Aplicações de segurança usando SDN

André Grégio, CTI

GTS 22

Dezembro, 2013

Agenda

1. Parte I
   - Introdução
2. Parte II
   - Ataques contra SDN
3. Parte III
   - SDN: Aplicações de Segurança

Agenda

Enquanto isso, na camada de rede...

Encaminhamento de IP

- O datagrama IP não precisa passar por um roteador se origem e destino:
  - estão diretamente conectados (link ponto-a-ponto);
  - são parte de uma rede compartilhada (Ethernet).
- Senão, o host de origem envia o datagrama para o roteador padrão, o qual intermedia a entrega para o host de destino.
- IP mantém a **tabela de encaminhamento** para lidar com pacotes que chegam via interface de rede.

Tabela de Encaminhamento

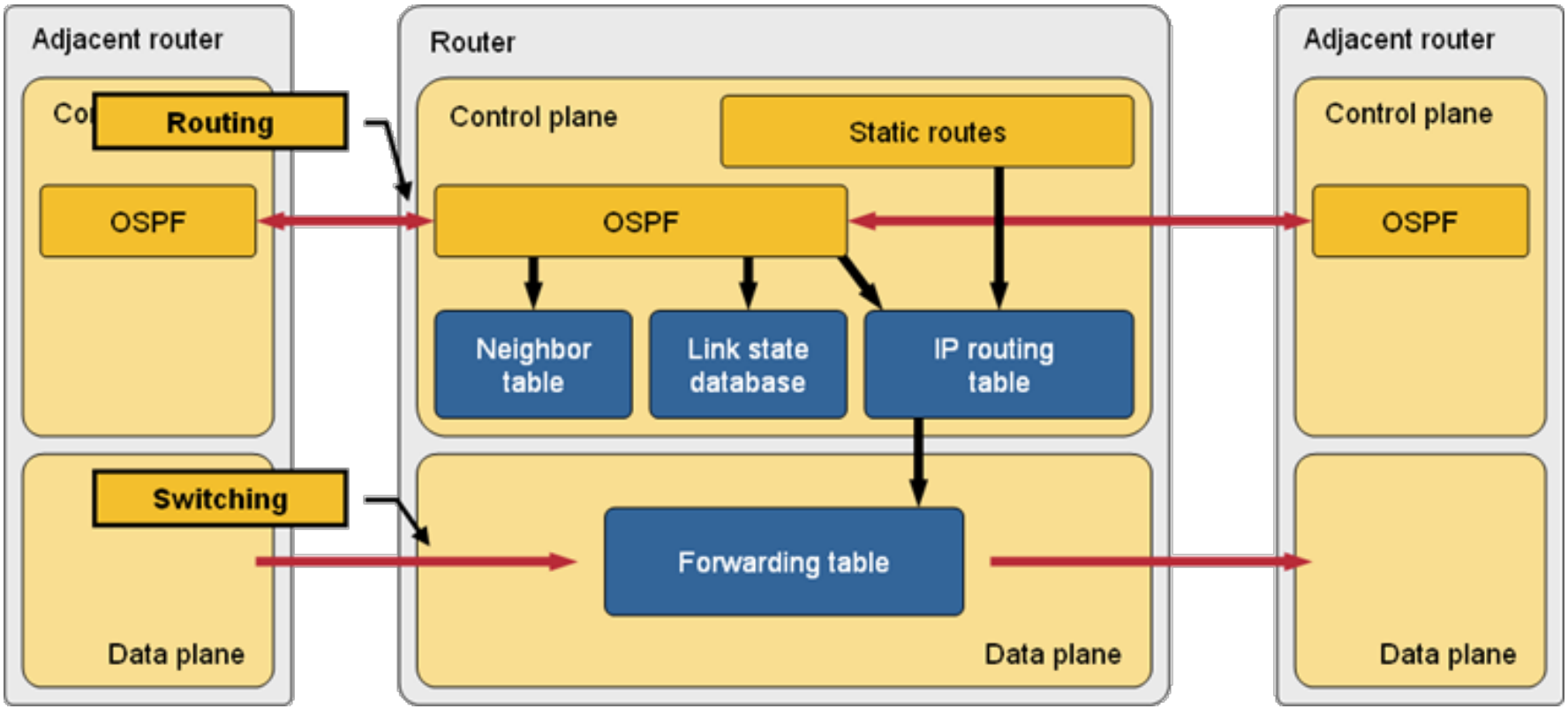
Campos importantes

- **Destino:** IP (32 ou 128 bits); 0 $\Rightarrow$ *default route*.
- **Next-hop:** IP da próxima entidade (roteador ou host).
- **Interface:** Identificador da interface de rede para envio.

