AINA

DeMONS: A DDoS Mitigation NFV Solution

Vinícius F. Garcia, Guilherme de F. Gaiardo, Leonardo da C. Marcuzzo, Raul C. Nunes and Carlos Raniery P. dos Santos

Universidade Federal de Santa Maria

SEDES SAPIENTIÆ

1960

Summary

- **Introduction**
- **Related Works**
- **DeMONS: DDoS Mitigation NFV Solution**
- **Evaluation**
  - Evaluation Methodology
  - Comparative Tests
  - Reputation Systems Test
- **Conclusion**

Introduction

- **Distributed Denial of Service (DDoS)**
    - IP spoofing and real source IPs
- **DDoS mitigation**
    - Capacity based
    - Filter based
- **Network Function Virtualization (NFV)**
    - Decoupling network functions from its associated hardware
    - Network services creation (Service Function Chaining)
- **Security provided by NFV**
    - Adaptability to network changes
    - Security Service Chaining (SSC)

Related Works

- **Holistic DDoS mitigation using NFV**
    - Generic architecture to attacks mitigation
    - Treatment by network layers
- **VFence: A Defense against Distributed Denial of Service Attacks Using Network Function Virtualization**
    - SYN Flood attacks mitigation
    - Three way handshake, blacklists and whitelists
- **A Collaborative DDoS Defence Framework using Network Function Virtualization**
    - SYN Flood attacks mitigation
    - Multidomain VFence application

Related Works

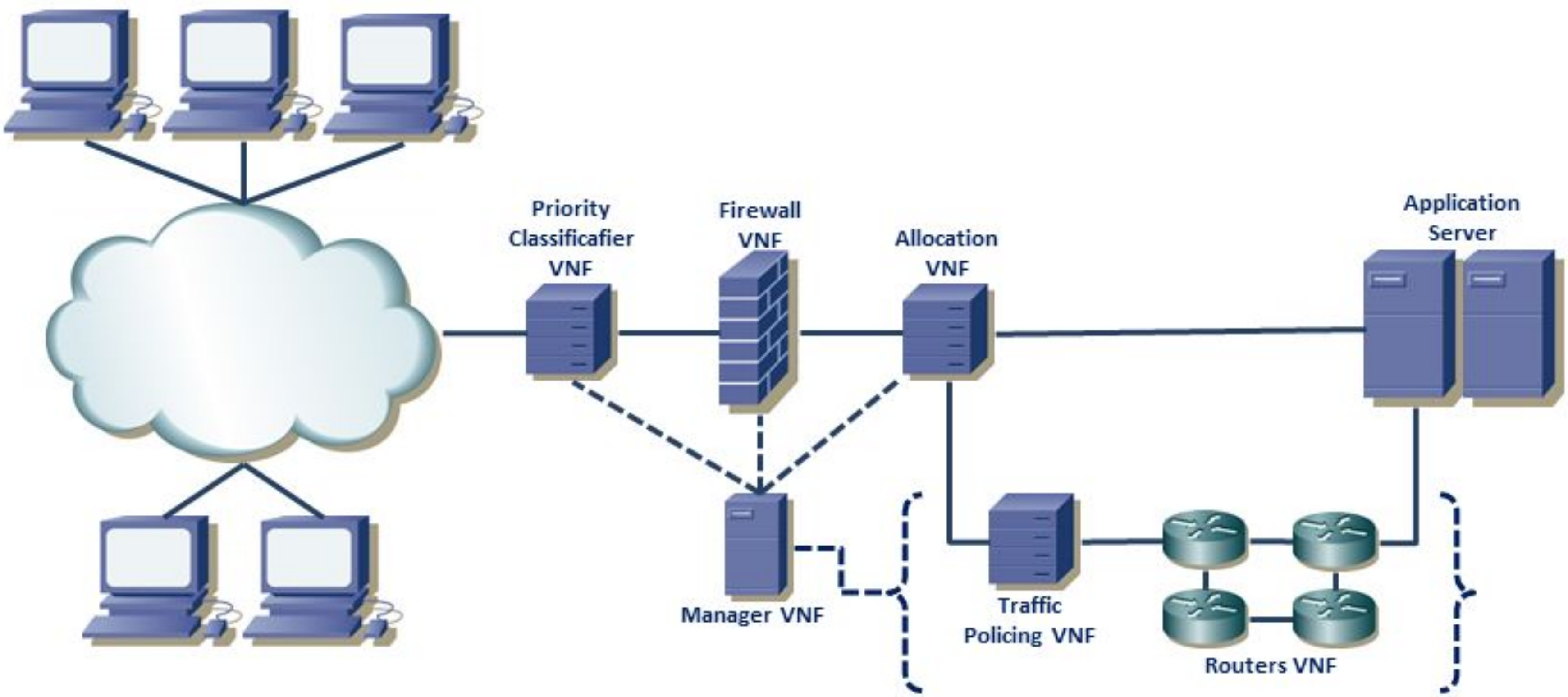
VGuard: A distributed denial of service attack mitigation method using network function virtualization

