ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA ELEKTROTECHNICKÁ
KATEDRA TELEKOMUNIKAČNÍ TECHNIKY

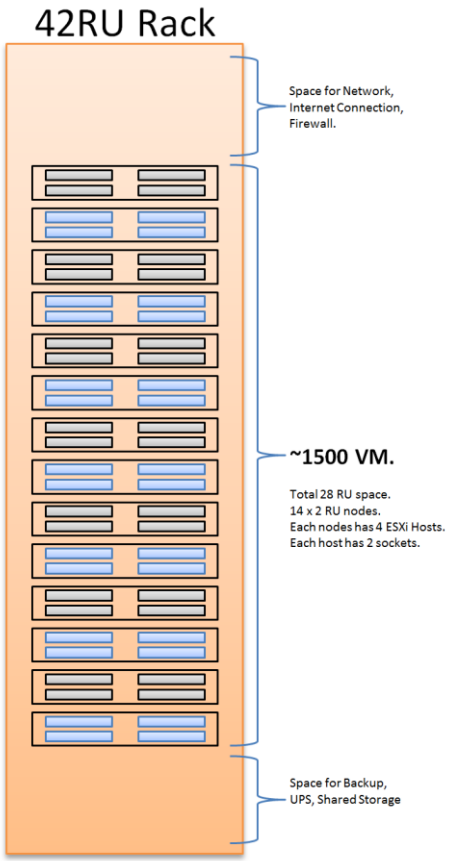
SDN technologie v souvislostech

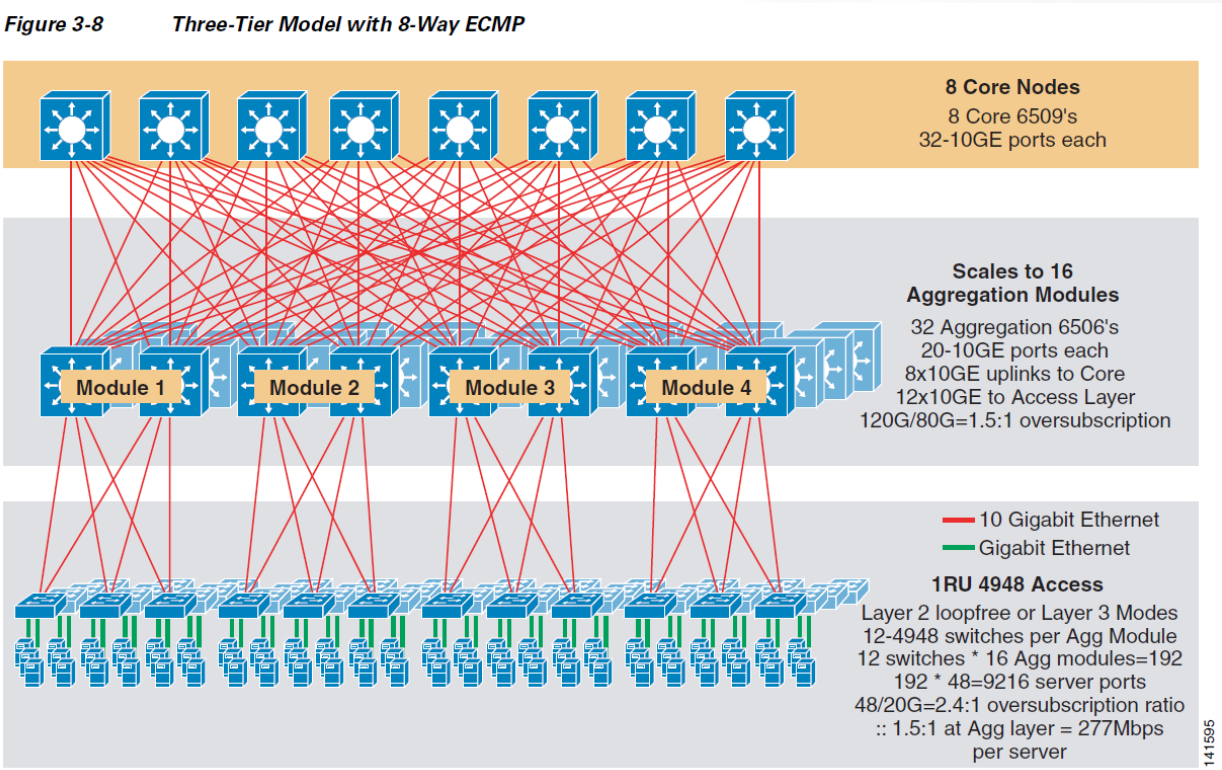
Tomáš Hégr
tomas.hegr@fel.cvut.cz
21. 6. 2016

Agenda

- Doba automatizační
- Softwarově Definované a Sítě
- SDN technologie a jejich specifika
- Nový přístup, nové hrozby
- Akademické výhledy
- Aplikační ukázka
- Shrnutí

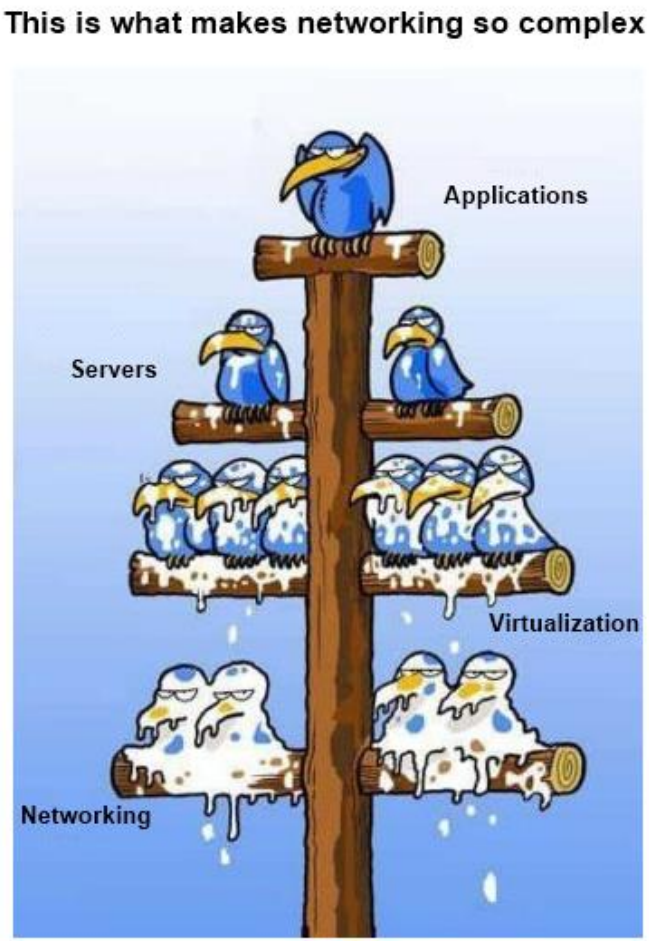
Hustota VM v DC





http://virtual-red-dot.info/1000-vm-per-rack-is-the-new-minimum/
Cisco Data Center Infrastructure 2.5 Design Guide

Kam to celé směřuje?



