Mitigação e Detecção de Ataques em Redes SDN utilizando NFV

Universidade Federal do Rio Grande do Sul

Autor: Pedro Henrique Arruda Faustini (pedro.faustini@inf.ufrgs.br)
Orientador: Alberto Egon Schaeffer-Filho (alberto@inf.ufrgs.br)

Introdução

- Redes de computadores são formadas a partir da conexão de hosts, que ocorre por meio de troca de pacotes, conduzida por switches e roteadores.

- Tradicionalmente, para se alterar o comportamento desses dispositivos é necessário modificá-los um a um. Já em uma rede definida for software (software defined network, ou **SDN**), cabe a um software controlador que tem visão global da rede definir a maneira com que esse encaminhamento é feito. SDN confere programabilidade aos administradores e torna o gerenciamento do fluxo de pacotes mais simples, pois o desacopla do hardware.

- Apesar dessa flexibilidade, SDNs estão sujeitas a diversas ameaças, o que torna necessária a investigação de mecanismos de detecção e mitigação de ataques.

Foco do trabalho

- É importante para a rede manter níveis aceitáveis de operação frente a eventos como ataques ou sobrecarga operacional.

- Módulos que realizam funções de monitoramento são tipicamente implementados em *middleboxes (*hardware otimizado para tarefas específicas). Contudo, tem se tornado popular a noção de virtualização de funções de rede (Network Function Virtualization, ou **NFV**), que substitui middleboxes por software executado em hardware de propósito geral.

- O presente trabalho investiga mecanismos para detectar ataques e reagir da forma mais apropriada para mitigá-los. Vislumbra-se que tais mecanismos possam ser providos na forma de NFVs dispostas em diferentes pontos na rede.

Proposta

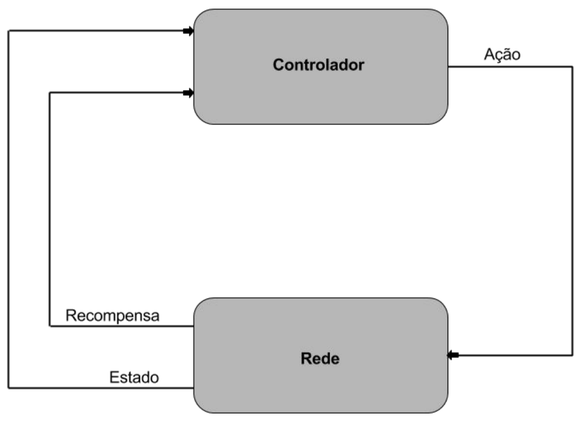
- Certas NFVs escaneiam portas de hosts para encontrar brechas para ataques. Outras realizam diferentes funções, como filtragem de pacotes segundo determinados critérios.

- O controlador monitora a rede e, baseado em evidências de anomalias, a partir de técnicas de aprendizagem de máquina do tipo *reinforcement learning*, adota uma política de mitigação para um determinado cenário.

- Por exemplo, se o tráfego por um switch envolve pacotes com destino a uma porta inadvertidamente aberta em um host, uma NFV pode barrar pacotes. Se o tráfego em uma região da rede força o controlador a adicionar muitas regras em flow-tables, este pode descartar pacotes. Busca-se assim manter a rede resiliente frente a anomalias.

A máquina controladora recebe informações da rede (tráfego, delay, portas abertas, etc), que representam um estado e uma recompensa associada à ação anterior.

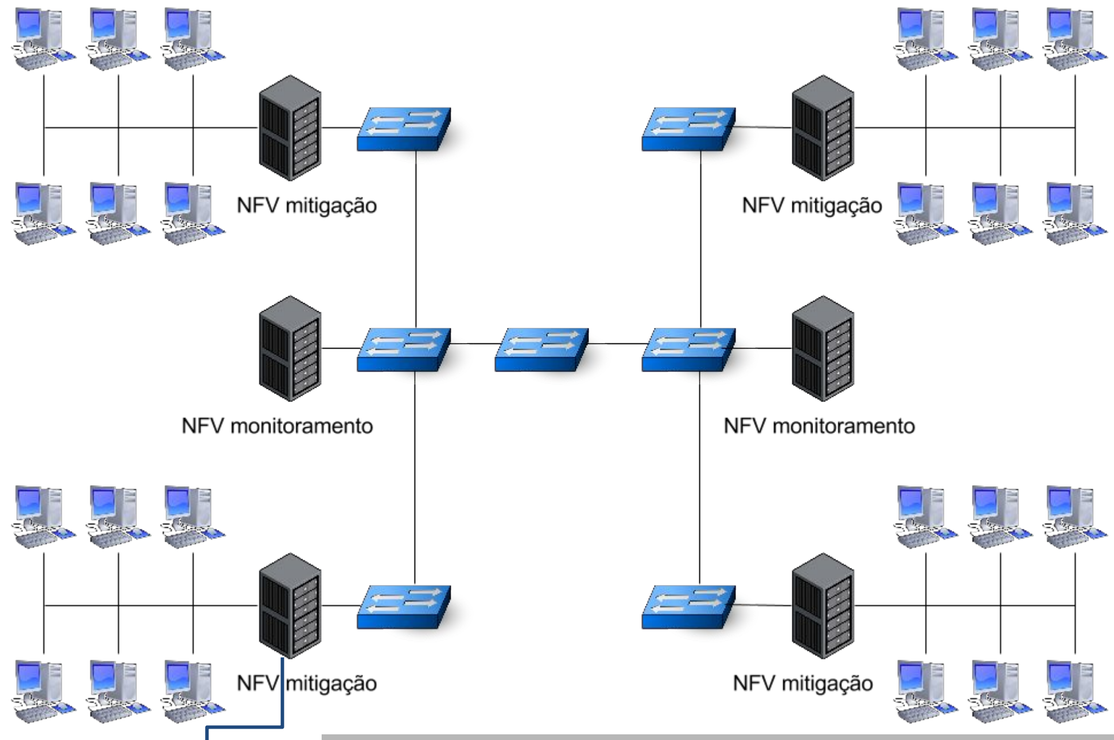
O controlador age para melhorar as condições da rede (via NFVs de mitigação, por exemplo), recebe uma recompensa e vai a um outro estado. O ciclo se repete até a rede chegar a um estado de normalidade.