- **DDoS attacks mitigation**
- **Uncertainty levels to determine if flows are malicious**
  - Specially appropriated to botnets attacks
- **Based mostly on capacity**
  - Only discards flows when there are a 100% certainty
- **VGuard architecture**
  - Traffic classifier
  - Firewall Virtualized Network Function
  - DDoS Virtualized Network Function
  - High and low priority tunnels

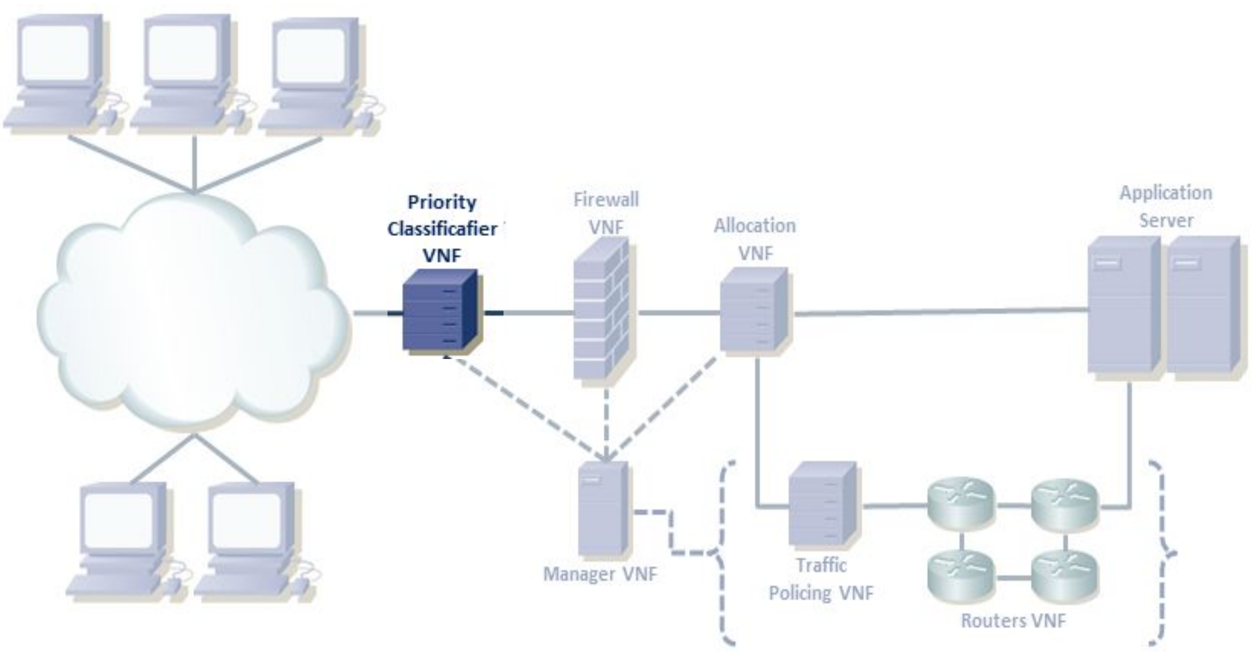
DeMONS: DDoS Mitigation NFV Solution

- **DDoS attacks mitigation**
- **Uncertainty levels to determine if flows are malicious**
  - Specially appropriated to botnets attacks
- **Hybrid approach - based on capacity and filter**
  - Discards all the flows considered 100% malicious
  - Partially discards flows considered suspects in a overloaded scenario