Peculiaridades

- *hop-by-hop*, sem o caminho completo.
- *next-hop*: mais perto do destino; diretamente conectado; sem *loops*.
- Protocolos de roteamento devem garantir que a tabela está correta.

Planos... [1/3]



Fonte: `http://wiki.nil.com/Control_and_Data_plane`

Planos... [2/3]

Control Plane (CP)

- Recebe e processa informações de outras "caixas";
- **Atualiza** mudanças ocorridas na topologia;
- **Passa instruções** para a tabela de encaminhamento no Data Plane;
- Pode usar seu próprio mecanismo de encaminhamento para determinar a interface de saída ou o *next-hop router*;
- Em SDN, o CP está fora do *switch/router* $\Rightarrow$ aplicação baseada em computadores comuns...
- Permite que um controlador modifique remotamente o **comportamento** de dispositivos de rede por meio de um conjunto de instruções bem definido.

Planos... [3/3]

Data Plane (DP)

- **Recebe** e **processa** pacotes de entrada e encaminha pacotes que necessitam de processamento especial ou de atualização de protocolos de roteamento para o CP;
- **Direciona** cada pacote para a saída correta;
- Cria a tabela de encaminhamento;
- Foco no **desempenho**.

Redes Definidas por Software

Características

- Abordagem de redes na qual o CP não é feito por hardware, mas por uma aplicação chamada “controlador”.
- Permite que o tráfego possa ser moldado de acordo com mudanças necessárias a partir de um ponto central de controle.
- Alta granularidade promove o gerenciamento de carga mais flexível e eficiente.
- Maior controle sobre o fluxo do tráfego de rede.
- Suporta uma matriz de comutação entre equipamentos de diferentes vendedores.

Motivação

SDN e segurança

- Complexidade das camadas/domínios de rede ⇒ dispositivos de segurança para controlar cada aspecto ou zona.
- SDN: rotinas podem ser escritas para adicionar funcionalidades aos dispositivos (controle de tráfego, inspeção, alertas);
- Separação dos planos (controle e dados) permite a criação de soluções mais "abertas", i.e., menos proprietárias e complexas do que as dos planos de controle dos dispositivos de rede atuais.

Vantagens de SDN

Possibilidades...

- Controle centralizado, automação distribuída;
- Rede pró-ativa, implementação de QoS facilitada;
- Requisição dinâmica de serviços de rede por aplicações;
- Segurança adaptativa;
- Pode levar a tratamento mais eficiente de incidentes.

OpenFlow

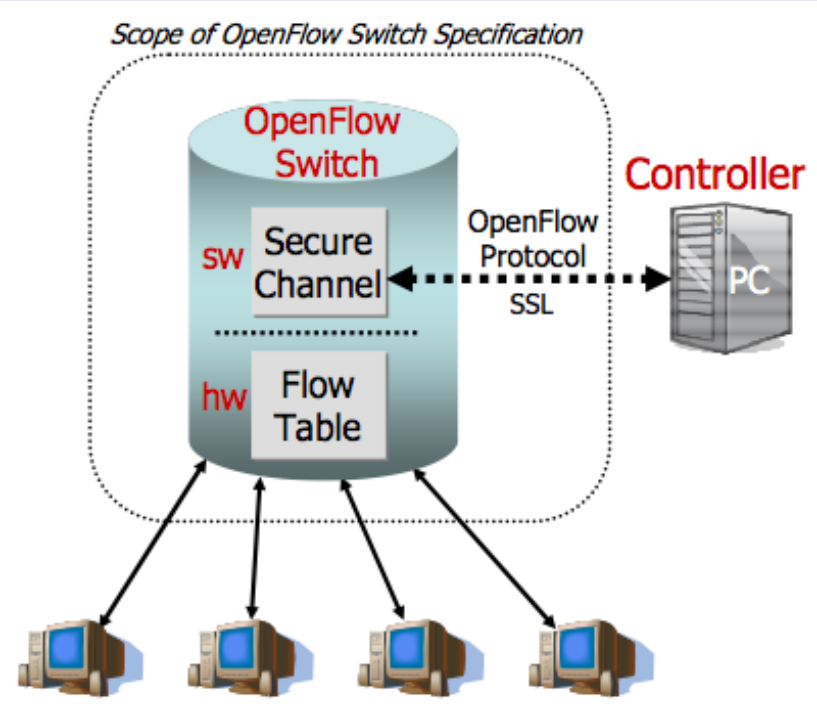
Características

- Especificado pela *Open Networking Foundation*;
- Padrão aberto para a implementação de SDN ⇒ provê acesso por software às tarefas de controle de fluxo;
- OF switches separam o encaminhamento rápido de pacotes (*data path*),ainda feito por switch convencional, das decisões de roteamento de alto nível (*control path*).