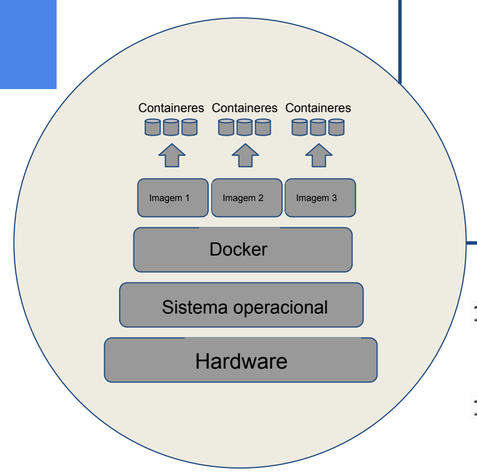


Ao contrário de máquinas virtuais, containeres compartilham o mesmo kernel do sistema operacional hospedeiro, mas também proveem isolamento de aplicações e sistema de arquivos.

Mininet fornece uma rede OpenFlow, com suporte a hosts, switches e controlador.

Containeres Docker podem abrigar funções de rede e portanto foram integrados ao Mininet como NFVs. Entre as funções que podem desempenhar estão monitoramento (e.g. port scanning e IDS) e mitigação (e.g. filtragem e descarte de pacotes). Além disso, são transparentes: uma rede funcional não deixa de operar sem eles.



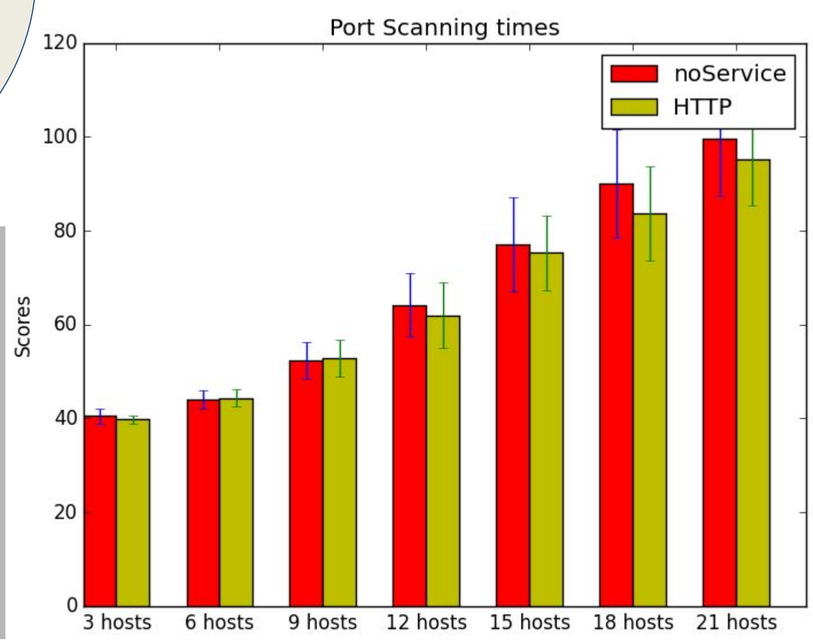


Docker fornece um ambiente (Dockerfiles ou um shell interativo) para que as dependências necessárias sejam instaladas (e.g. Nmap ou Iptables) e imagens sejam criadas. Containeres são as instâncias das imagens.

Containeres com NFVs são instanciados no Mininet como nodos por uma chamada especial (addDocker). A seguir, podem proativamente executar as funções adicionadas ou esperar por mensagens do controlador antes de tomarem decisões.

Leva-se mais tempo para escanear hosts sem portas abertas, possivelmente em função da espera de um timeout por parte da ferramenta de escaneamento Nmap.

NFVs de monitoramento devem ser replicadas pela rede para minimizar tempo de trabalho.



Resultados e trabalhos futuros

- O **protótipo** desenvolvido até o momento inclui a rede SDN aliada a containeres Docker com NFVs de escaneamento de portas. Entretanto, o objetivo é adicionar novas funções de rede, incluindo mitigação de anomalias e monitoramento.

- Uma simulação de ataque DDOS derrubou um servidor. O controlador recebeu mais de 10 mil endereços IP em poucos segundos e ficou ocupado ao ter que criar regras em diversos switches. Pacotes legítimos não chegavam ao controlador e nem ao destino se já não houvessem regras nas flow-tables.

- A implementação das NFVs de mitigação via algoritmos de *reinforcement learning* contribuirão para manter a rede resiliente. É necessário definir métricas de entrada que constituem os estados e a recompensa devolvida para a aplicação, após esta executar ações de mitigação.

UFRGS
UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL

.inf
INSTITUTO DE INFORMÁTICA
UFRGS