DeMONS: DDoS Mitigation NFV Solution



DeMONS: DDoS Mitigation NFV Solution



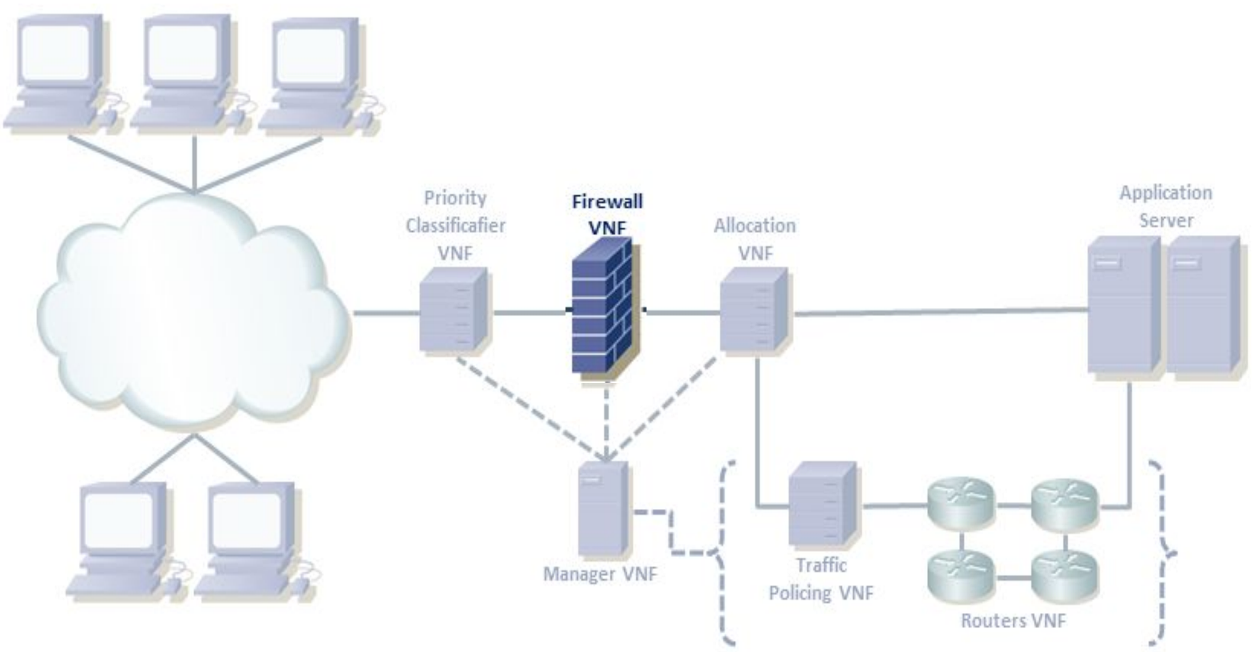
Priority classifier

Determines the flow priority according to its confidence ([0;1])

