SBRC2018
CAMPOS DO JORDÃO - SP

Uma Solução para Mitigação de Ataques DDoS Através de Tecnologia NFV

Vinícius F. Garcia, Guilherme de F. Gaiardo, Leonardo da C. Marcuzzo, Thales N. Tavares, Nilton C. B. da Silva, Anderson Monteiro, Raul C. Nunes, Carlos Raniery P. dos Santos

Universidade Federal de Santa Maria
SEDES SAPIENTIÆ
1960

Sumário

- **Introdução**
- **Trabalhos Relacionados**
- **DeMONS: DDoS Mitigation NFV Solution**
- **Avaliação**
  - Metodologia de Avaliação
  - Avaliação Comparativa
  - Avaliação de Sistemas de Reputação
- **Conclusão**

Introdução

- ***Distributed Denial of Service*** **(DDoS)**
  - Falsificação de IPs e IPs de origem real
- **Mitigação de DDoS**
  - Baseados em capacidade
  - Baseados em filtros
- ***Network Function Virtualization*** **(NFV)**
  - Desacoplamento das funções de rede do hardware associado
  - Criação de serviços de rede (SFC)
- **NFV provendo segurança**
  - Adaptabilidade a mudanças na rede
  - *Security Service Chain* (SSC)

Trabalhos Relacionados

- ***Holistic DDoS mitigation using NFV***
  - Arquitetura genérica para mitigação de ataques
  - Tratamento por camada de rede
- ***VFence: A Defense against Distributed Denial of Service Attacks Using Network Function Virtualization***
  - Mitigação de ataques do tipo *SYN Flood*
  - *Three way handshake*, listas negras e listas brancas
- ***A Collaborative DDoS Defence Framework using Network Function Virtualization***
  - Mitigação de ataques do tipo *SYN Flood*
  - Aplicação multidomínio do VFence

Trabalhos Relacionados

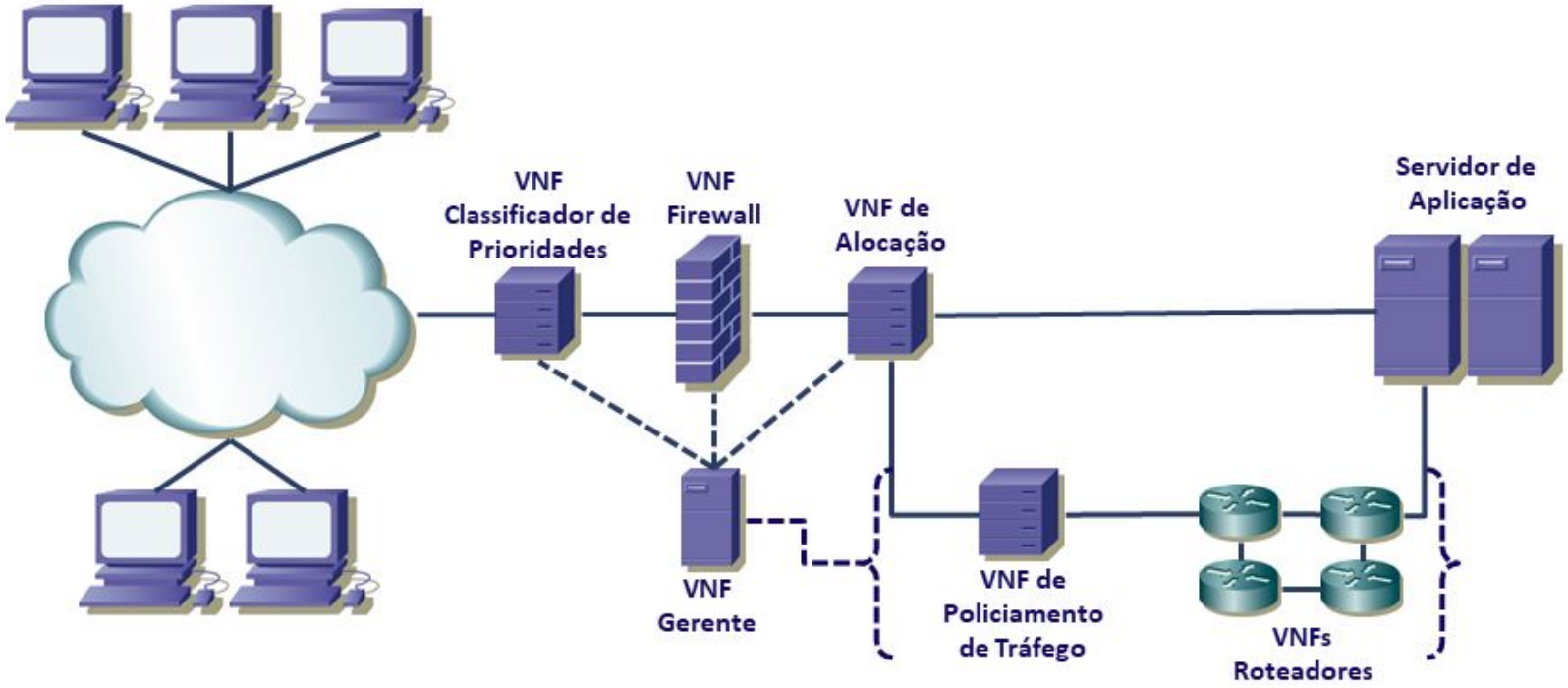
VGuard: A distributed denial of service attack mitigation method using network function virtualization