- Narůstající komplexnost systémů na všech vrstvách ISO/OSI modelu.
- Nedostatečná flexibilita CLI.
- Potřeba programovatelnosti zařízení, frameworků, nástrojů, zavedení procesů a procedur jejichž fundamentální součástí je testování.

RFC 1925 - It is more complicated than you think.

Hlavní cíle síťaře

- Automatizované a konzistentní nasazení služeb do sítě.
- Bezpečnostní politiky konzistentní skrze celou síť.
- Rozhodnutí tvořená na základě centralizovaného pohledu na síť od hrany k hraně.
- Automatizovaná konfigurace a řízení síťových zařízení.
- Dynamická reakce na změny stavy sítě.
- Odstranění hop-by-hop mechanismu?

Everything that can be automated will be automated.

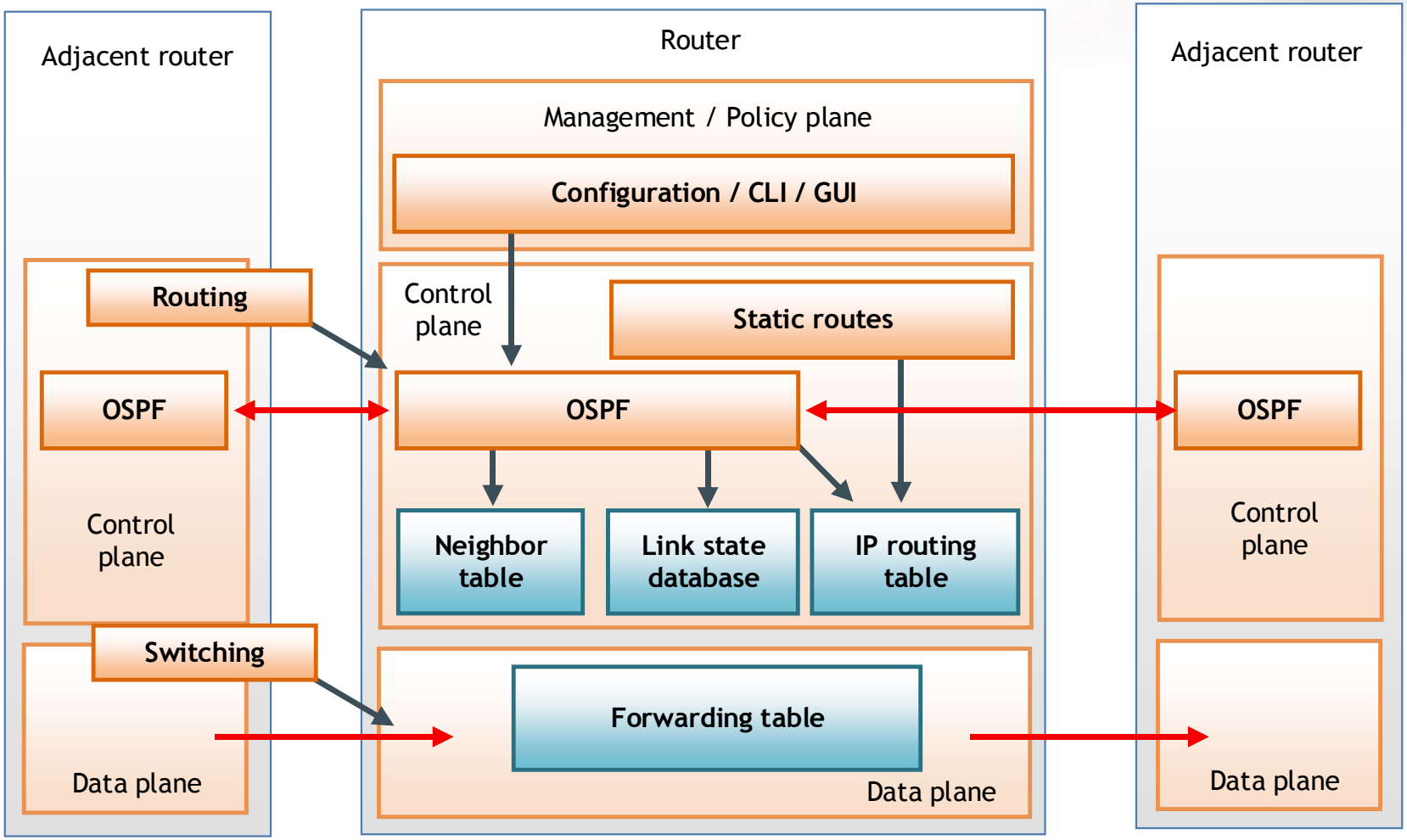
Shoshana Zuboff

Expect -> Puppet / Chef / Ansible / Salt

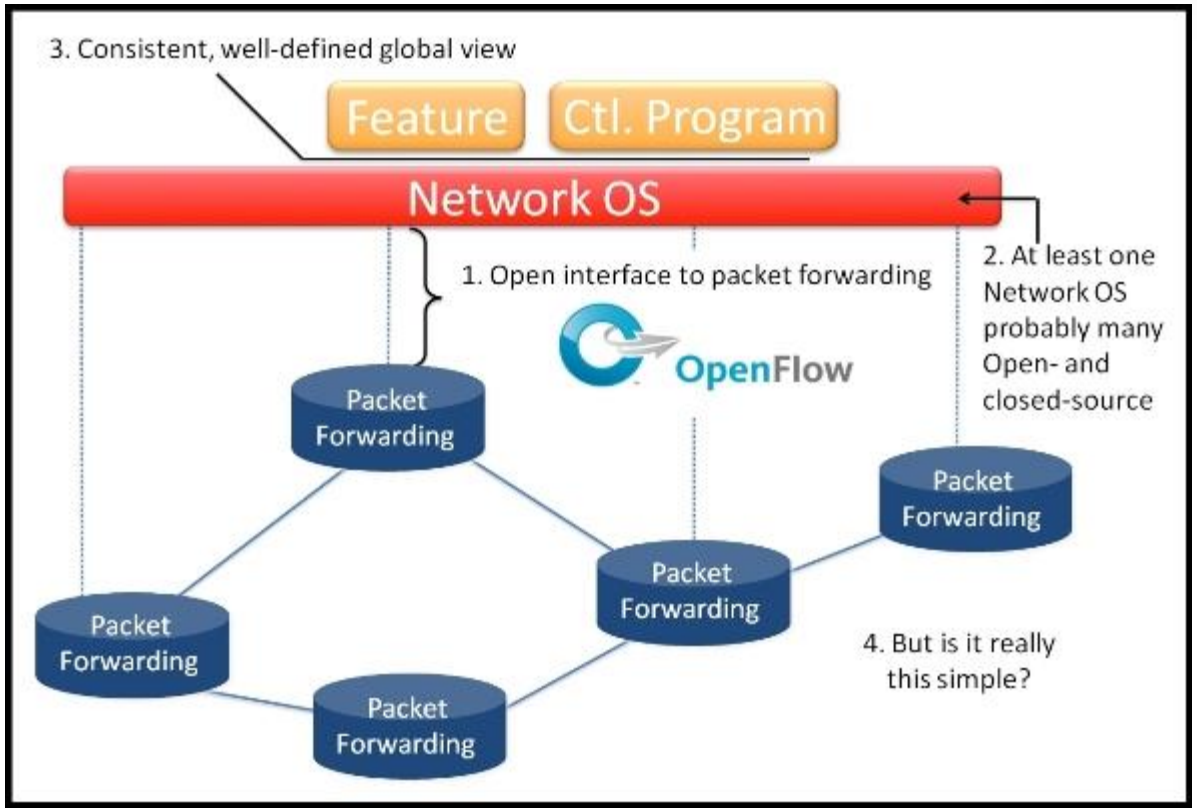
Co je to Softwarově Definované?