May use IDS, IPS or DPI techniques

User policies may be included

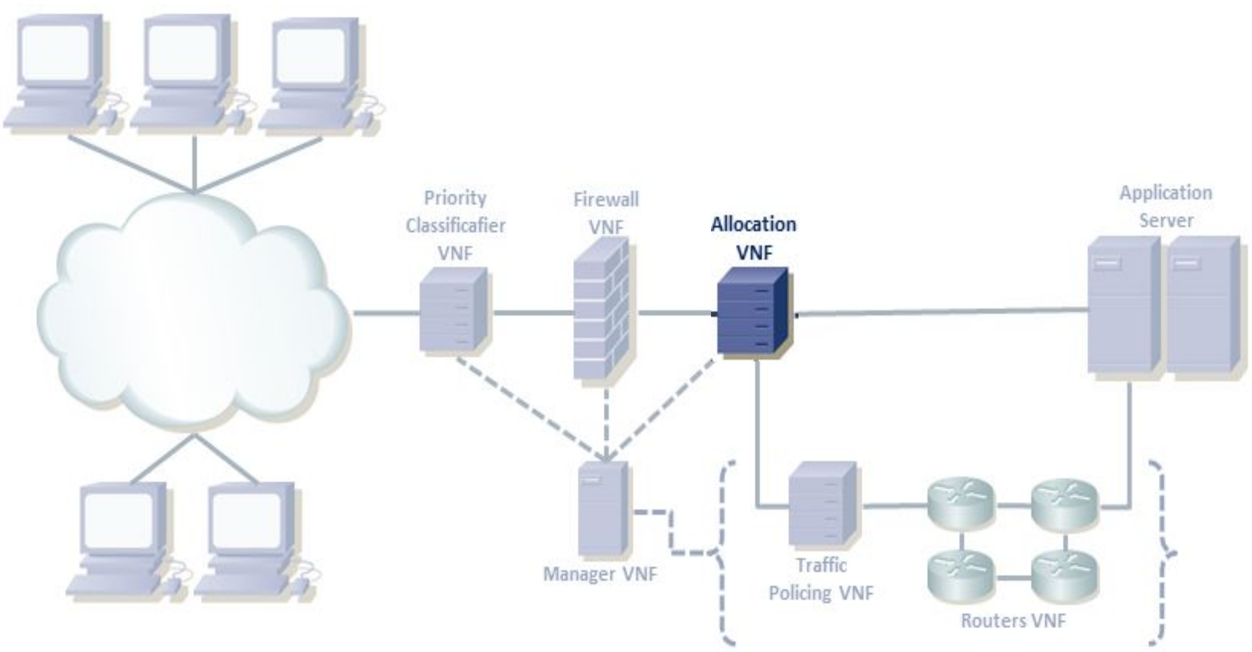
DeMONS: DDoS Mitigation NFV Solution



Firewall

Blocks all 0 priority flows

DeMONS: DDoS Mitigation NFV Solution

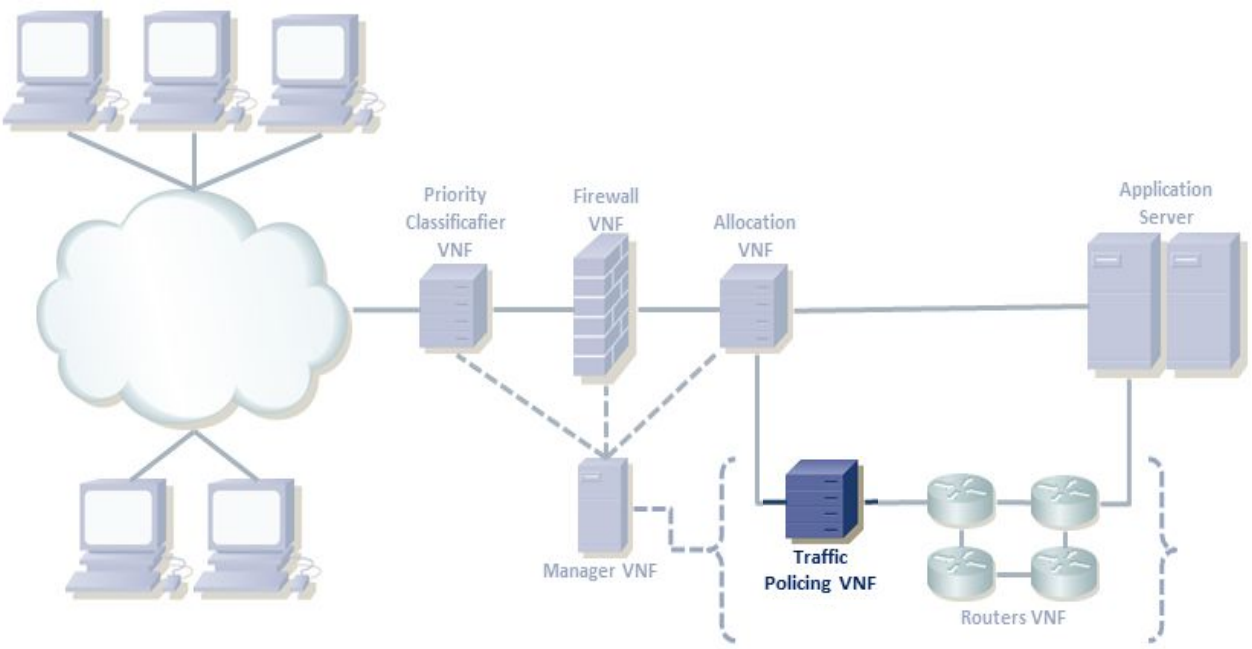


Allocation

Executes an allocation algorithm to insert flows in the low or high priority tunnel