- **Mitigação de ataques DDoS**
- **Níveis de incerteza para determinar se um tráfego é malicioso**
  - Especialmente apropriado para ataques advindos de *botnets*
- **Baseado majoritariamente em capacidade**
  - Apenas descarta fluxos considerados 100% maliciosos
- **Arquitetura**
  - Classificador de tráfego
  - *Firewall Virtualized Network Function*
  - DDoS *Virtualized Network Function*
  - Túneis de alta e baixa prioridade

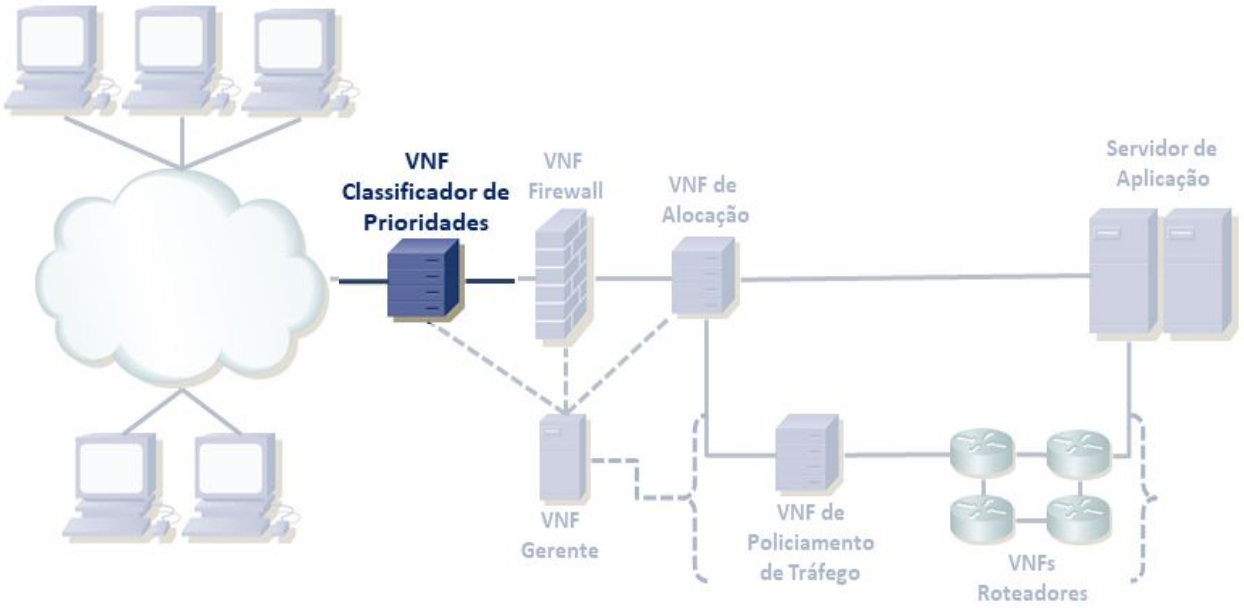
DeMONS: DDoS *Mitigation NFV Solution*

- **Mitigação de ataques DDoS**
- **Níveis de incerteza para determinar se um tráfego é malicioso**
  - Especialmente apropriado para ataques advindos de *botnets*
- **Proposta híbrida - baseado em capacidade e filtros**
  - Descarta totalmente fluxos considerados 100% maliciosos
  - Descarta parcialmente fluxos considerados suspeitos em caso de sobrecarga

