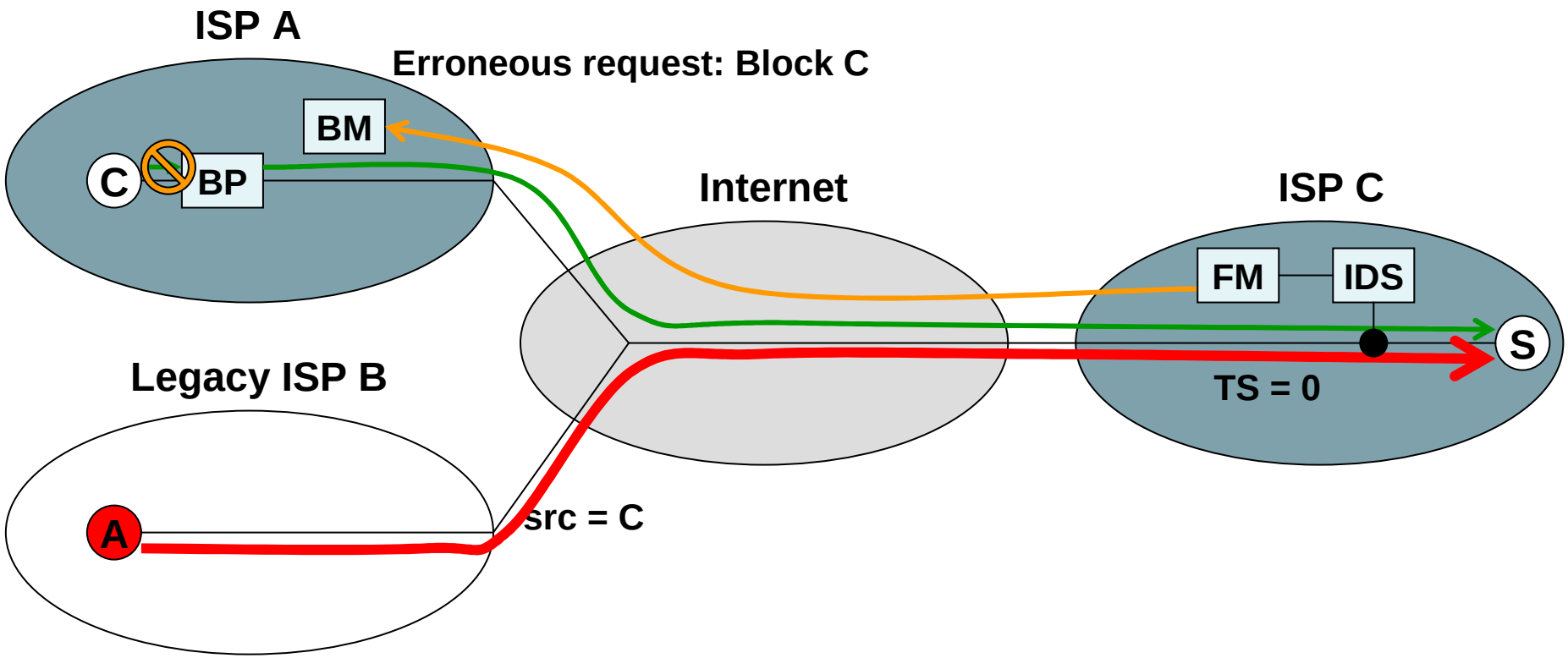


Problem 2: Filtering Requests



- Where to send request?
  - Digitally-signed p2p mechanism used to distribute source-to-BM mappings
- Where can it come from?
  - Same mechanism distributes signed destination-to-FM mappings
  - BM checks if FM allowed to request filter for destination
- BM must validate source of a filtering request
  - Cannot rely on TS=1 since path may be asymmetric
  - Simple nonce exchange validates FM