Fonte:`https://www.opennetworking.org`

OpenFlow [1/2]

OpenFlow Switch*



A tabela de fluxos é controlada por um dispositivo remoto.

*http://archive.openflow.org//documents/openflow-wp-latest.pdf

OpenFlow [2/2]

Do ponto de vista da segurança:

- OF permite rígido controle sobre decisões de roteamento dos fluxos pelos DP dos componentes de rede.
- O controle envolve a possibilidade de implementação de lógica mais complexa, por ex.:
  - Regras *stateful* para procedimentos de quarentena;
  - Migração/redirecionamento transparente de conexões maliciosas;
  - Técnicas para detecção de ataques baseadas em fluxos podem ser reimplementadas e distribuídas de maneira mais eficiente.

Agenda

Ataques contra SDN* [1/3]

Introdução

- Ataque eficiente contra SDN por meio de conhecimentos de características básicas da tecnologia.
- Varredura e identificação de SDN (*fingerprinting*).
- Lançamento de ataque de consumo excessivo de recursos - violação do princípio da disponibilidade.
- "SDN trazem novos problemas de segurança..."

*Shin, S., Gu, G. Attacking Software-Defined Networks: A First Feasibility Study. HotSDN 2013.

Ataques contra SDNs [2/3]

Motivação

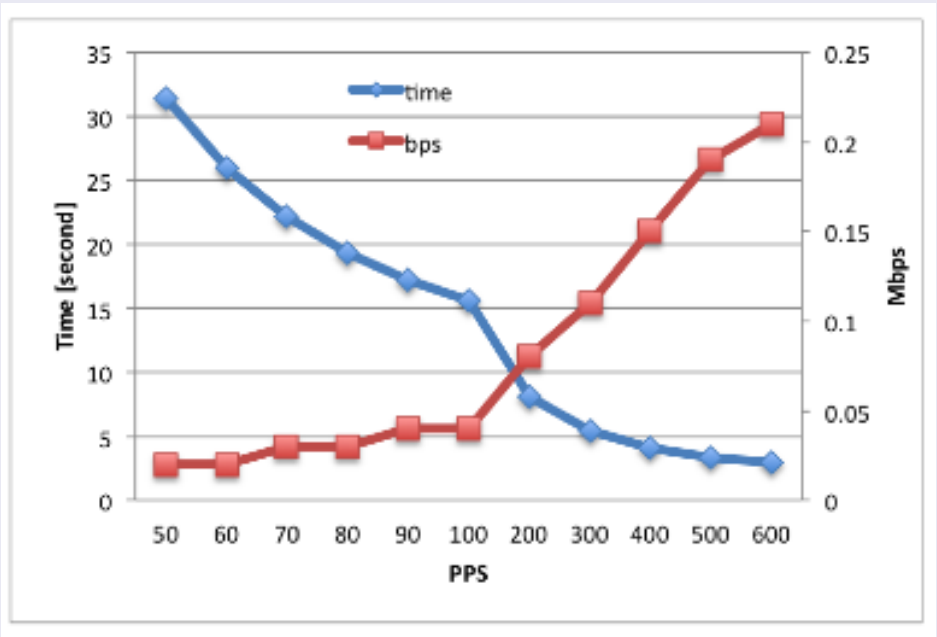
- Propriedade básica de operação ⇒ separação dos planos de dados e controle.

1. Plano de **dados** solicita por regras de fluxo ao plano de controle para tratar novos pacotes.
2. Plano de **controle**, reativo, reforça suas regras dinamicamente para manter a eficiência.
3. Problemas ocorrem quando há muitas requisições do plano de dados para o de controle.
   - DP pode inundar o CP com mensagens de requisição.
   - DP (tabela de fluxos) pode ser inundado pelas regras por tratar tantas requisições.

Ataques contra SDNs [3/3]

O Ataque

- **Fingerprinting:** determina, com base em tempo de resposta, se uma rede usa switches baseados em SDN/OpenFlow para gerar requisições "especiais" de fluxos do DP ao CP.
- **DoS por consumo de recursos nos Planos.**



Agenda

Projetos Open Source em SDN [1/2]

Networks Functions Virtualization Security Application

- **CPqD / of13softswitch:** *An OpenFlow 1.3 compatible user-space software switch implementation based on the Ericsson TrafficLab 1.1 softswitch implementation.*
- **Indiana University InCNTRE / FlowScale:** *FlowScale is a project to divide and distribute traffic over multiple physical switch ports. FlowScale replicates the functionality in load balancing appliances but using a Top of Rack (ToR) switch to distribute traffic.*