DeMONS: DDoS *Mitigation NFV Solution*



DeMONS: DDoS *Mitigation NFV Solution*



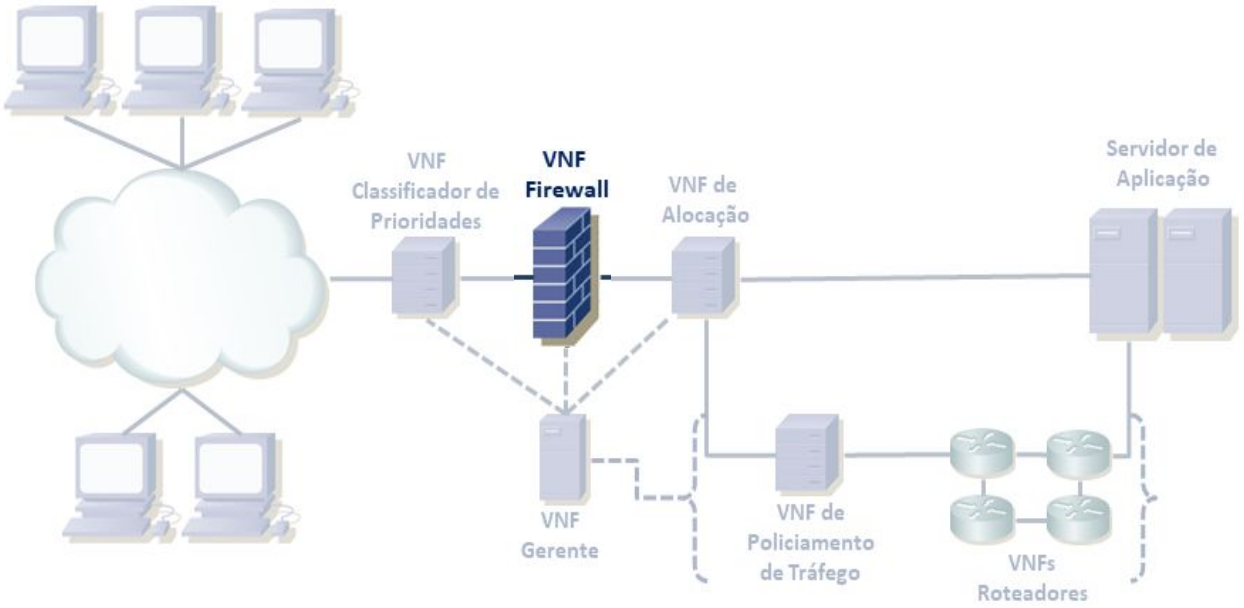
Classificador de prioridades

Determina a prioridade de um fluxo ([0;1])