Problem 3: Triggering Requests Through Spoofing

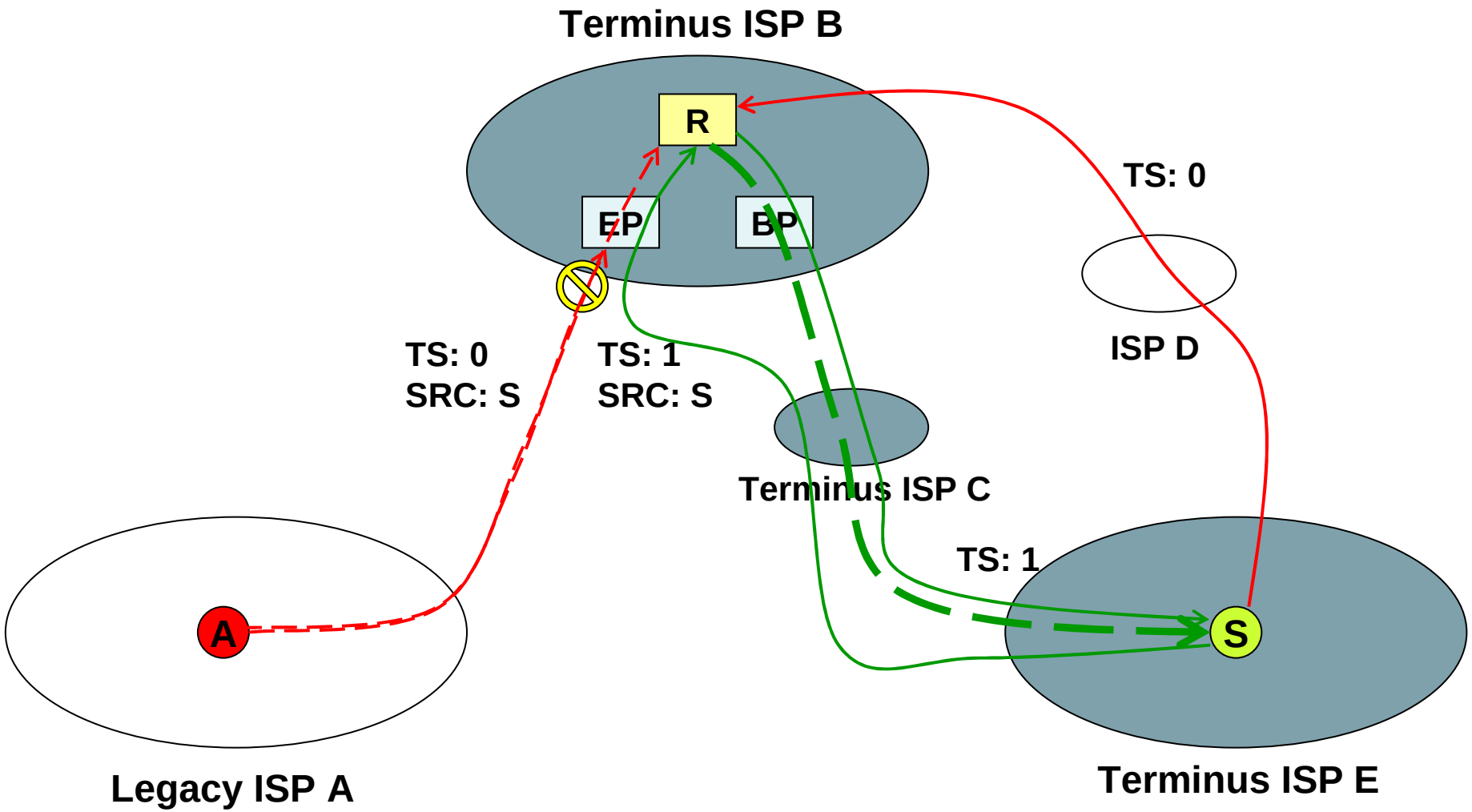


Scenario: attacker is in a legacy ISP that allows spoofing
Solution: do not issue filtering request if TS = 0