Fonte: `http://www.sdncentral.com/comprehensive-list-of-open-source-sdn-projects/`

Projetos Open Source em SDN [2/2]

Networks Functions Virtualization Security Application

- **SRI International / FortNOX:** *FortNOX is an extension to the open-source NOX OpenFlow controller. FortNOX automatically checks whether the new flow rules violate security policies.*
- **SRI International / FRESCO:** *FRESCO is an initiative to develop an OpenFlow application framework for rapidly prototyping security detection and mitigation modules, and composing these modules into efficiently deployable security services.*
- **CPqd / RouteFlow:** *RouteFlow is an open source project to provide virtualized IP routing services in OpenFlow networks.*

FortNOX*

Motivação

- Um switch OpenFlow deve ser continuamente reprogramado para lidar com os fluxos correntes.
  - Como reforçar a política de segurança evitando conflitos?
- NOX OpenFlow controller: encaminha regras de fluxos de uma aplicação OF para o switch.
  - Diversas aplicações OF podem inserir dinamicamente diferentes políticas de controle de fluxo ⇒ sobrescrita de regras, evasão de políticas de segurança.
- FortNOX ⇒ Extensão do NOX OF controller.

*Porras, P., Shin, S., Yegneswaran, V., Fong, M., Tyson, M. Gu, G. Security Enforcement Kernel for OpenFlow Networks. HotSDN 2012.

FortNOX

Características

- Provê reforço (*non-bypassable*) das regras de fluxo com base em políticas aplicadas nas requisições de inserção de regras de fluxo feitas por aplicações OF.
- *Role-based Source Authentication*: validação/priorização de regras por assinatura digital;
- *Conflict Analyzer*: avalia regras candidatas contra o conjunto vigente;
- *State Table Manager*: mantém a tabela agregada de fluxos, que armazena as regras;
- *Flow Rule Timeout Callback*: interface para atualizar a tabela de fluxos.

Security-Enhanced Floodlight

Versão melhorada e estendida do FortNOX

- **Menor privilégio:** aplicações OpenFlow operam fora do contexto de processo do controlador.
- **Autenticação digital** para produtores de regras de fluxo.
- **Detecção de conflitos inline** para as regras de fluxo.
- **Auditoria de segurança:** subsistema OF que traça eventos de segurança produzidos pela plilha de rede OpenFlow.
- **Download:** `www.openflowsec.org/Download-SEK.html`

CloudWatcher*

O que é?

- Framework com o objetivo de proteger uma rede em *cloud*.
- Controla fluxos de rede para garantir que todos os pacotes necessários sejam inspecionados por dispositivos de segurança (e.g., NIDS).
- Provê uma linguagem simples para rotinas de implementação das políticas que garantirão o objetivo anterior.
- Tira vantagem da tecnologia de SDN para controlar os fluxos.
- Opera como uma aplicação sobre um S.O. de rede (e.g., NOX, Beacon)

*Shin, S., Gu, G. CloudWatcher: Network Security Monitoring Using OpenFlow in Dynamic Cloud Networks. ICNP-NPSec 2012.