Pode utilizar técnicas de DPI, IDS, IPS

Políticas de usuários podem ser incluídas

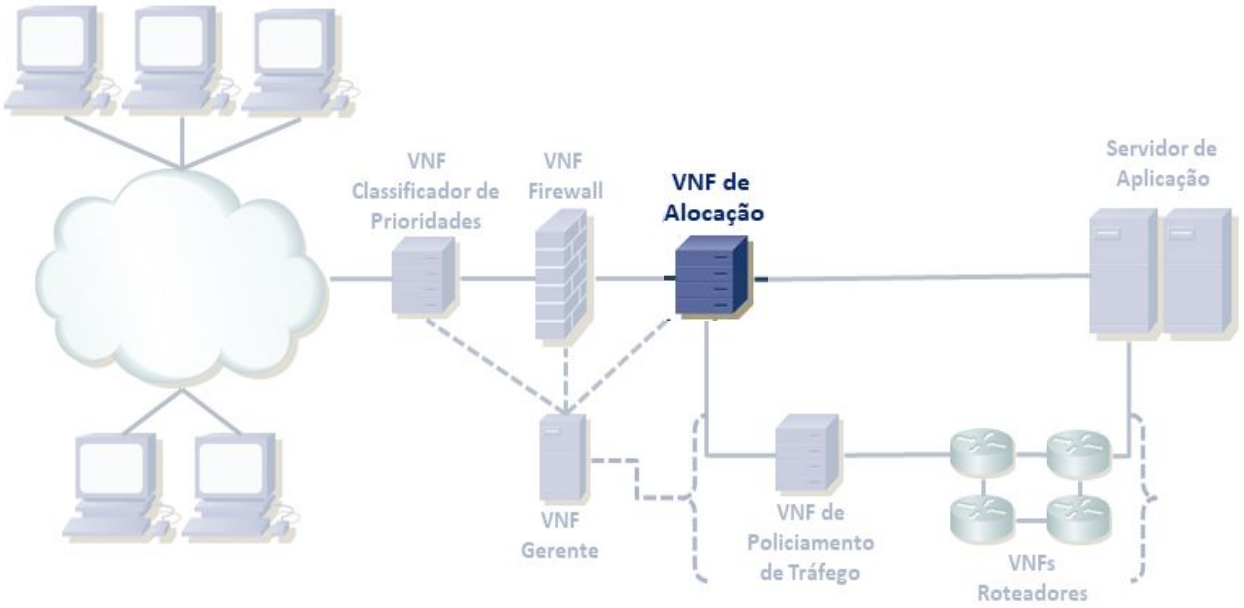
DeMONS: DDoS *Mitigation NFV Solution*



Firewall

Destinado ao bloqueio de fluxos com prioridade 0

DeMONS: DDoS *Mitigation NFV Solution*

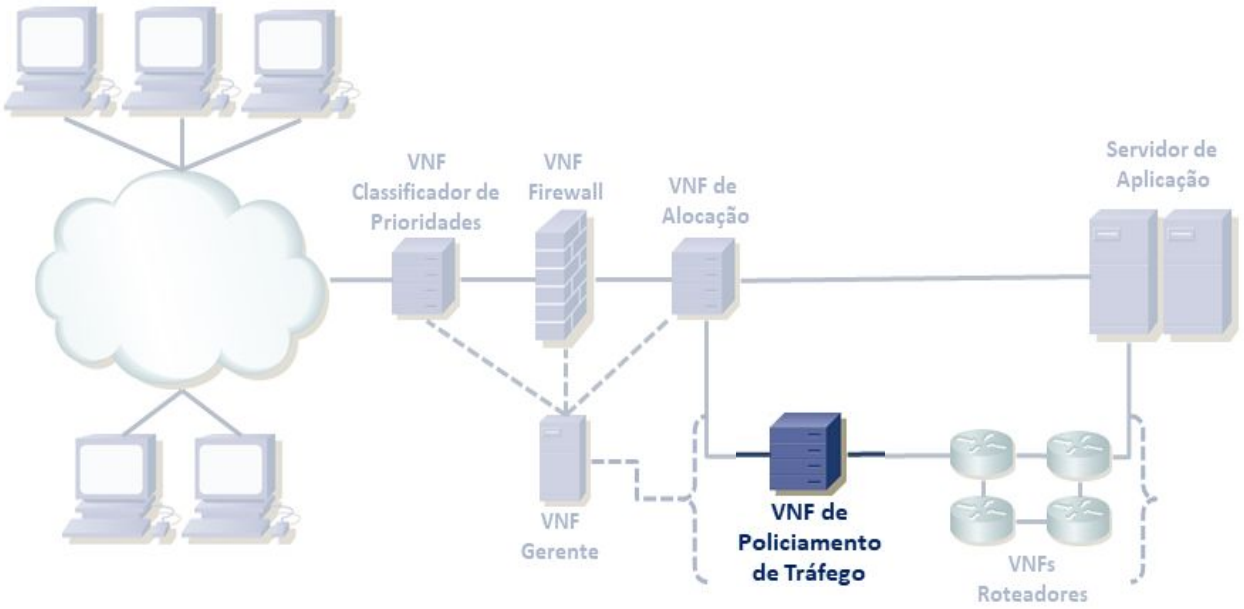


Alocador de Fluxos

Executa um algoritmo de alocação de fluxos em túneis de alta e baixa prioridade

Algoritmo dinâmico - adapta-se a mudanças de tráfego

DeMONS: DDoS *Mitigation NFV Solution*



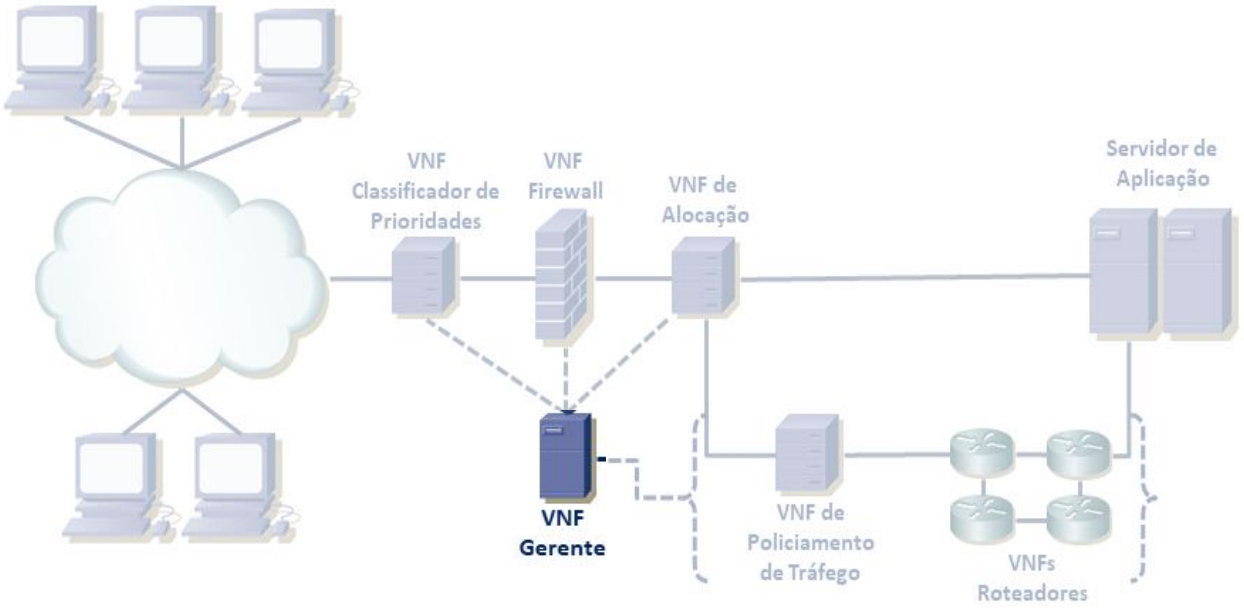
Policiador de tráfego

Presente no túnel de baixa prioridade

Aplica políticas de descarte parcial

Ativado em caso de sobrecarga do túnel

DeMONS: DDoS *Mitigation NFV Solution*



Gerente

Realiza gerenciamento da solução de defesa

Não substitui o MANO, mas sim indica a ele ações a serem tomadas do ponto de vista de segurança

