Demilitarizovaná zóna (DMZ)

Bezpečnostní seminář ČP AFCEA

Aktuální trendy v zabezpečení DMZ

Dalibor Sommer/ březen 2013

Agenda

HP Enterprise Security Strategy

Aktuální bezpečnostní hrozby

SDN a jeho využití v bezpečnostních řešeních

Bezpečnostní strategie HP

HP Enterprise Security

Produktové portfolio

HP ArcSight

- skupina produktů pro správu, zpracování a archivaci událostí

HP TippingPoint

- síťové IPS systémy

HP Fortify & WebInspect

- rodina produktů pro bezpečnostní testování aplikací

HP Enterprise View

- systém pro výpočet rizik

Bezpečnostní hrozby

Aktuální bezpečnostní hrozby

HP 2012 Cyber Risk Report

Zveřejněné zranitelnosti

- 19% nárůst zveřejněných zranitelností
- 68% nárůst zveřejněných zranitelností pro mobilní zařízení
- Pomalejší a složitější odhalení či zveřejnění
- Web aplikace stále primárním cílem

Aktuální bezpečnostní hrozby

OWASP 2013 - https://www.owasp.org/index.php/Top_10_2013

- A1-Injection
- A2–Broken Authentication and Session Management
- A3–Cross-Site Scripting (XSS)
- A4–Insecure Direct Object References
- A5–Security Misconfiguration
- A6–Sensitive Data Exposure
- A7–Missing Function Level Access Control
- A8-Cross-Site Request Forgery (CSRF)
- A9-Using Components with Known Vulnerabilities
- A10–Unvalidated Redirects and Forwards

Aktuální bezpečnostní hrozby

Je tedy vše jako dřív?

ROZHODNĚ NE!

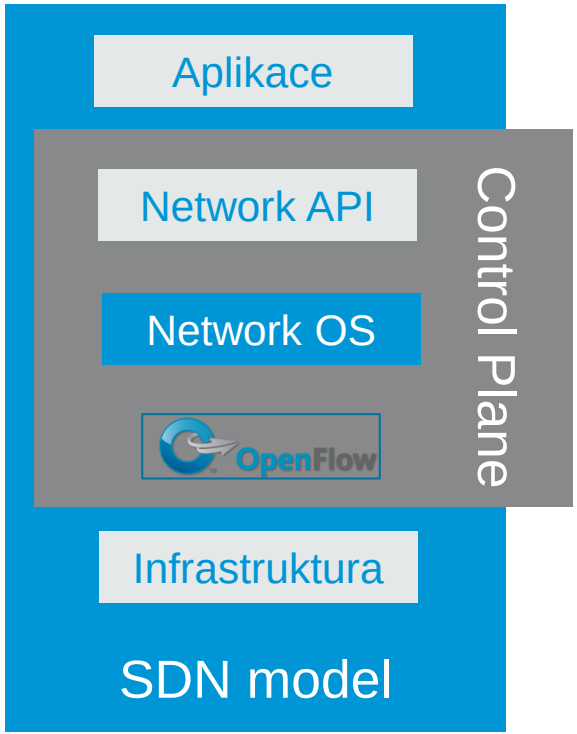
- Masivní nárůst mobilních zařízení
- Přesun aplikací a dat do „Cloudu“
- Síla a dopady DoS a DDoS útoků

Unauthorized access | Cross-site scripting | Sensitive information disclosure | Insecure session handling | Cookie handling vulnerabilities | Improper encryption | Poor logging practices | Autocomplete on sensitive form fields | Cleartext credentials | Poor error messages

SDN a jeho využití v bezpečnostních řešeních

Software-defined Networking (SDN)

Nová pružnější síťová architektura



Abstrakce rozhodování (control plane) od zpracování (forwarding hardware)

- Centrální softwarové řízení
- Centrální přehled topologie a datových toků
- Dynamicky programovatelná síť reagující na aplikace
- Lze implementovat více metodami, například s OpenFlow