Problem 4: Reflection Attacks

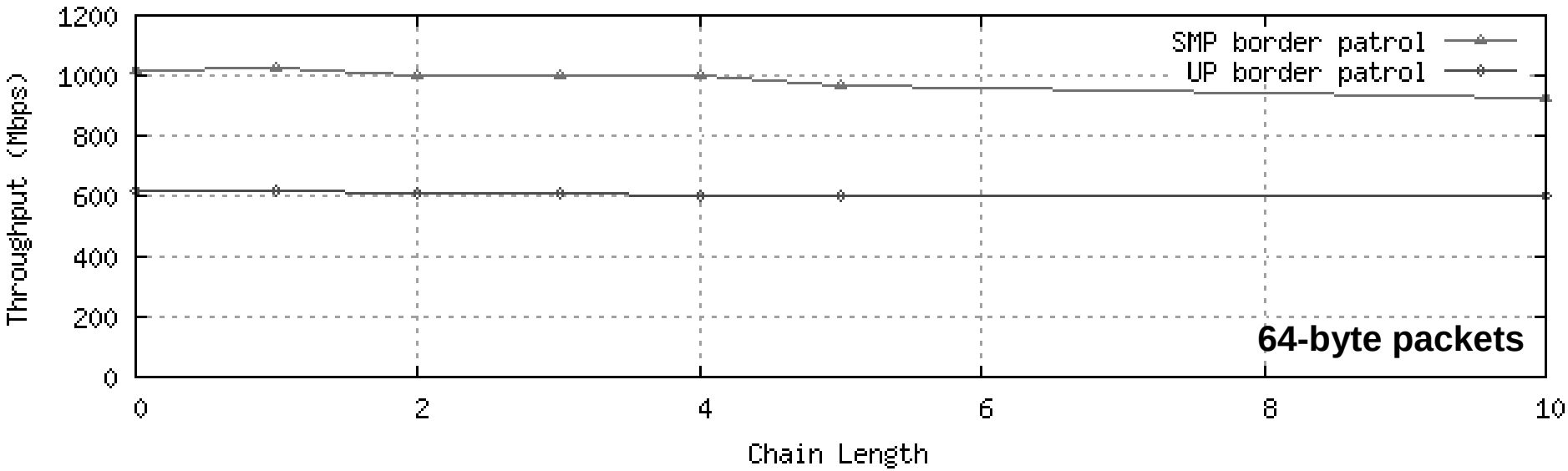
- In a reflection attack
  - The attacker spoofs requests using victim's address
  - The requests are sent to third-party servers (reflectors)
  - Response flood overwhelms victim
- For most part, Terminus unaffected, except when:
  - Reflector is in a Terminus ISP
  - Terminus path between reflector and victim

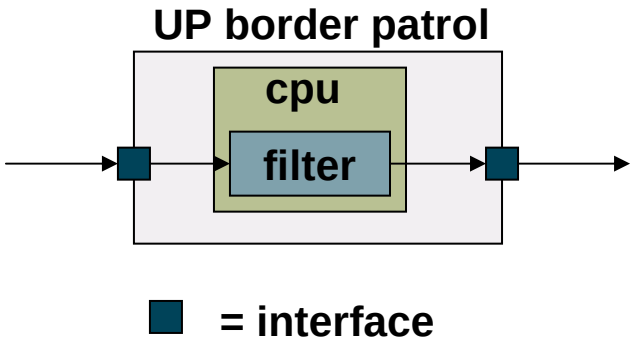
Reflection Attacks

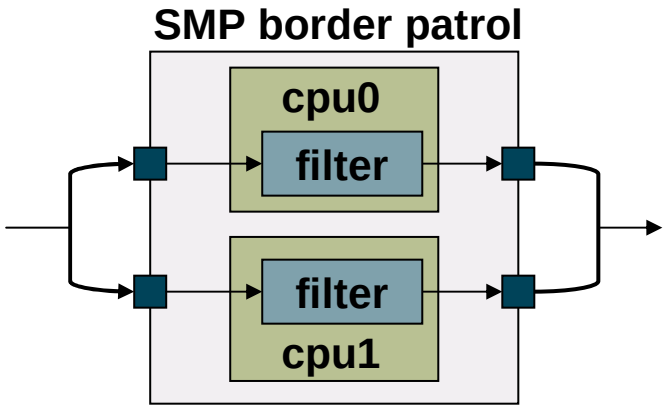


Performance Results

Border Patrol Parallelism







Summary

- Presented Terminus, a deployable architecture against large DDoS that uses *minimum* mechanism
- Robust against attack
- Performs well even on cheap hardware

Terminus: God of boundaries

Paper under submission, URL:
http://www.cs.ucl.ac.uk/staff/F.Huici/publications/terminus-lsad.pdf