Ativação e desativação de módulos, além de requisição por processos de escala

DeMONS: DDoS *Mitigation NFV Solution*

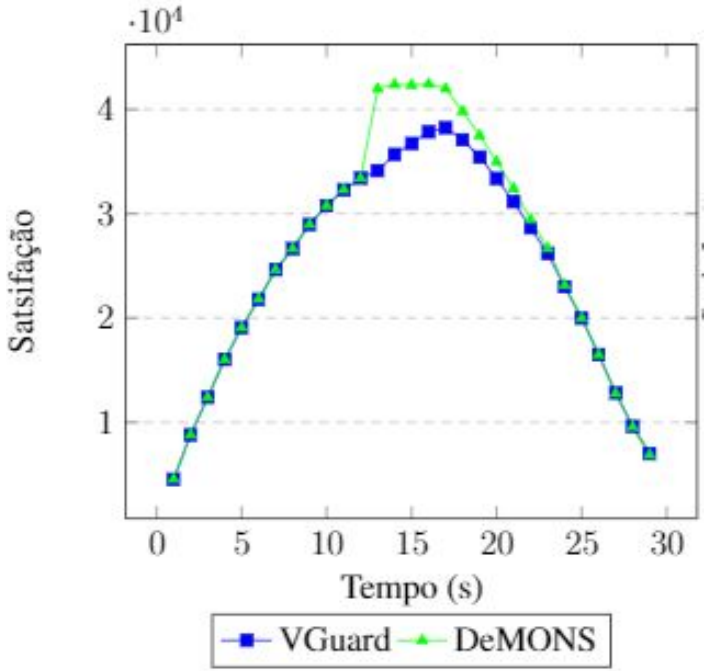
Algoritmo de Alocação de Fluxos		
	VGuard	**DeMONS**
Subutilização	Alternada	Alternada ou no túnel disponível
Limitação de tráfego	Modo seletivo	Modo seletivo
Balanceamento de fluxos	-	Entrada em modo seletivo
Análise em modo seletivo	Média da prioridade	Menores prioridades
Sobrecarga	Alocação incondicional	Alocação condicional

Metodologia de Avaliação

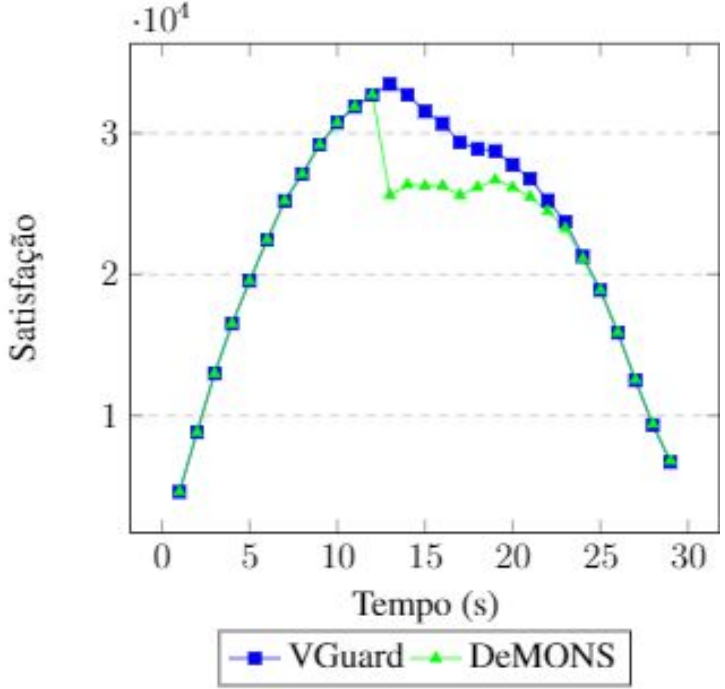
- **DeMONS**
  - Sistema de reputação: descarte mínimo de 10%, média restritividade
- **VGuard**
  - Versão de alocação dinâmica original
- **Configuração para avaliação**
  - Capacidade dos túneis (ambos): 50 Mbps
  - Modo seletivo: 97%
  - Fluxos benignos: 100 Kbps - degradação 10 Kbps (0,4 <= p <= 1)
  - Fluxos maliciosos: 100 Kbps - sem degradação até o fim do ataque (0,1 <= p <= 0,4)
  - Duração: 30 segundos
- **Métricas de avaliação**
  - Satisfação agregada e ponderada