- Mnoho je dnes Sofwarově Definované (SD), ale bylo tomu někdy jinak?
- SDN v Software-Defined Anything – SDDC (Data Center), SDS (Storage), SDSec (Security), SD-WAN.
- Obecně přidání abstraktní (unifikované) vrstvy aplikačního programového rozhraní nad systémy nižších vrstev.
- Nejednoznačná definice pojmu vede k různému výkladu a pohledu na SDN.

Roviny v síťových zařízeních



Původní idea SDN

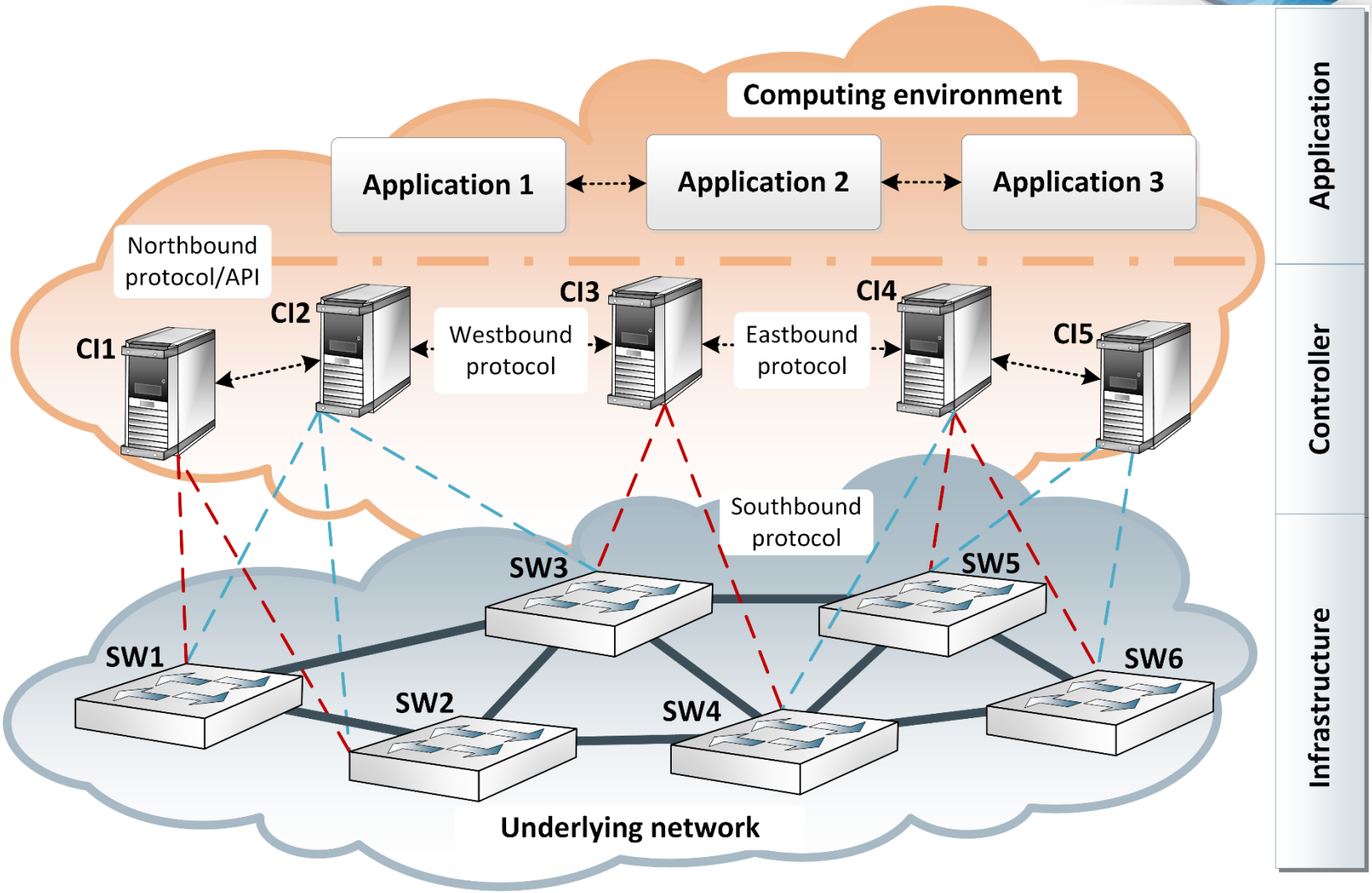


http://www.nojitter.com/post/232602872/how-software-defined-networking-will-change-communications

Definice SDN

- *SDN je takový přístup ke správě počítačových sítí, který umožňuje správcům řídit služby v síti skrze abstrakci funkcí nižších vrstev.*
- Toho je dosaženo pomocí
  1. separace řídící a datové roviny,
  2. logicky centralizovaného kontroleru poskytujícího jednotný pohled na řízenou síť,
  3. otevřeného aplikačního rozhraní mezi řídící rovinou a zařízeními operujícími v datové rovině,
  4. aplikací tvořících logiku síťových funkcí.

Obecná architektura SDN



Co na to historie?

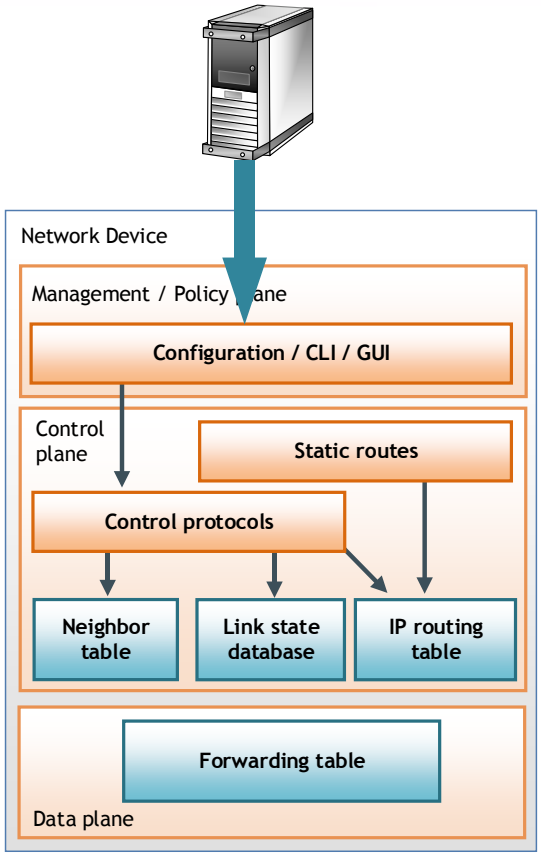
- SDN není prvním svého druhu:
  - The Tempest (1998),
  - Forwarding and Control Element Separation (2004),
  - Path Computation Element (2006),
  - Ethane (2007),
  - OpenFlow (2009),
  - OpFlex (2011),
  - OnePK (2014),
  - a další.