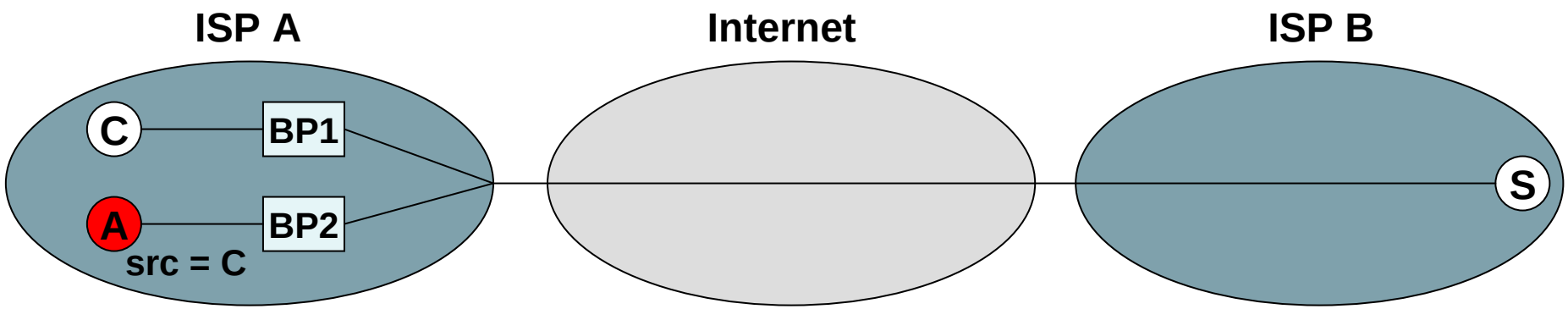
Additional Slides

Motivation

- Majority of operators spend more resources on DDoS than any other security threat
- Attack firepower increasing
- Majority of ISPs mitigate attacks by filtering all traffic to victim
- Attacks happen in the thousands per day

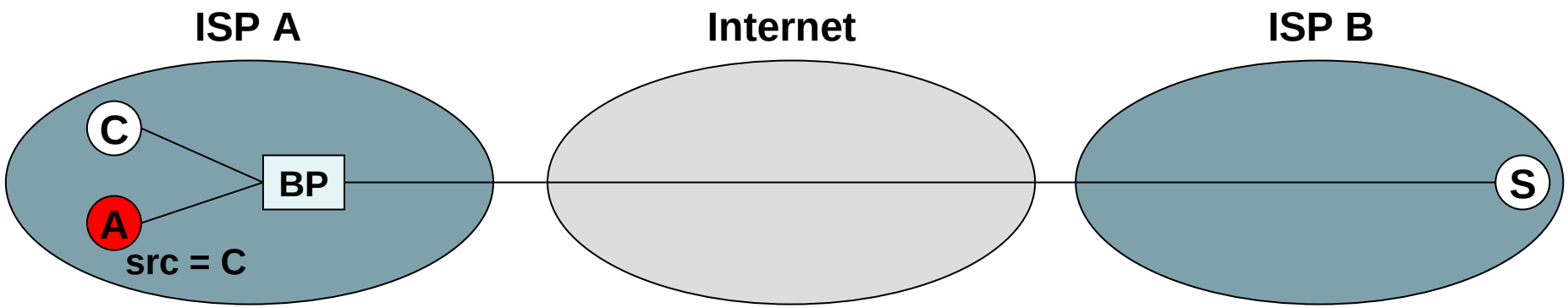
Sources: *Symantec Internet Security Threat Report XI and Arbour Worldwide Infrastructure Security Report 2006*

Triggering Requests Through Spoofing



Scenario 2: Attacker is in same Terminus ISP as victim, but behind different BP

Triggering Requests Through Spoofing



Scenario 3: Attacker is behind same BP as victim

Control Plane Performance

- Filter manager
  - 75,000 requests/sec
  - Biggest botnets about 1,500,000 hosts, filter in 20 secs
- Border manager
  - 87,000 requests/sec
- Border patrol
  - 354,000 requests/sec (in batches of 100 filters)