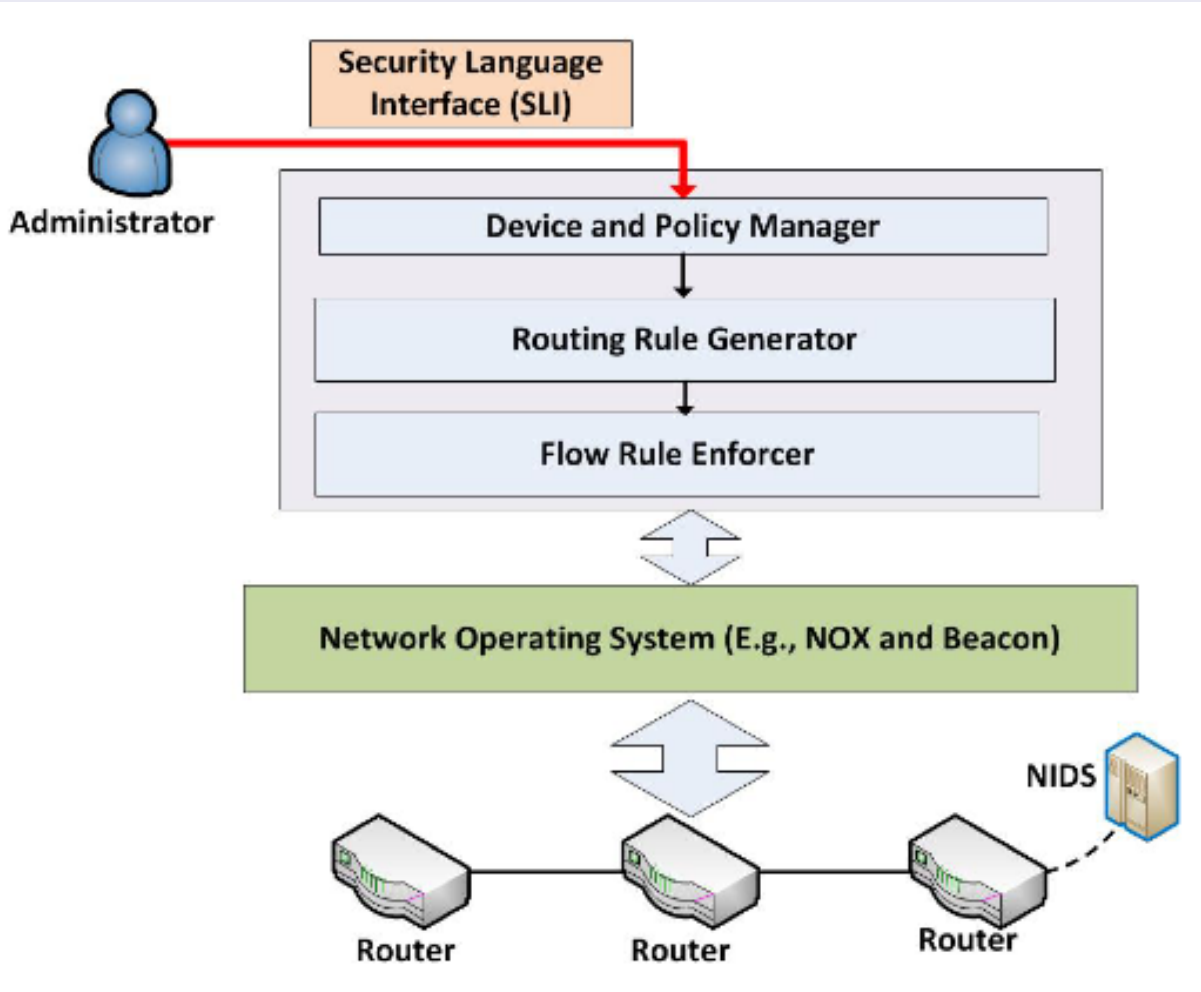
CloudWatcher

Características

- Componentes:
  - Gerenciador das informações sobre os dispositivos de segurança;
  - Criador de regras para lidar com os pacotes de cada fluxo;
  - Implantador das regras de fluxo geradas para os switches.
- Limitações:
  - Se o administrador especificar dois dispositivos de segurança que não se comunicam entre si, não serão gerados caminhos de roteamento;
  - Muitos novos fluxos $\Rightarrow$ problemas de desempenho.

CloudWatcher

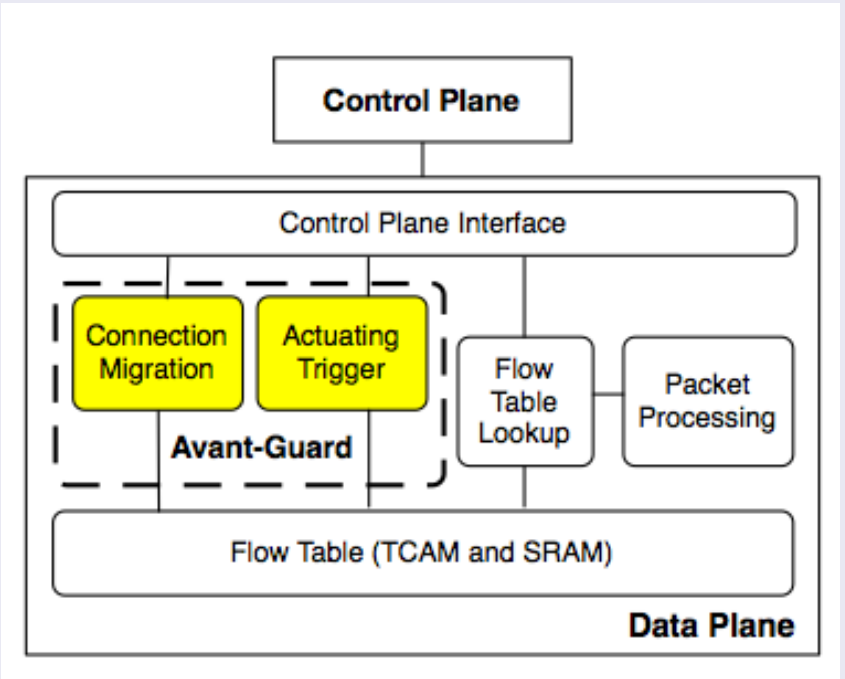
Arquitetura



AVANT-GUARD*

Problemas de SDN

- Controlador centralizado é o gargalo da escalabilidade das SDN durante rajadas de tráfego anômalo.
- OF não facilita a inspeção do conteúdo de pacotes, fazendo com que o DP tenha seu desempenho degradado.