RFC 1925 - Every old idea will be proposed again with a different name and a different presentation, regardless of whether it works.

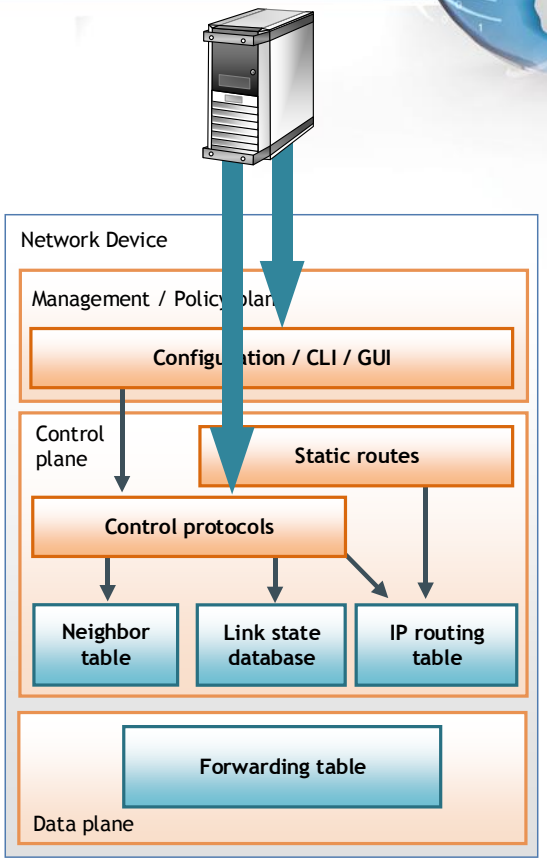
Čtyři cesty k SDN

- Separace řídící a datové roviny:
  - OpenFlow
- Interakce řídící a management roviny:
  - Existující nebo nový řídící protokol (BGP, I2RS)
  - Existující nebo nový management protokol (NETCONF XMPP, OpFlex, OF-Config, SNMPv3, OVSDB)
- Oddělení a abstrakce
  - Překryvné virtuální sítě
  - VPN řešení
- Proprietární API
  - OnePK, eAPI, DirectFlow, …

Architektura nasazení služeb a zařízení v SDN



- Kontroler řídí nasazení nové služby/prvku do sítě s využitím vzorů konfigurace.



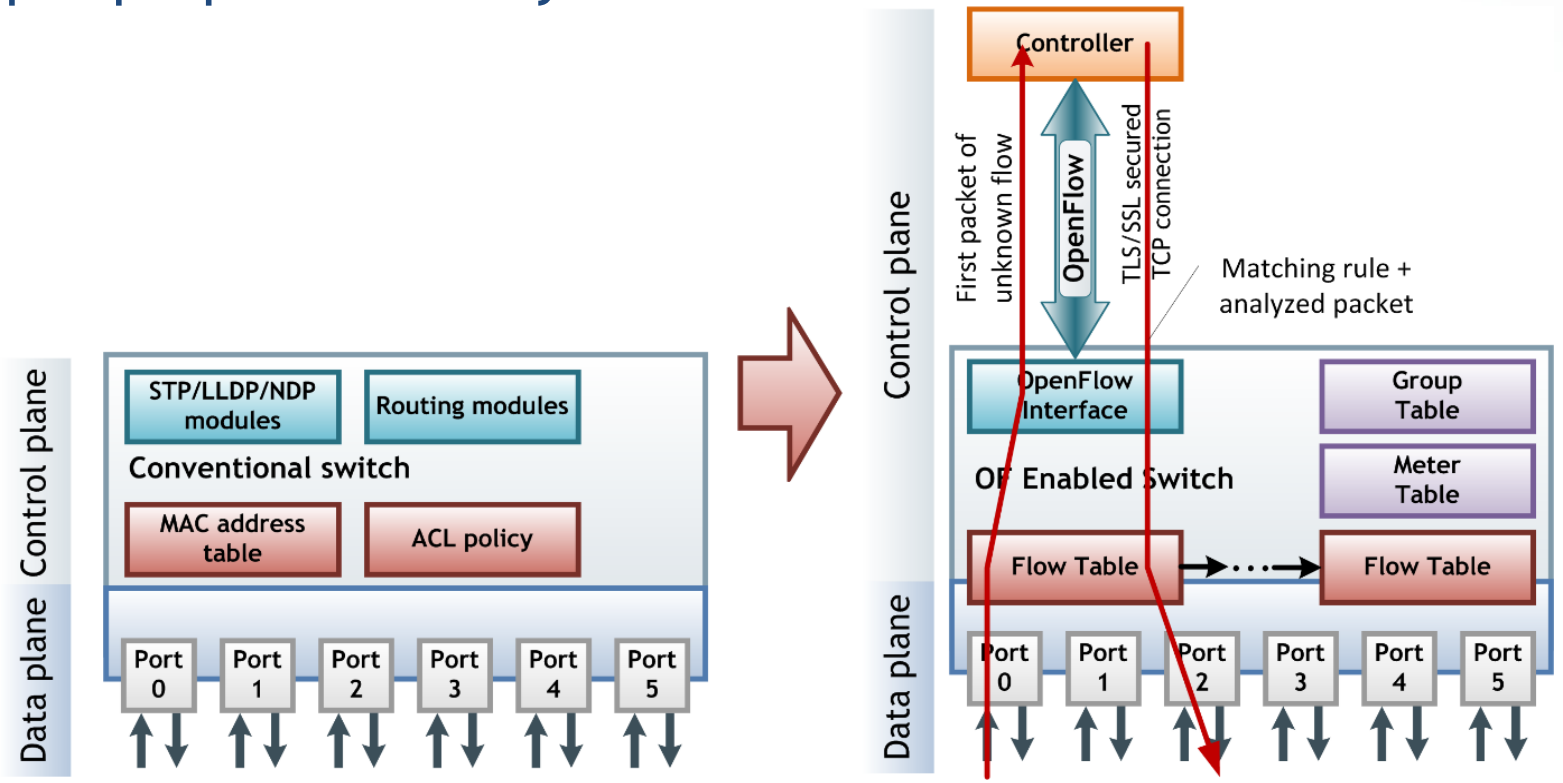
- Kontroler je využíván k úpravám cest v síti skrze programové rozraní nebo protokol řídicí vrstvy.