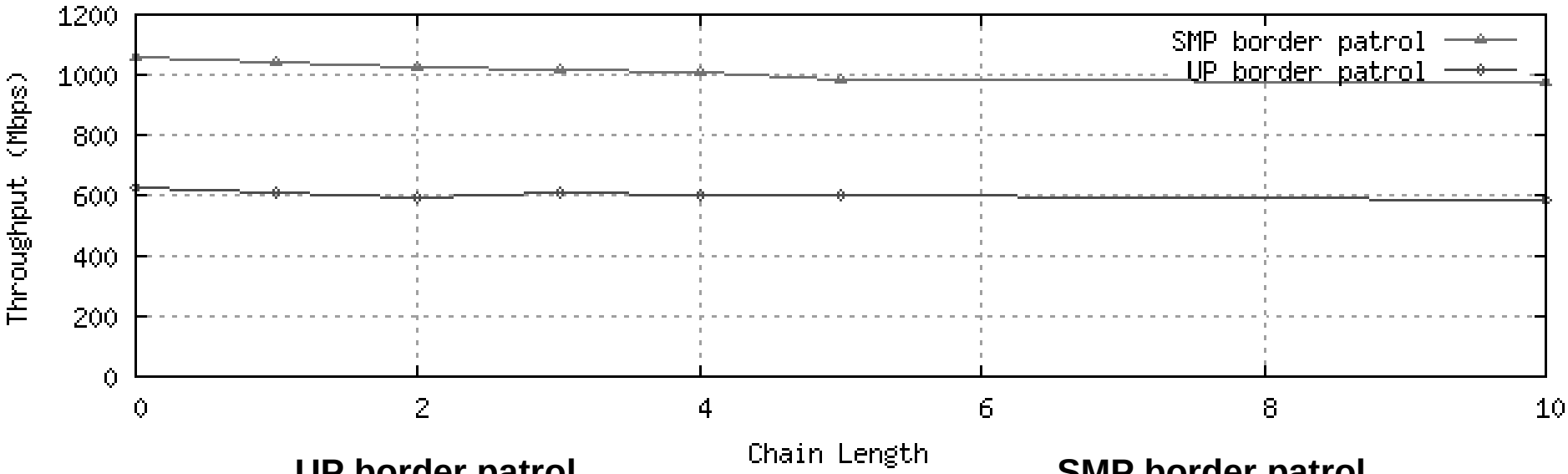
Setup

- Testbed
  - Non-blocking Force10 E1200 switch
- Computers
  - Inexpensive 1U servers
  - Two dual-core processors at 2.66GHz
  - Two dual-port Gigabit Ethernet cards
- Software
  - Linux 2.6
  - Click modular router for forwarding plane
  - C++ for control plane

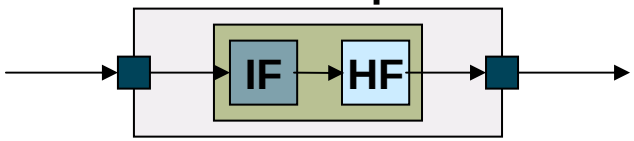
Protecting Terminus' Components

- Border and egress patrols
  - Not externally visible
- Border manager
  - Off fast-path
  - Low return on investment for attacker
- Filter manager
  - Off fast-path
  - Only has to handle incoming nonces, which have priority at edge