Dynamic algorithm - adapts to network changes

DeMONS: DDoS Mitigation NFV Solution



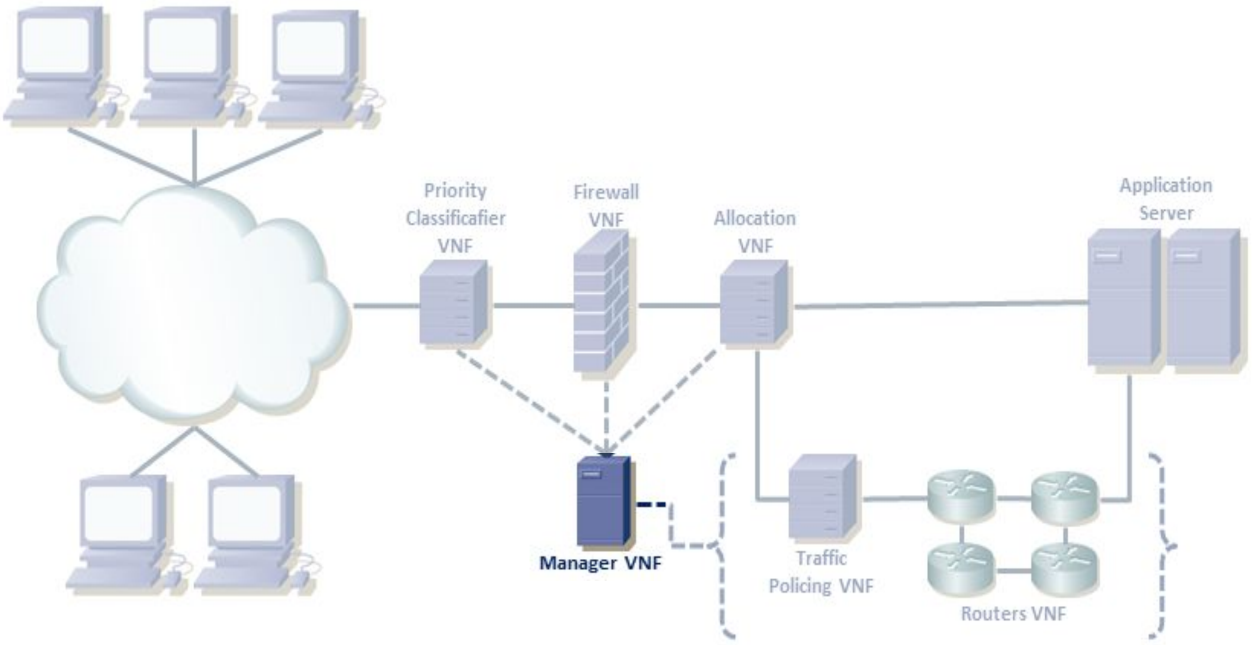
Traffic policing

Operates in the low level tunnel

Applies partial discarding policies

Activated in an overloaded tunnel scenario

DeMONS: DDoS Mitigation NFV Solution



Manager

It does not replace the MANO, but indicates actions according to the security topology analysis

Turns up or down the low priority tunnel

Request to MANO scaling operations

DeMONS: DDoS Mitigation NFV Solution

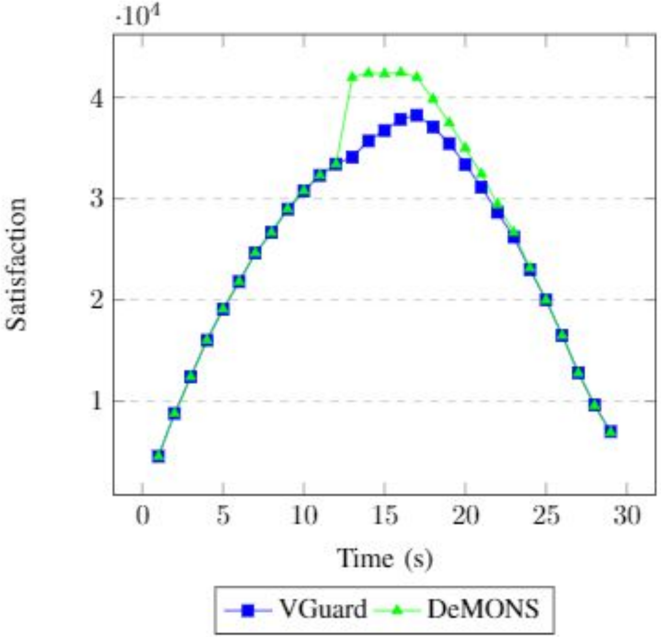
Flow allocation algorithm		
	VGuard	**DeMONS**
Underload	Alternate	Alternate or in the available tunnel
Traffic limitation	Selective mode	Selective mode
Flow balancing	-	In the selective mode entrance
Selective mode analysis	Priorities average	Lowest priorities
Overload	Unconditional allocation	Conditional allocationl

Comparative Tests

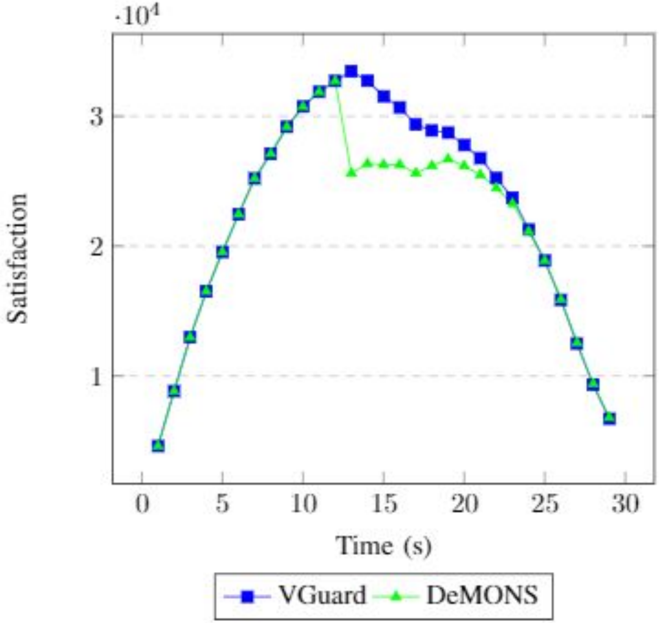
- **DeMONS**
  - Minimum discarding of 10%, medium restirctivity
- **VGuard**
  - Original dynamic flow allocation version
- **Tests configurations**
  - Tunnel capacity (both): 50 Mbps
  - Selective mode: 97%
  - Benign flows: 100 Kbps - degradation of 10 Kbps (0,4 <= p <= 1)
  - Malicious flows: 100 Kbps - no degradation until the attack ending (0,1 <= p <= 0,4)
  - Duration: 30 seconds
- **Evaluation metric**
  - Aggregated and weighted satisfaction