Případy užití

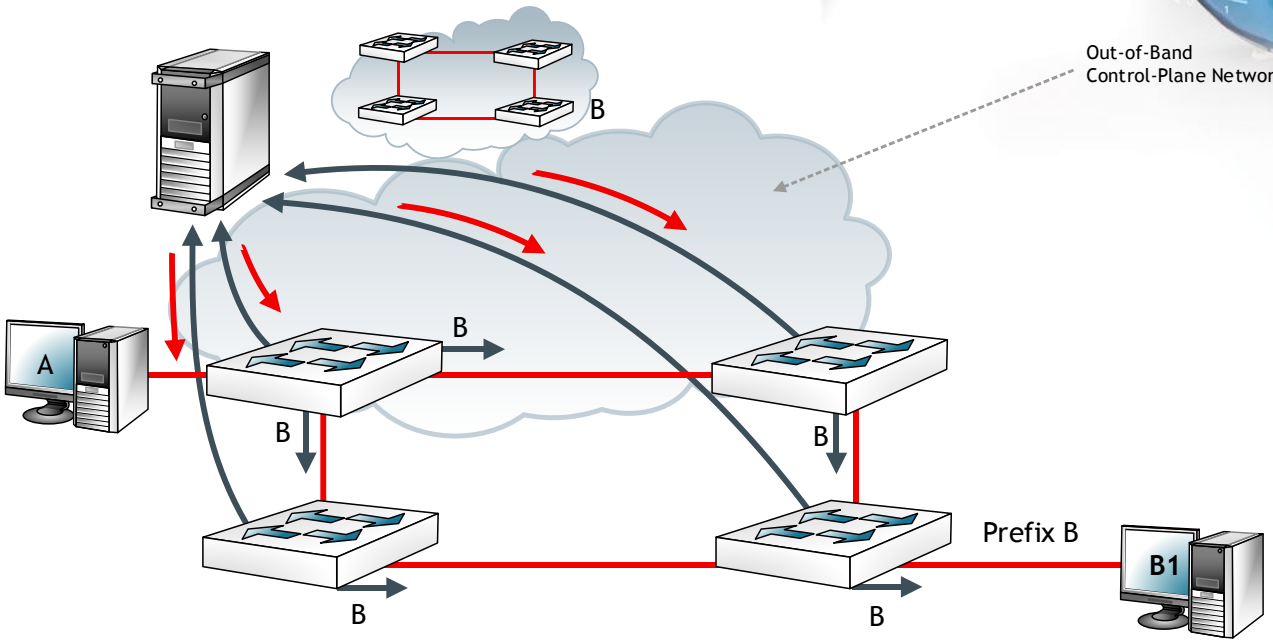
- Záležitosti, které umíme dobře:
  - směrovaní dle L3 destinace hop-by-hop mechanismem.
- Co neumíme tak dobře:
  - řetězení služeb – mikrosegmentace,
  - poskytování služeb s využitím orchestrace (DC),
  - synchronizovaná distribuce politik (QoS, bezpečnost),
  - optimální směrování provozu v síti – problém batohu,
  - směrování *elephant* toků.
- Co neumíme vůbec:
  - adaptace směrování založené na QoS nebo zatížení,
  - směrování postavené na L3/L4 nebo zdroj/cíl,
  - integrace bezpečnostních funkcí do datové roviny.

OpenFlow a separace rovin

- OpenFlow, základní kámen SDN, je postaveno na myšlence oddělení řídící a datové roviny a využití univerzálních TCAM pro přepínání datových rámců.



Základy OpenFlow



- OpenFlow klient v přepínači inicializuje spojení s kontrolerem.
- Kontroler je klíčovým elementem v infrastruktuře a je zodpovědný za distribuci řídicích zpráv.
- Kontroler buduje topologickou mapu řízené sítě (LLDP, operator, ARP, DHCP, etc.)
- Kontroler dotazuje přepínač na jeho vlastnosti a na základě nich a dalších vstupů generuje a odesílá pravidla pro datovou rovinu přepínače.
- Přepínač na základě pravidel toků zanešených do tabulek toků následně přepíná rámce tak, jak v konvenční přepínané síti.

Konfigurační nástroje/protokoly

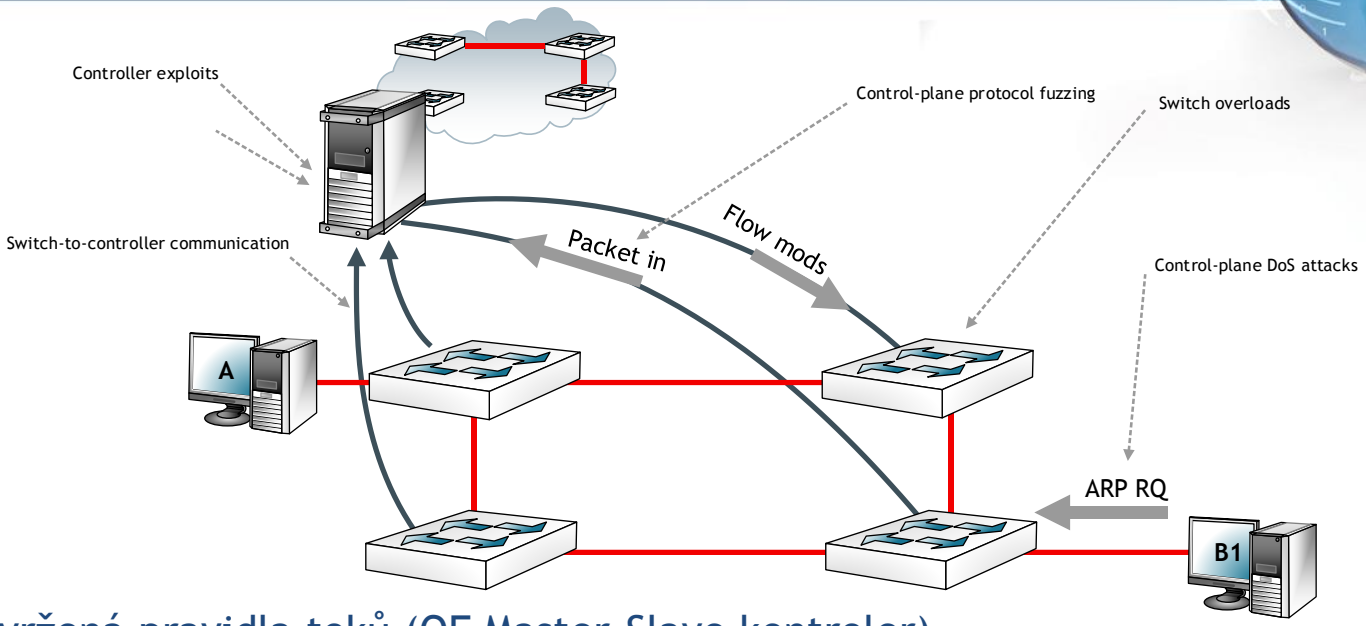
	REST	SNMP	NETCONF	CLI
Data Models	In Code	MIBs	Modules	?
Data Modeling Language	Descriptor?	SMI	YANG	?
Management Ops	GET/PUT etc.	SNMP	NETCONF	?
RPC Protocol	JSON, XML, Forms	BER	XML	CL
Transport	HTTP over TCP + TLS	UDP	SSH, SOAP + TLS, BEEP	SSH, Telnet, Serial port, RS232

- API založená HTTP API jsou pouze moderní CLI, nelze efektivně řešit transakce nebo atomicitu, chybí možnost vrácení stavu při výpadku a notifikace o stavu nelze odeslat jinak než přes *WebSockets*.