Avaliação Comparativa

- **Cenário 01: fluxos benígnos e tráfego total máximo de 99.1 Mbps**



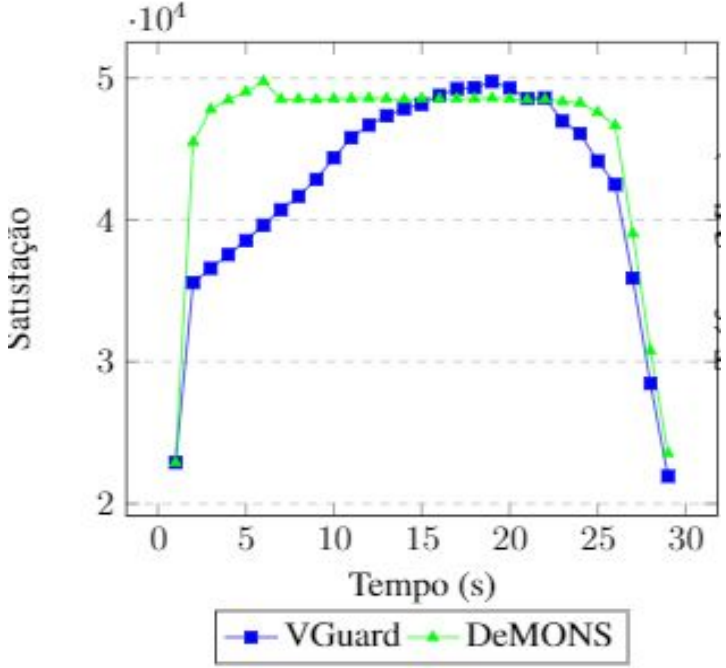
Túnel de Alta Prioridade



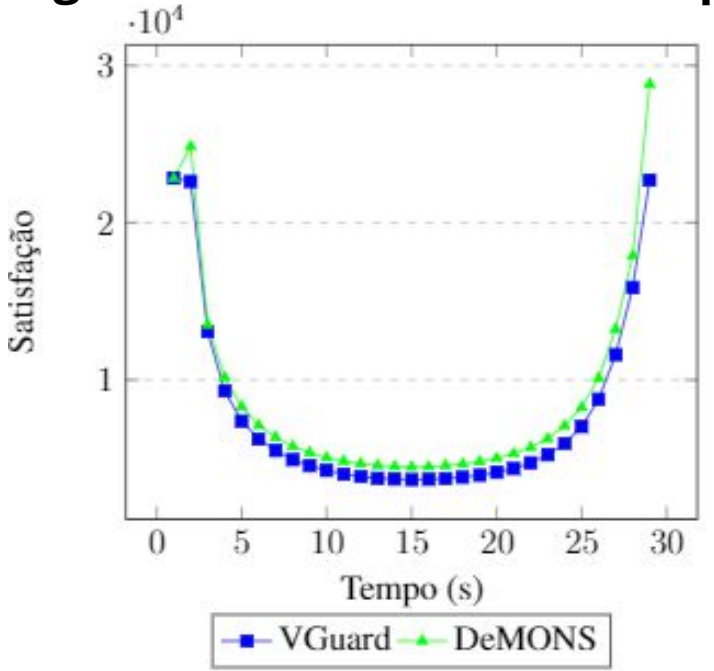
Túnel de Baixa Prioridade

Avaliação Comparativa

- **Cenário 02: fluxos benígnos e tráfego total máximo de 506 Mbps**



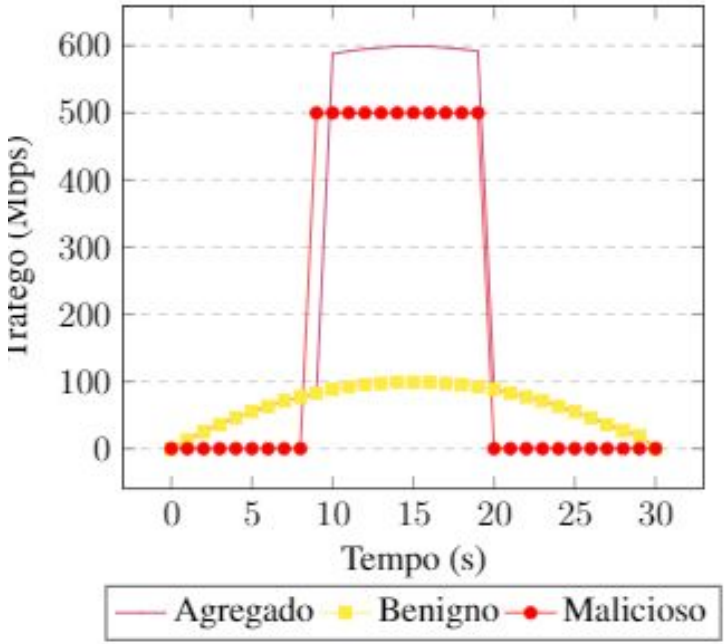
Túnel de Alta Prioridade



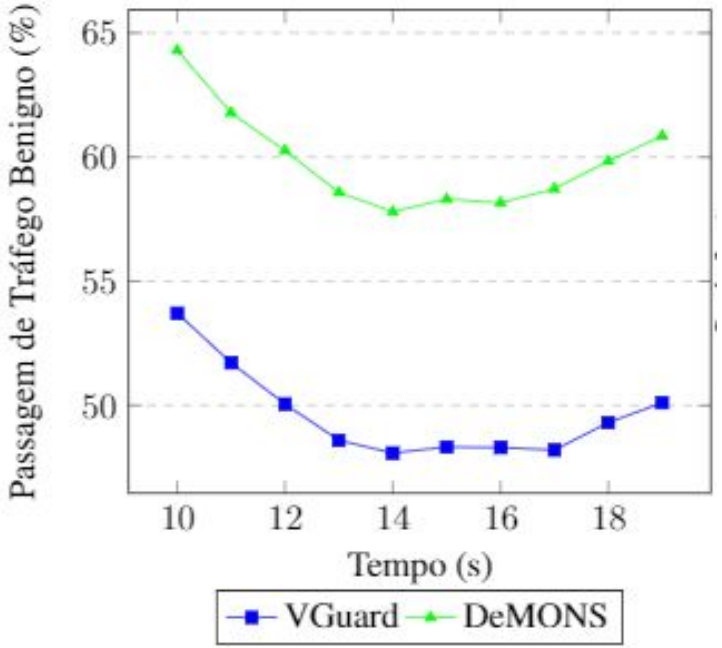
Túnel de Baixa Prioridade

Avaliação Comparativa

- **Cenário 03: Ataque DDoS**



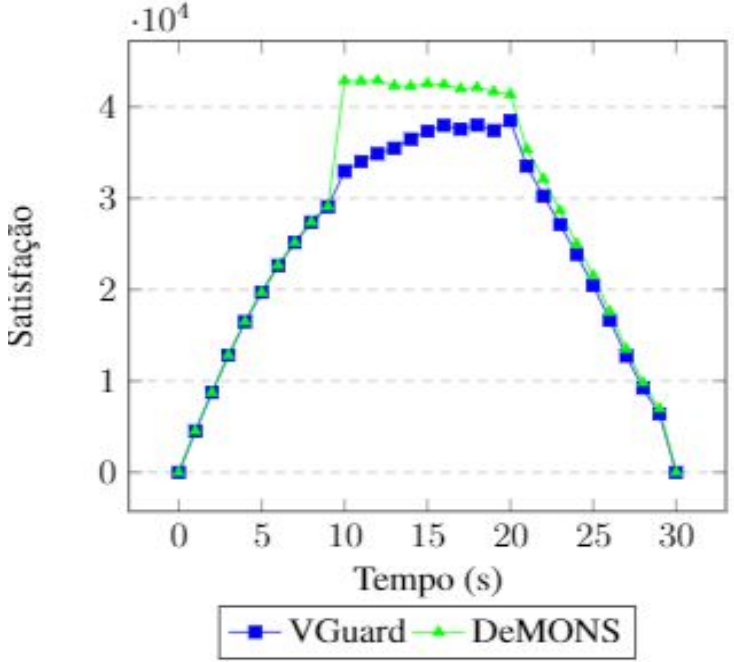
Cenário de Ataque



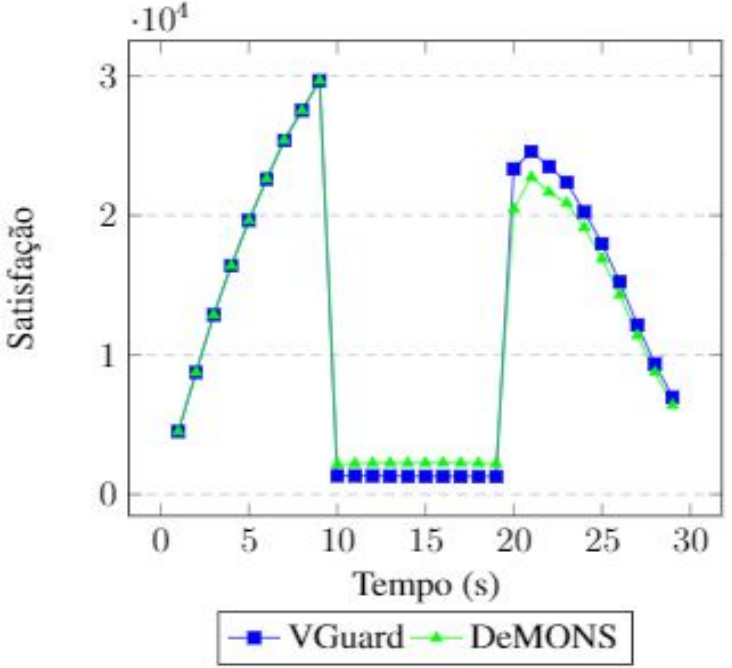
Entrega de Tráfego

Avaliação Comparativa

- **Cenário 03: Ataque DDoS**



Túnel de Alta Prioridade



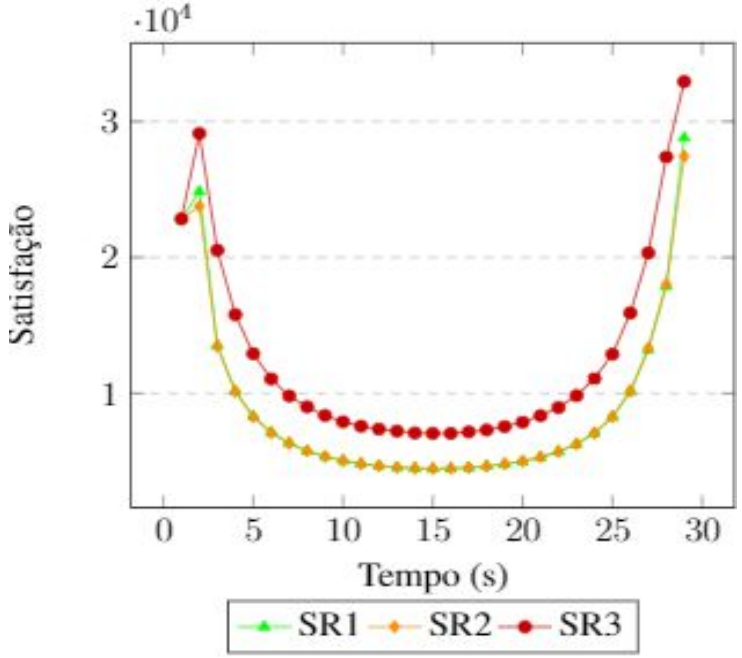