Comparative Tests

- Scenario 01: benign flows and maximum total traffic of 99.1 Mbps



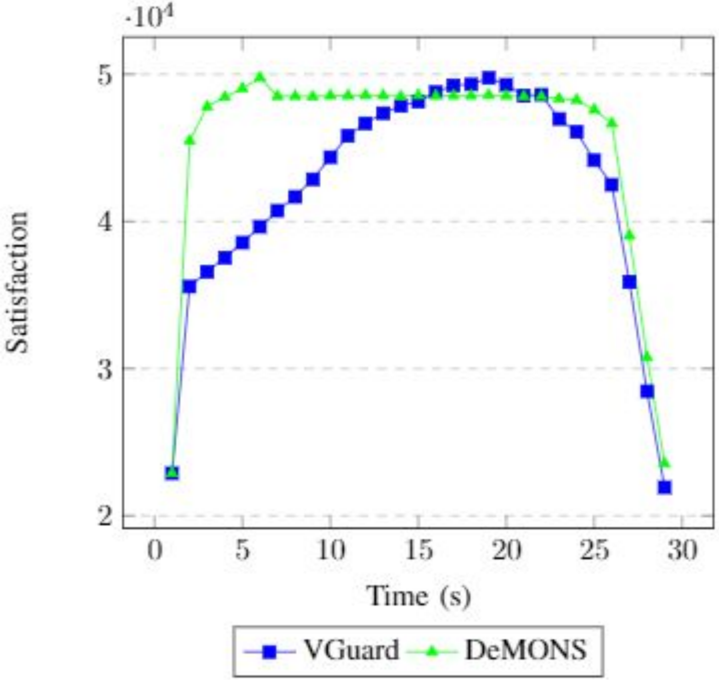
High Priority Tunnel



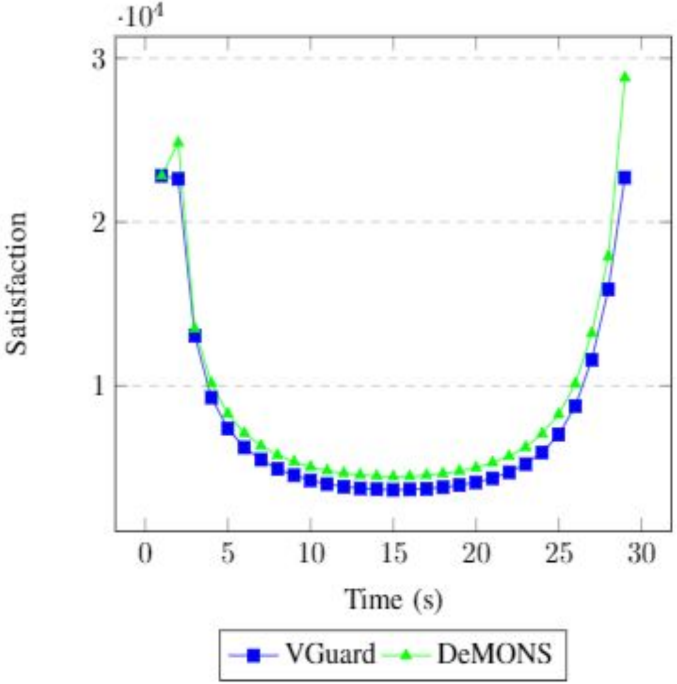
Low Priority Tunnel

Comparative Tests

- **Scenario 02: benign flows and maximum total traffic of 506 Mbps**



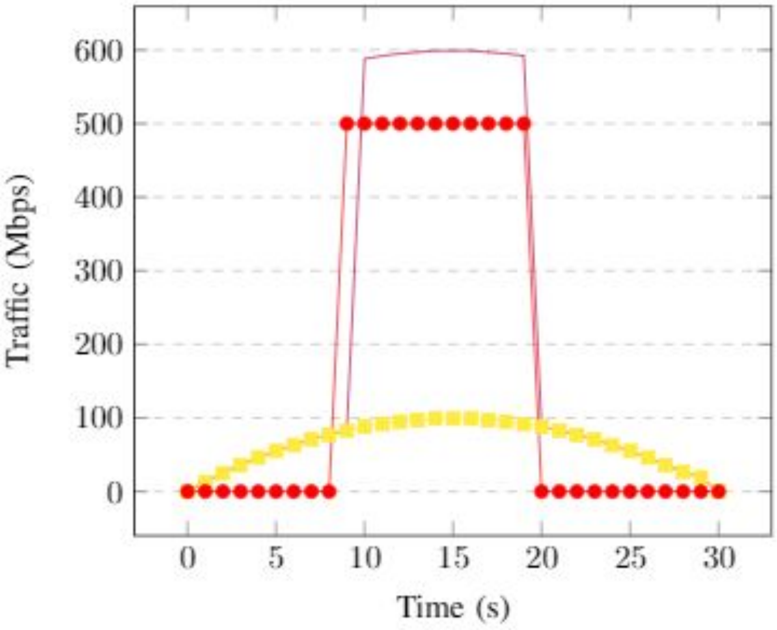
High Priority Tunnel



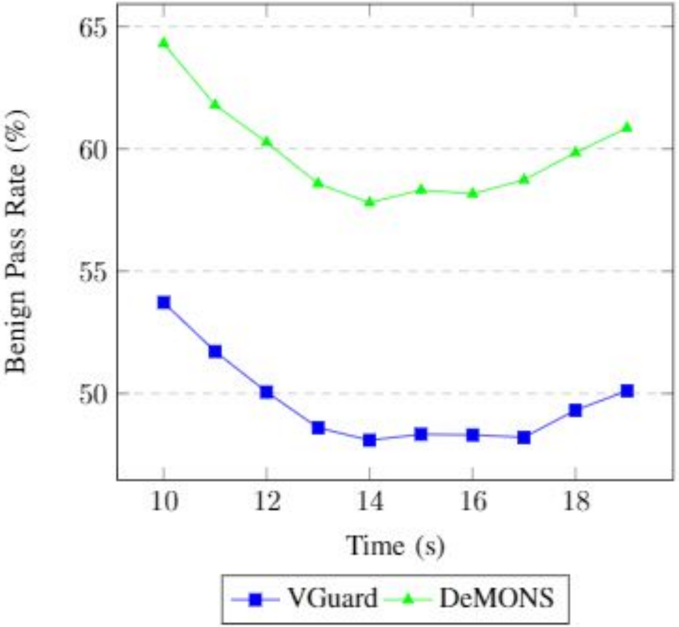
Low Priority Tunnel

Comparative Tests

- **Scenario 03: DDoS flood attack**



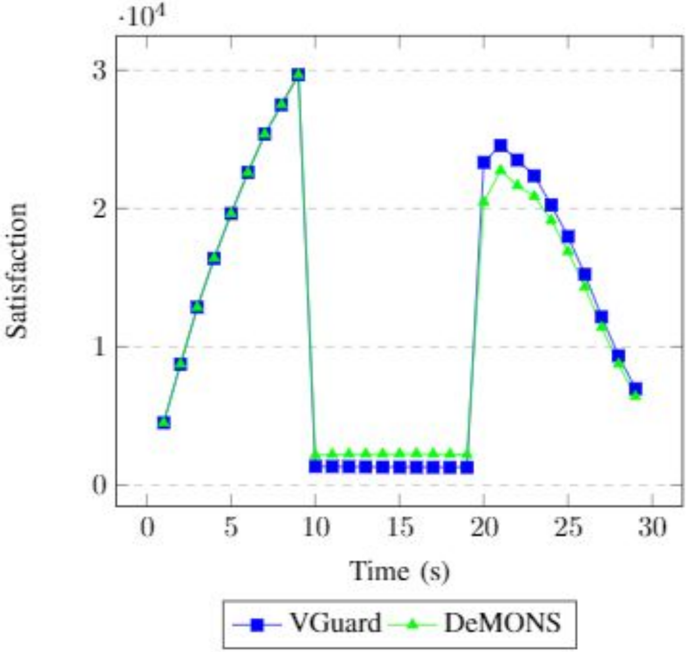
Attack Scenery



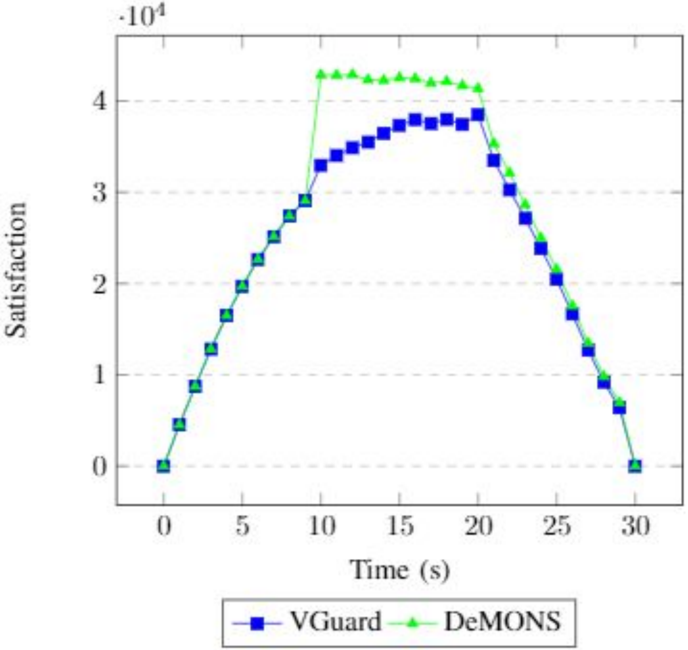
Benign Traffic Delivery

Comparative Tests

- **Scenario 03: DDoS flood attack**



Low Priority Tunnel