Nasazení SDN

- **Hardwarové selhání** – Co když selže logický nebo fyzický kontroler?
- **Softwarové selhání** – Jsou použité aplikace bez chyb, byly dostatečně testovány a jsou srozumitelné?
- **Kompatibilita** – Jsou vybrané HW a SW prostředky kompatibilní?
- **Údržba** – Existuje strategie pro SW a HW upgrade? Mohou služby v síti akceptovat výpadek?
- **Latence** – Může zpoždění tvořené vyhodnocením toku negativně ovlivnit poskytované služby?
- **Škálovatelnost** – Je možné škálovat kontroler vertikálně nebo horizontálně? Umožňují aplikace provoz v multikontrolerovém prostředí?
- **Bezpečnostní slabiny** – Je všechny prvky v řídícím řetězci dostatečně zabezpečeny a jsou potenciální hrozby identifikovatelné?

(Ne)bezpečnost SDN

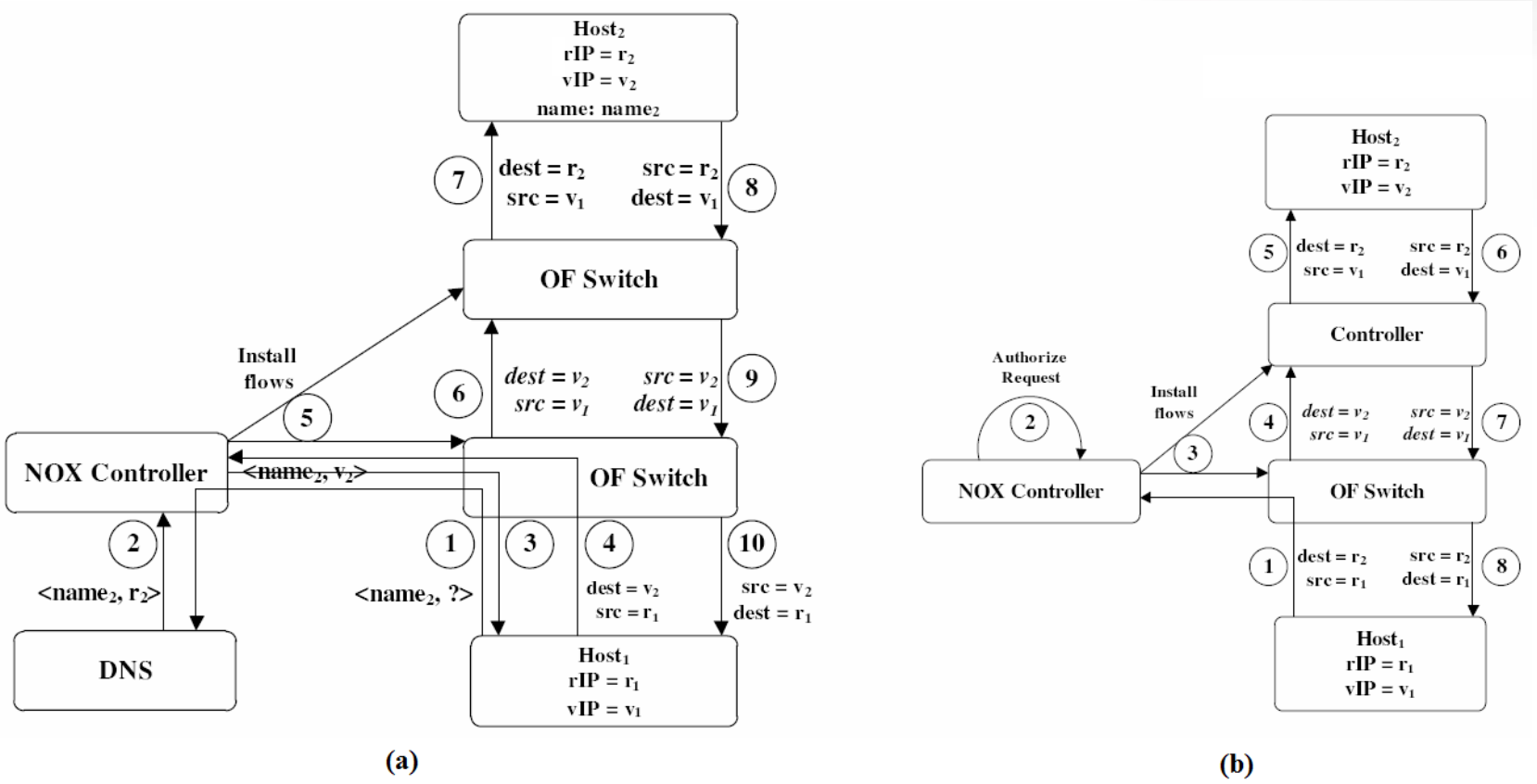


- Podvržená pravidla toků (OF Master-Slave kontroler).
- Útok na slabá místa přepínačů.
- Útoky na řídící rovinu (XXE NETCONF, Topology spoofing, DoS)
- Útoky na slabá místa na kontroleru, validnost a konzistence instalovaných pravidel.
- Nedostatky mechanismů zajišťující důvěru mezi kontrolerem a management systémem.
- Útoky na administrační stanici.
- Nedostatky v procesu šetření a napravení incidentů.
- Odříznutí kontroleru od řízené sítě.