*Shin, S., Yegneswaran, V., Porras, P., Gu, G. AVANT-GUARD: Scalable and Vigilant Switch Flow Management in Software-Defined Networks. ACM CCS 2013.

AVANT-GUARD

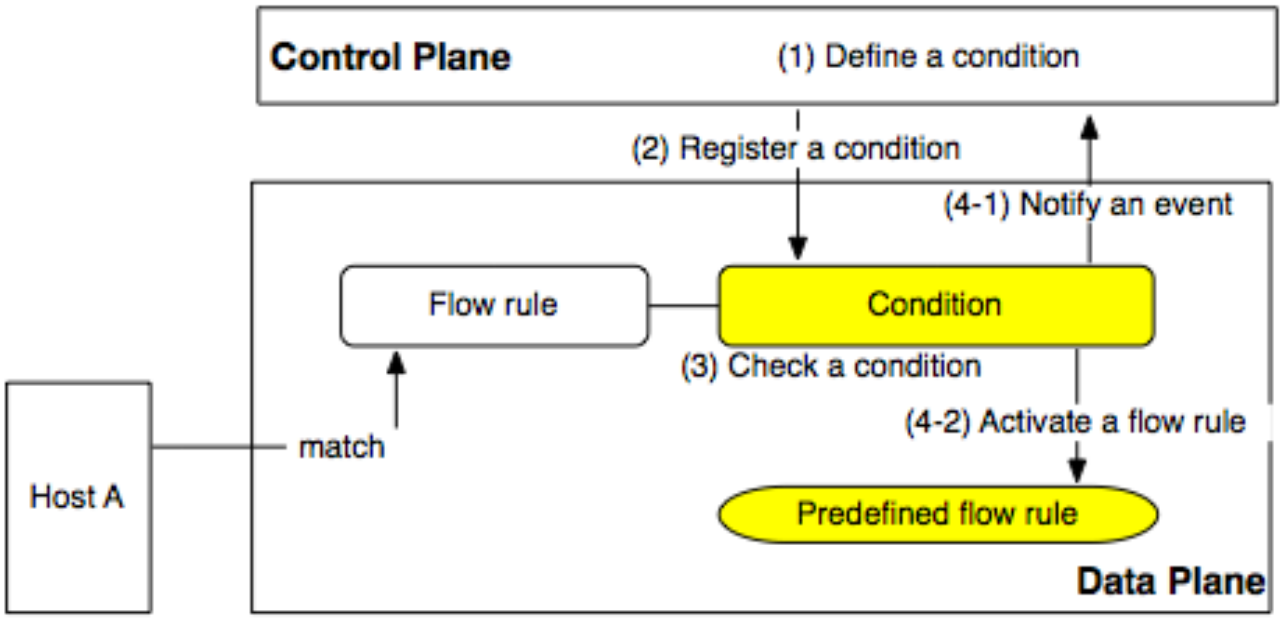
Connection Migration

- Adiciona inteligência ao DP para diferenciar origens que completarão conexões TCP.
- Proxy de TCP *handshake* $\Rightarrow$ SYN cookies!
- Apenas as requisições de fluxo que completam o *handshake* vão para o CP.
- Protege contra ataques de inundação e/ou com origem forjada (requisição de fluxo não é encaminhada).
- *Overhead* mínimo.

AVANT-GUARD

Actuating Triggers

- Retorna para o CP informações de estado e *payload* da rede de maneira assíncrona.
- Permite ativar regras sob condições pré-definidas para que o CP gerencie os fluxos sem atrasos.



FRESCO*

O que é?

- Framework de desenvolvimento de aplicações de segurança voltado para o padrão OpenFlow:
  - Design rápido;
  - Composição de módulos para detecção e mitigação de ataques em OpenFlow.
- O próprio framework é uma aplicação baseada em OpenFlow.
  - OF capturam e armazenam estado de sessões TCP de maneira não uniforme.
  - Provê API para facilitar regras de aplicações baseadas em DPI.