Klíčové výhody

- Umožňuje rychlejší inovace
  - Méně změn v OS, HW, bez potřeby nových komunikačních protokolů, zdlouhavé standardizace či uzavřených řešení
- Velké výhody pro campus, datové centrum, cloud i ISP

Software-defined Networking (SDN)

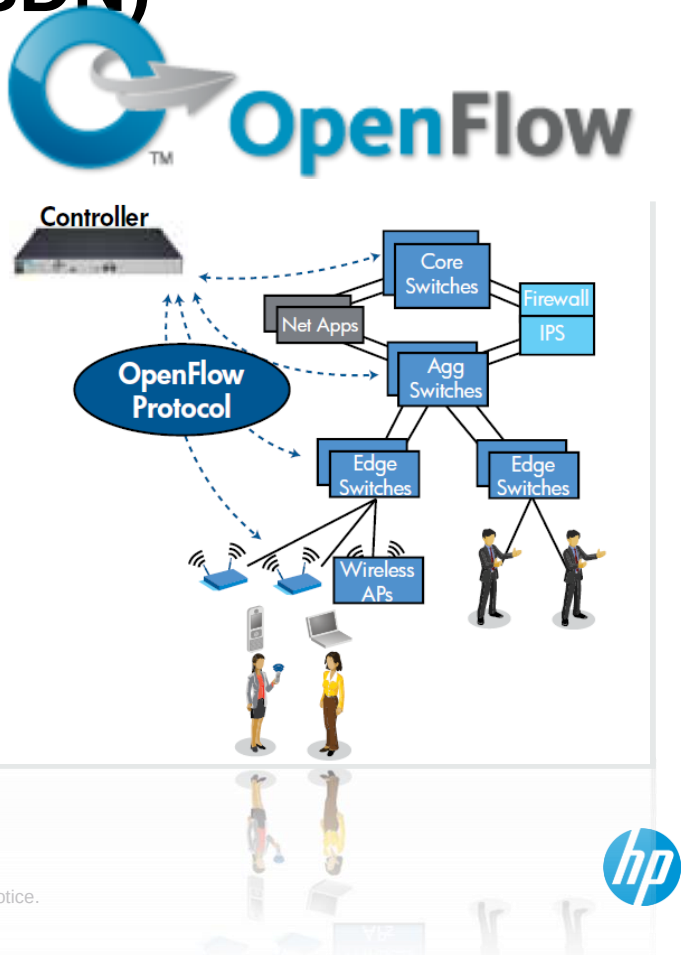
Co je OpenFlow?

OpenFlow je API pro dynamické nastavování forwarding plane switchů

Umožňuje centrální řízení s jemností na jednotlivá flow

Kontroler má perfektní možnosti rozhodovat o každém flow dynamicky a v reálném čase

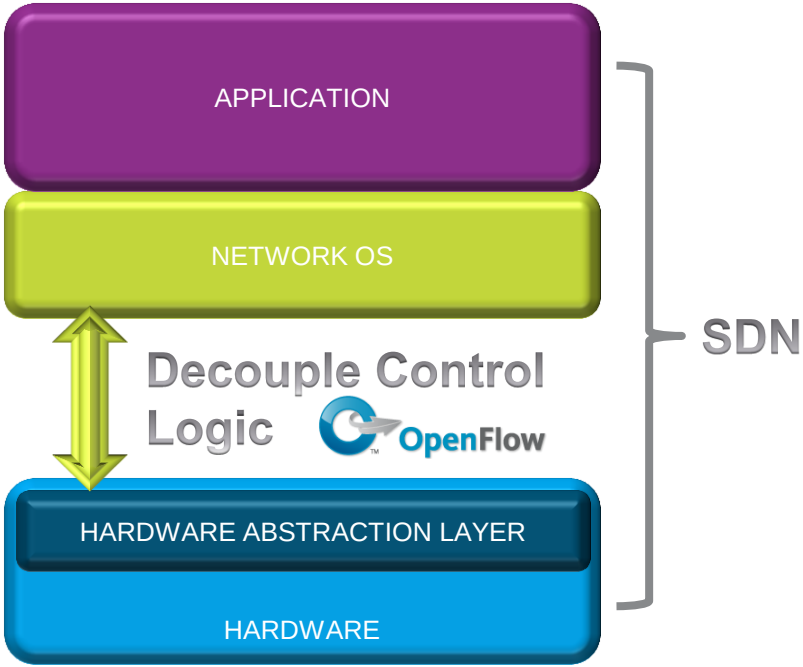
Definováno v Open Networking Foundation



Software-defined Networking (SDN)

Co SDN není?