Vynucení bezpečnostních politik

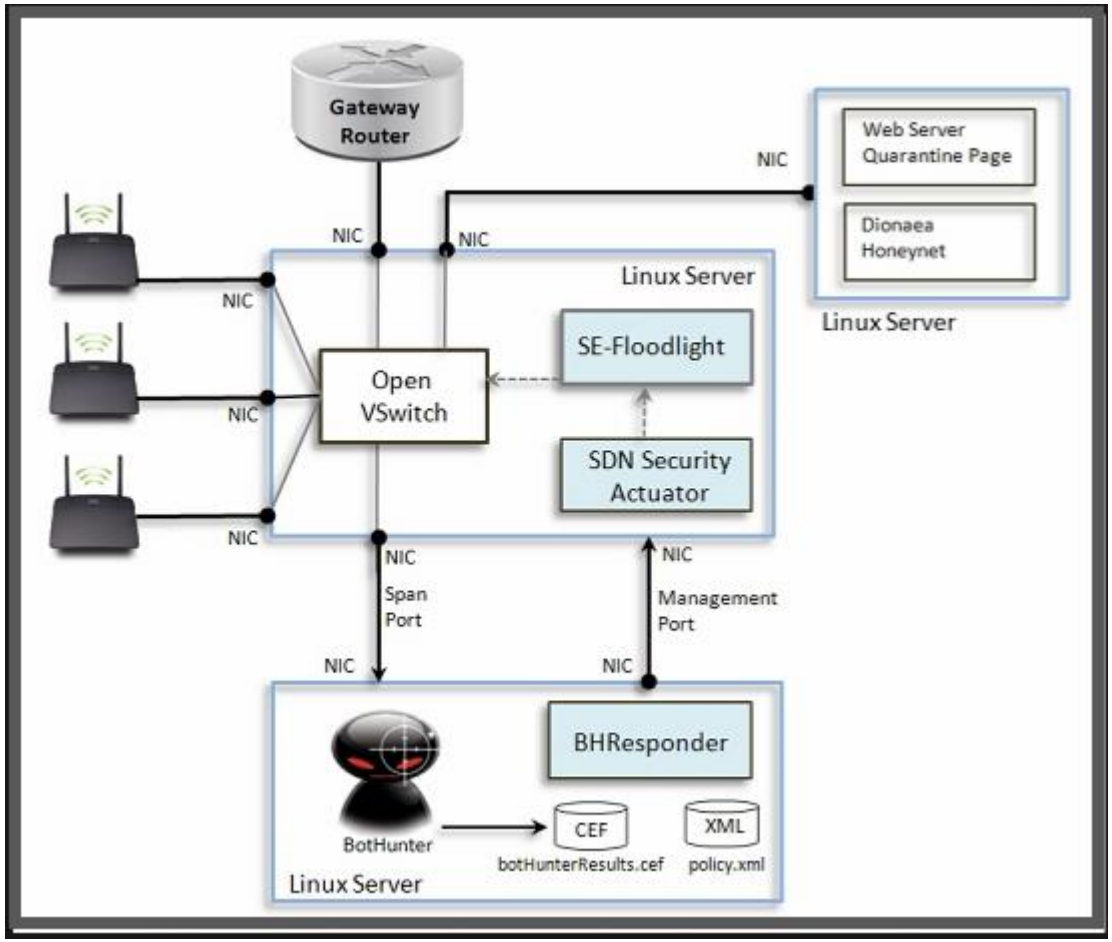
- Jak se vypořádat s konfliktními pravidly vedoucími k nekonzistentnímu chování sítě?
- Externí kontrola modelu
  - Vyhrazený modul, přidaná vrstva provádí inspekci (simulaci) pravidel a blokuje ty, která nejsou validní.
  - FlowChecker, Flover, VeriFlow.
- Omezení kompaktním frameworkem
  - FRESCO – SE-kontroler s řadou rolí omezující akce modulů.
  - FatTire, Frenetic – jazyk pro popis *fault-tolerant* směrování v síti.

Obrana mutací adres hostů



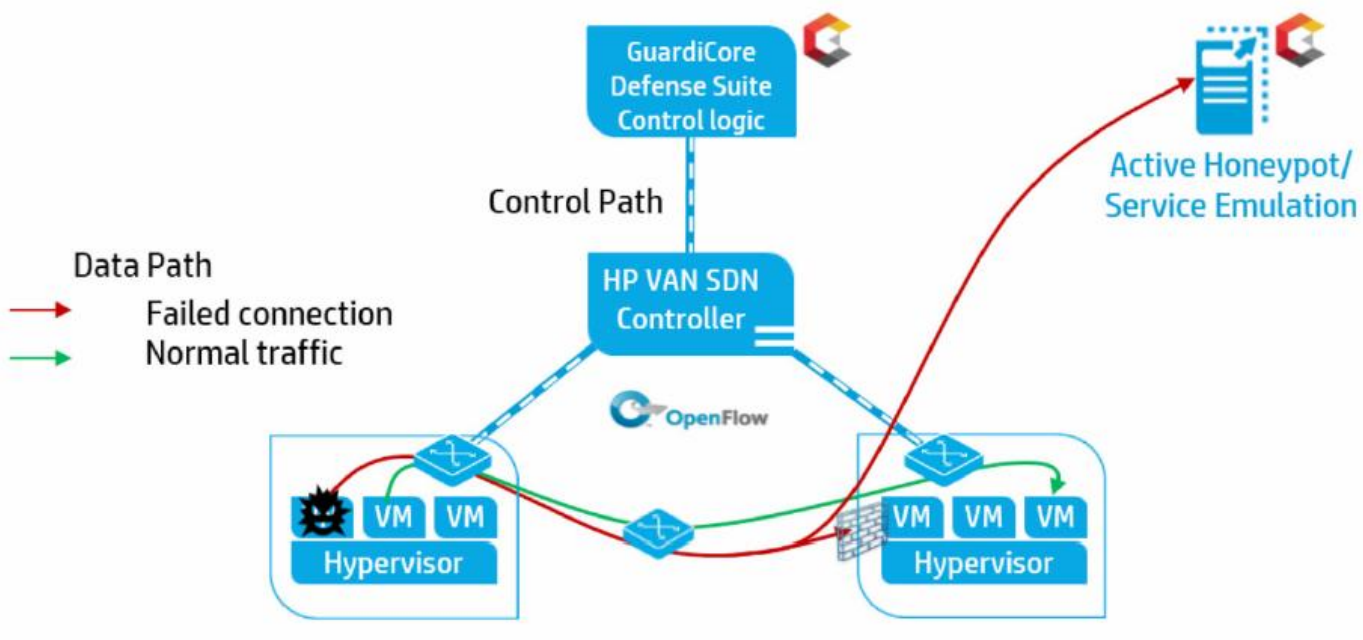
Jafar Haadi Jafarian, Ehab Al-Shaer, and Qi Duan. Openflow random host mutation: Transparent moving target defense using software defined networking. In Proceedings of the First Workshop on Hot Topics in Software Defined Networks, HotSDN '12, pages 127-132, New York, NY, USA, 2012. ACM. ISBN 978-1-4503-1477-0