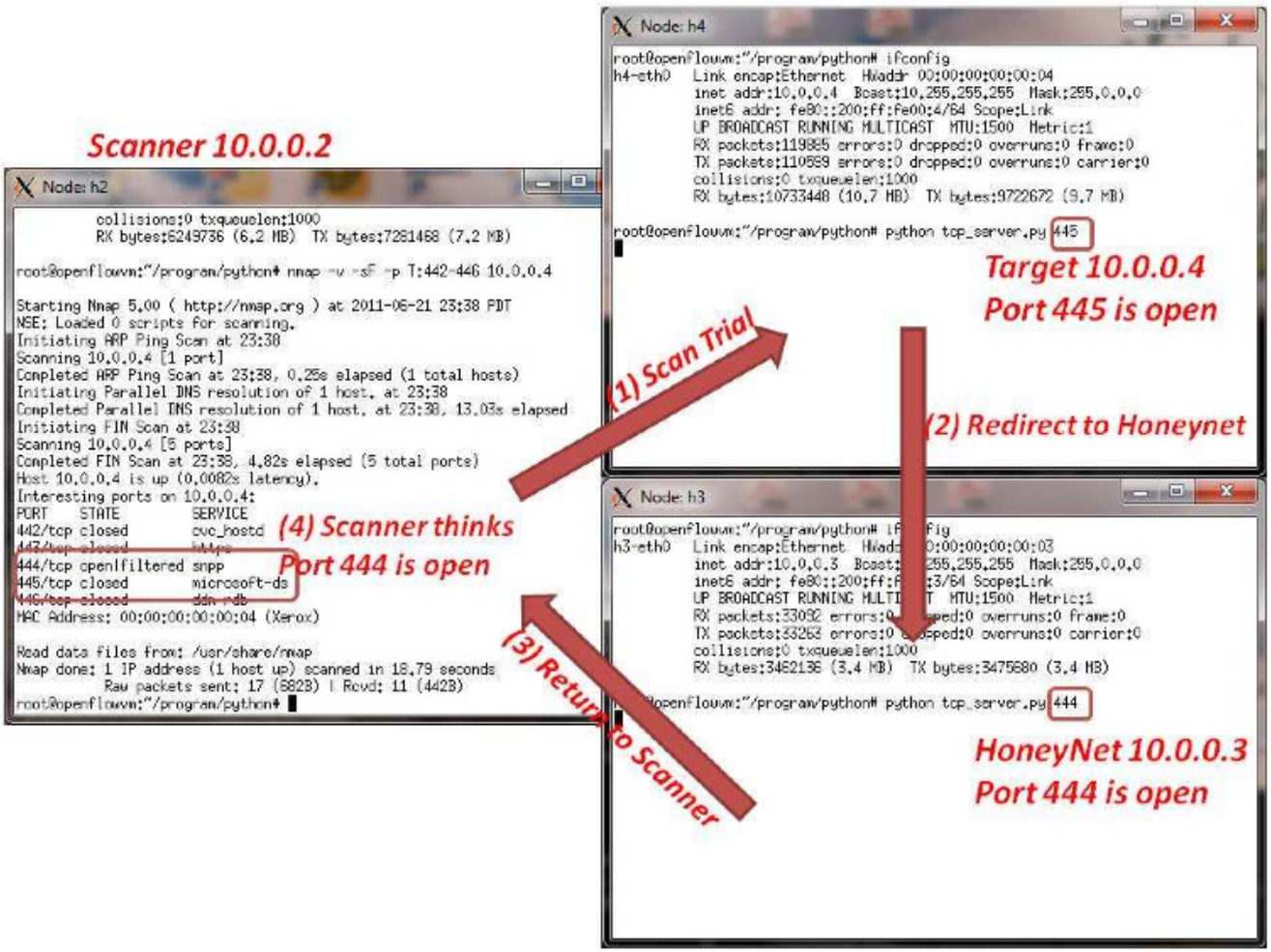
*Shin, S., Porras, P., Yegneswaran, V., Fong, M., Gu, G., Tyson, M. FRESCO: Modular Composable Security Services for Software-Defined Networks. NDSS 2013.