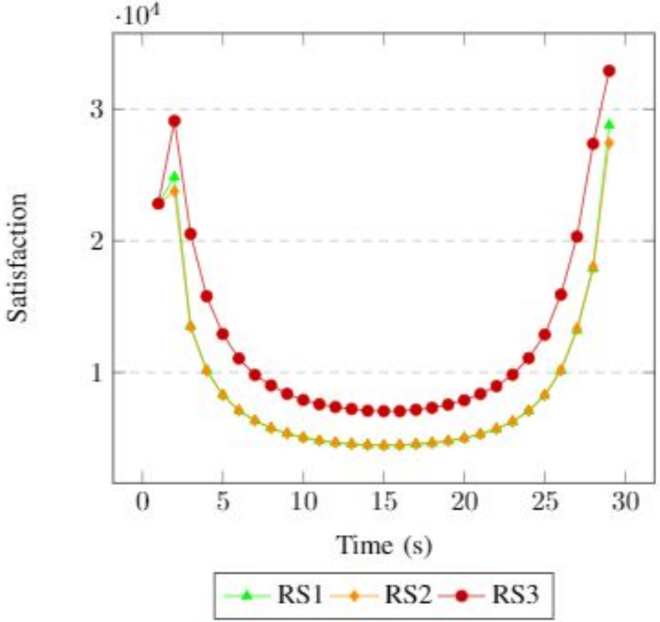
High Priority Tunnel

Reputation System Tests

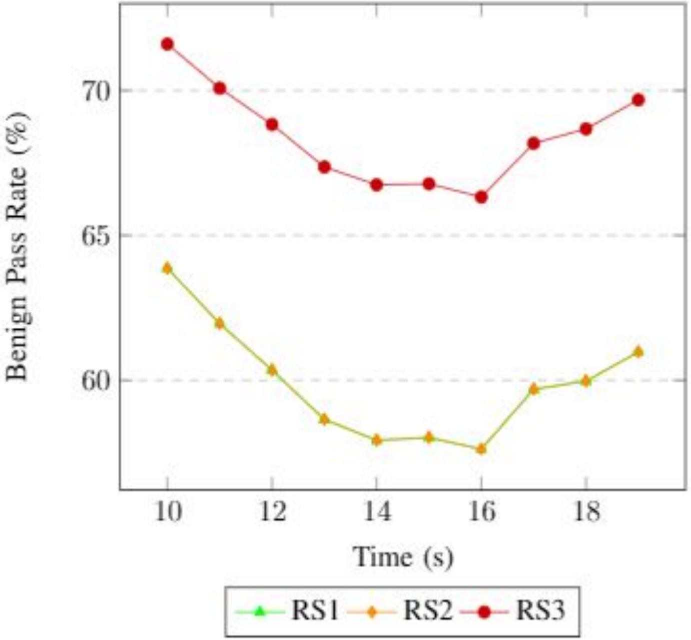
- **Different reputation systems integrated to the traffic policing module**
- **RS1**
  - Minimum discarding of 10%, medium restirctivity
- **RS2**
  - No minimum discarding, low restrictivity
- **RS3**
  - Discarding associated to total traffic excess, high restrictivity

Reputation System Tests

- Scenario 03: DDoS flood attack



Low Priority Tunnel



Benign Traffic Delivery

Conclusion

- **DeMONS solution viability**
  - Similar results to VGuard in benign traffic overload sceneries, but DeMONS reaches high priority tunnel satisfaction stability more fastly
  - Results superior to those of VGuard in the tested DDoS scenario, being able to 10% to 15% more of the amount of benign traffic delivery
  - Possibility of adapting system modules according to usage policies and scenarios
- **Future works**
  - Analysis of new reputation systems and verification of suitability in different scenarios
  - Analysis of the impact and time of the activation and deactivation of the architecture modules
  - Simulation of new DDoS scenarios
  - Solution Implementation in real NFV platform (Click-on-OSv - FENDE)

AINA

DeMONS: A DDoS Mitigation NFV Solution

Thanks!!

Carlos R. P. dos Santos
csantos@inf.ufsm.br

Universidade Federal de Santa Maria
SEDES SAPIENTIÆ
1960