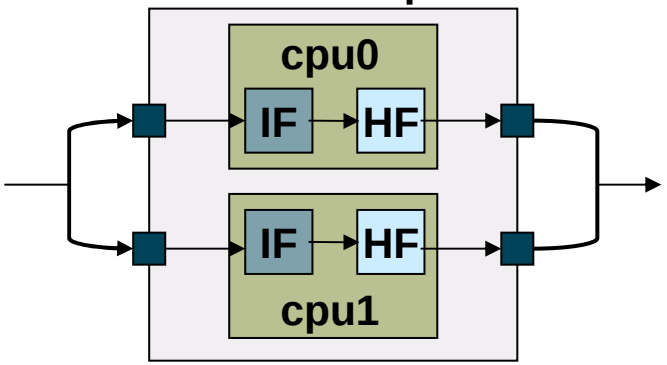
BP Forwarding Plane – HashFilter



UP border patrol

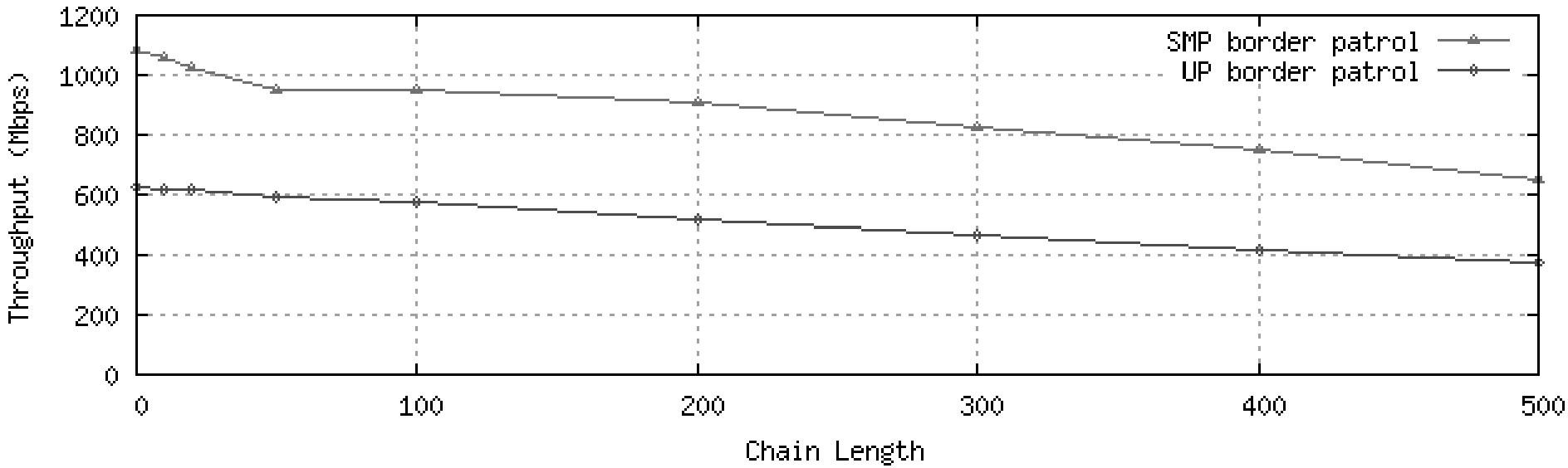


SMP border patrol



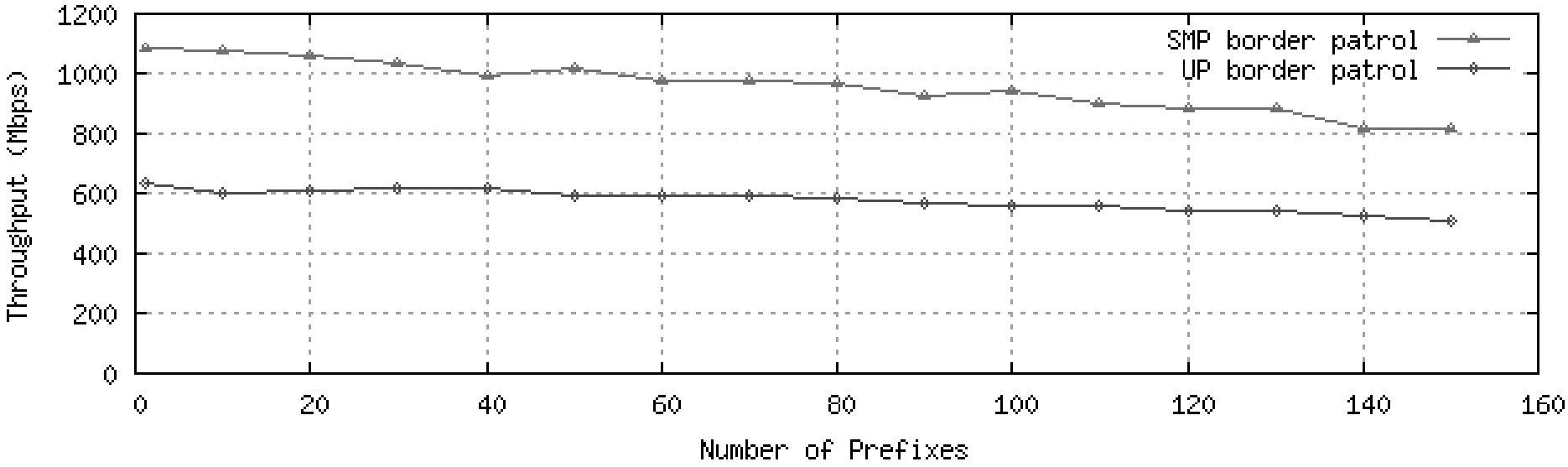
IF = Ingress Filter
HF = Hash Filter
■ = interface

BP Forwarding Plane – HashFilter



- **All filters hash to same chain**
- **All packets fully traverse chain before being forwarded**

BP Forwarding Plane – IngressFilter



- **Packets force look-up against all prefixes before being forwarded**