OF-BotHunter



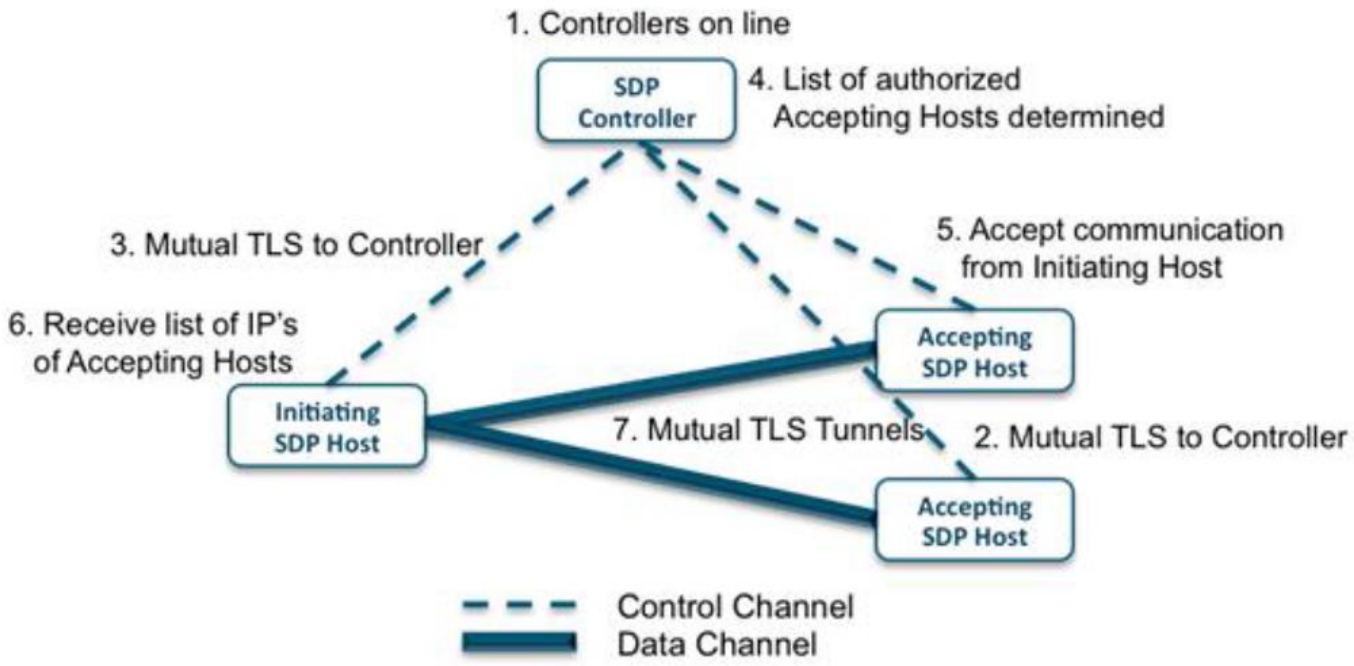
sdnsecurity.org/project_attack_defense.html

Aktivní *honeypots*



GuardiCore. Data center security redened. Technical report, Hewlett-Packard, 2014. http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-1629ENW.

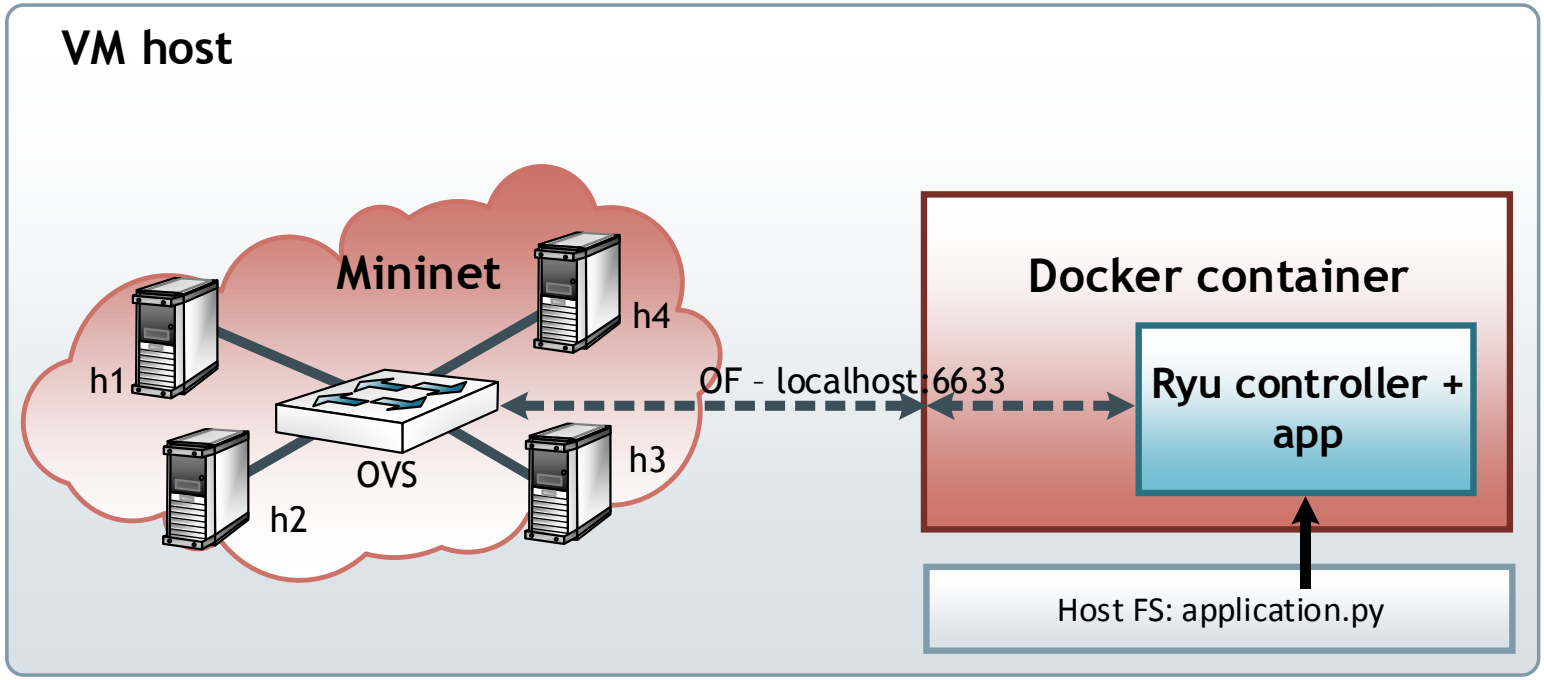
Softwarově Definovaný Perimetr



Brent Bilger, Alan Boehme, Bob Flores, Zvi Guterman, Mark Hoover, Micahela Iorga, Junaid Islam, Marc Kolenko, Juanita Koilpilla, Gabor Lengyel, Gram Ludlow, Ted Schroeder, and Je Schweitzer. SDP Specication v1.0. Technical report, Cloud Security Alliance, 2014. https://downloads.cloudsecurityalliance.org/initiatives/sdp/SDP_Specification_1.0.pdf

Aplikační ukázka

- Dopady neinteligentní aplikace na výkon sítě.



Shrnutí

- Rychle rostoucí počet aplikačních služeb nasazovaných do sítí a jejich logické dělení vede na stále vyšší potřebu efektivního, spolehlivého a bezodkladného nasazení síťových služeb.
- Centralizované řízení musí být velmi dobře navrženo s ohledem na maximální možní omezení nedostupnosti kontroleru a vysokou škálovatelnost.
- Je téměř nemožné odpovědně spravovat více, jak 100 zařízení přes CLI.
- OpenFlow není SDN je to pouhá jeho součást.
- SDN přináší mnoho benefitů, ale zároveň také nové bezpečnostní hrozby.
- SDN za posledních několik let urazilo obrovskou část cesty do produkčního prostředí a v některých oblastech začíná být nezbytné.