- Samotná implementace síťových funkcí jako software nebo VM
- Samotná implementace programovatelných proprietárních API do síťových zařízení
- Konec inovací v hardwaru



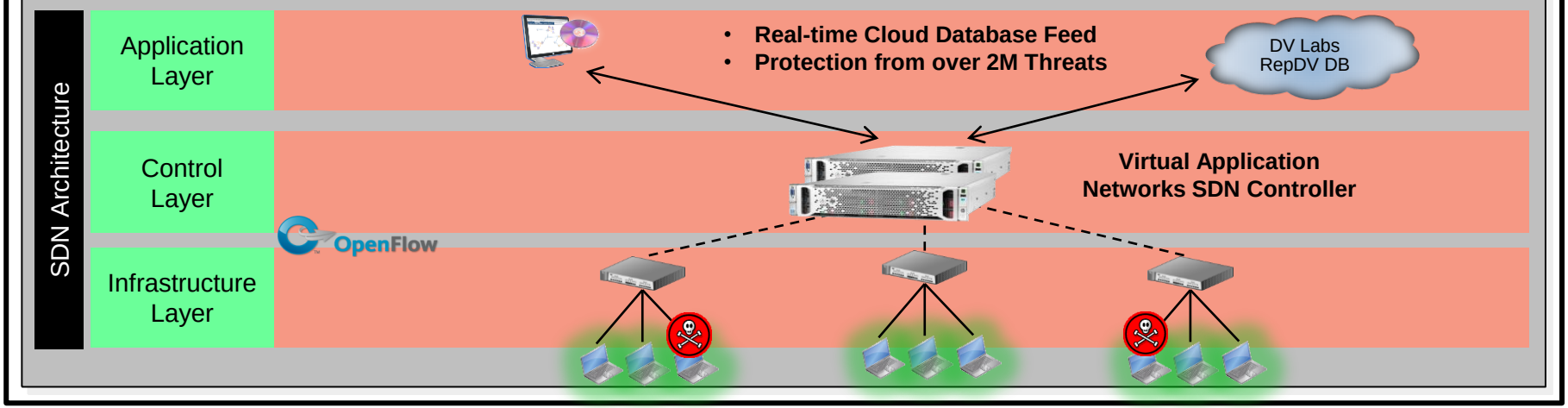
Source: ONF Forum

SDN Security Application Use Case

Campus & Branch Security

Data Center Security

Cloud Security



Scales to Thousands of Endpoints

Eliminates Need for Dedicated Appliances

Automates Threat Protection for BYOD

Uses standard-based OpenFlow

Sentinel – bezpečnostní SDN aplikace

Ochrana sítě v reálném čase

- Přináší nepřetržitou ochranu sítě v reálném čase s využitím databáze HP TippingPoint DVLabs
- Chrání před více jak 700,000+ botnety, malware a škodlivými stránkami
- Lepší visibilita a přesnost díky integraci s ArcSight
- Tajemství je ve využití OpenFlow
- Běží na HP Virtual Application Networks SDN kontroleru

Shrnutí

Závěr

- Opusťte tradiční pohled na problematiku DMZ – chybí vliv Cloudu a Mobility
- Neexistuje jedno zařízení, které dokáže pokrýt aktuální útoky a hrozby
- Využívejme více řešení založená na „*security by design*“
- Vzrůstá potřeba optimalizace výstupů ze systémů pro správu bezpečnostních událostí
- Moderní analytické nástroje budou potřebovat výkonnou složku

Děkuji za pozornost