FRESCO

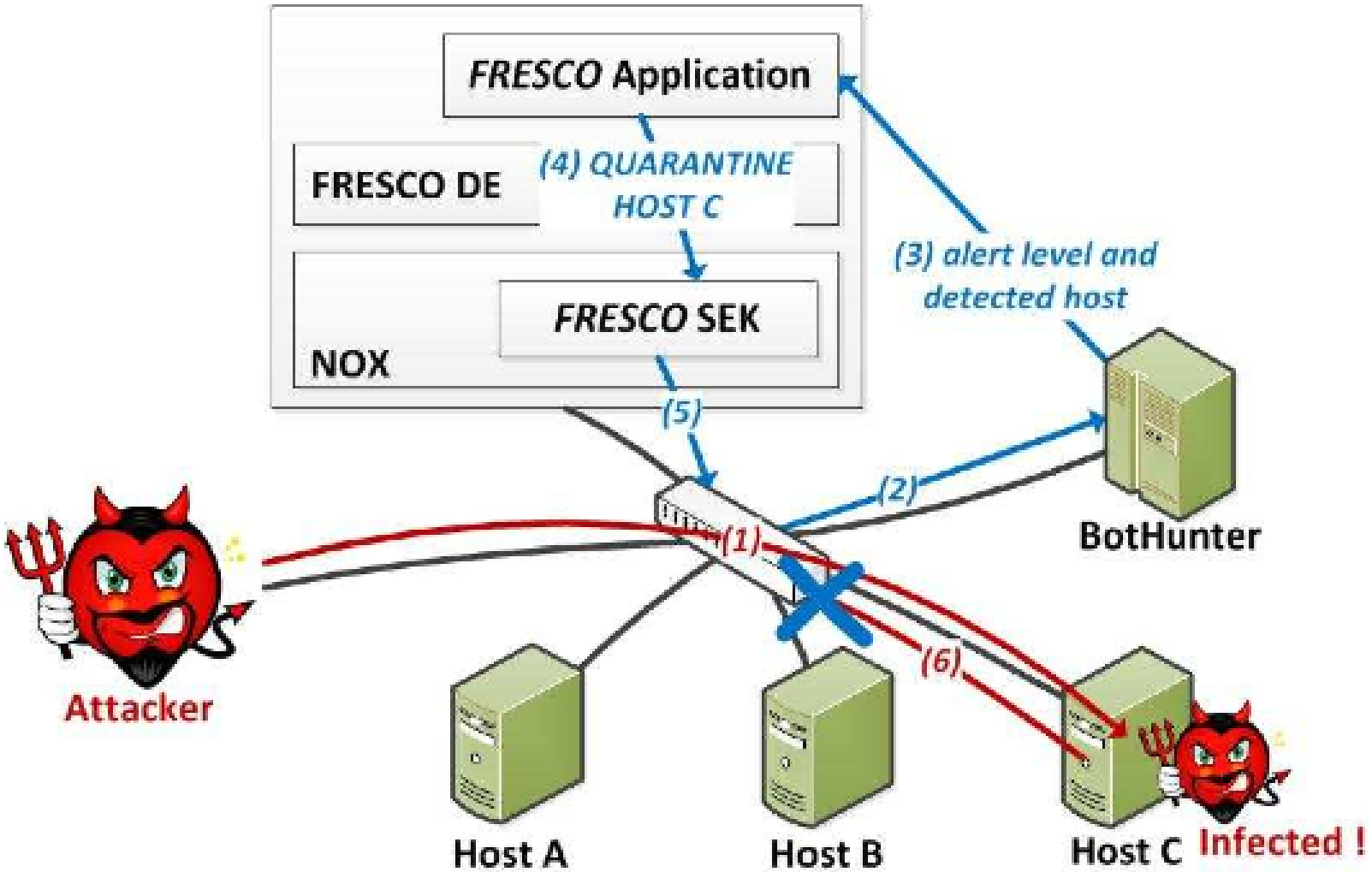
Características

- Camada de aplicação (interpretador e APIs) + SEK (implementação de políticas de segurança).
- Controlador de recursos $\Rightarrow$ monitora switches de rede OF e mantém registro dos estados (tabela de fluxos).
- Linguagem de scripting $\Rightarrow$ desenvolvimento de aplicações de segurança a partir de módulos básicos.
- Criação de funções de segurança com sobrecarga mínima e cerca de 90% menos linhas de código.
- A ser disponibilizado como software open source.

FRESCO: Aplicações - Reflector



FRESCO: Aplicações - Quarentena



Mais aplicações de segurança

SDN Security Actuator

- Permite que produtos de segurança legados sejam integrados a uma pilha de rede OF.
- Traduz diretivas de resposta em regras OF enviadas ao SE-Floodlight.
- Foco em identificar máquinas infectadas/maliciosas.
- **Download:** `www.openflowsec.org/Download-SAC.html`

OF-BotHunter

- Aplicação de referência para um serviço antimalware.
- Sistema de análise passivo baseado em rede que detecta bots, worms, etc. na rede interna.
- **Download:** `www.openflowsec.org/Download-OFB.html`

Wrapping up

Segurança vs. SDN

- Novas preocupações e vulnerabilidades.
- Soluções podem ser projetadas do início para atender ao novo paradigma.
- Problemas de dispositivos legados para tratar.
- Portabilidade de soluções pode ser mais fácil.
- Disseminar a tecnologia e desenvolver aplicações que a utilizem ajuda a resolver suas limitações atuais...

Obrigado!

Contato

André Grégio
andre.gregio@cti.gov.br