Túnel de Baixa Prioridade

Avaliação de Sistemas de Reputação

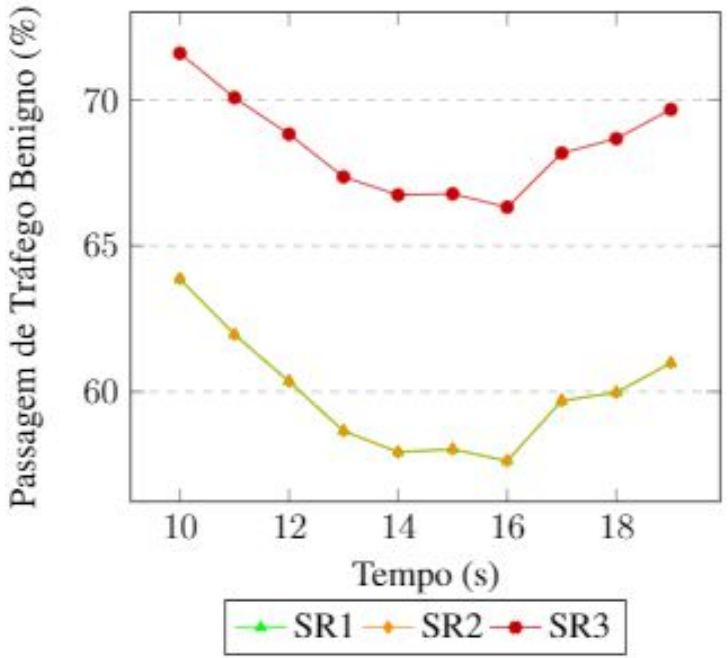
- **Integração de diferentes sistemas de reputação ao módulo de policiamento de tráfego**
- **SR1**
  - Descarte mínimo de 10%, média restritividade
- **SR2**
  - Sem descarte mínimo, baixa restritividade
- **SR3**
  - Descarte associado ao excedente de tráfego, alta restritividade

Avaliação de Sistemas de Reputação

- **Cenário 03: Ataque DDoS**



Canal de Baixa Prioridade



Entrega de Tráfego

Conclusão

- **Viabilidade da solução DeMONS**
  - Resultados semelhantes ao VGuard nos cenários de sobrecarga de tráfego benigno, porém alcança estabilidade de satisfação no túnel de alta prioridade mais rapidamente
  - Resultados superiores aos do VGuard no cenário de DDoS testado, sendo capaz de obter 10% a 15% a mais no montante de entrega de tráfego benigno
  - Possibilidade de adaptações de módulos do sistema de acordo com políticas e cenários de uso
- **Trabalhos futuros**
  - Análise de novos sistemas de reputação e verificação de adequação dos mesmos em diferente cenários
  - Análise do impacto e tempo da ativação e desativação dos módulos da arquitetura
  - Simulação de novos cenários de DDoS
  - Implementação da solução em plataforma NFV real (Click-on-OSv - FENDE)

SBRC2018
CAMPOS DO JORDÃO - SP

Uma Solução para Mitigação de Ataques DDoS Através de Tecnologia NFV

Obrigado!!

Vinícius Fülber Garcia
vfulber@inf.ufsm.br

Universidade Federal de Santa Maria
SEDES SAPIENTIÆ
1960