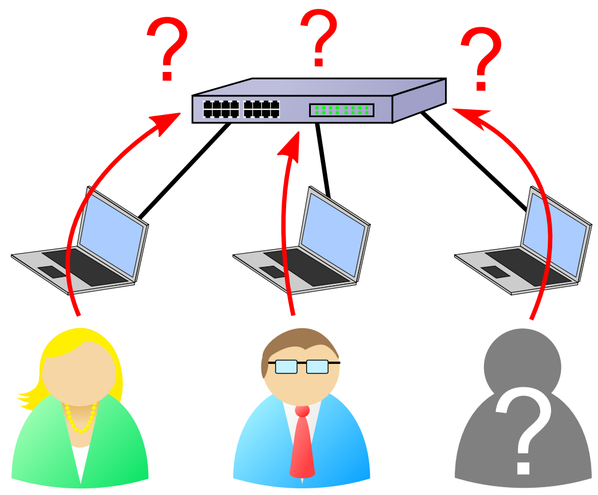
SDN riadené pomocou identity používateľov

Martin Holkovič
xholko00@stud.fit.vutbr.cz

Excel@FIT 2015
ID:77

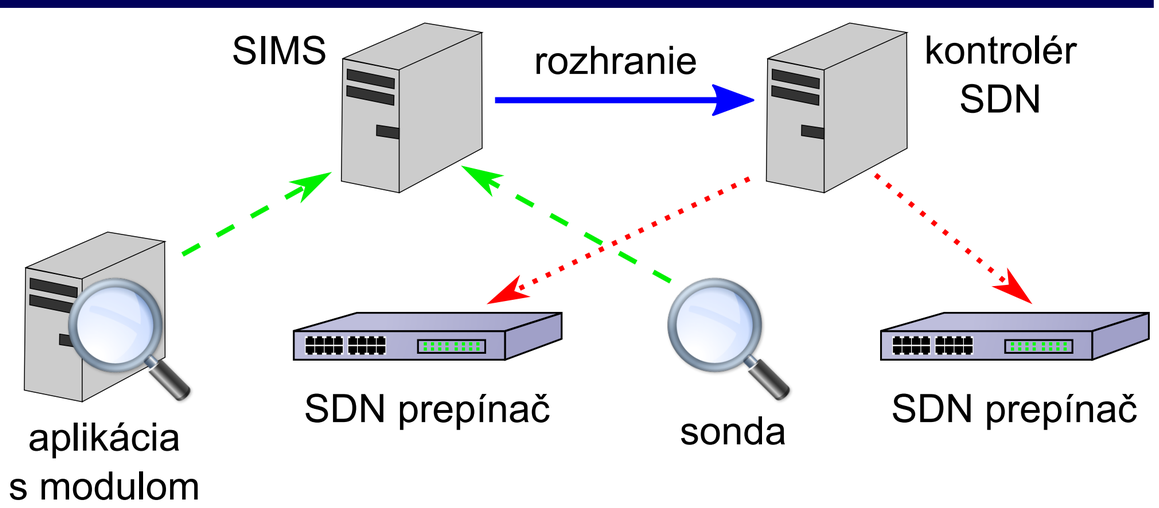
Úvod a motivácia

- Správa počítačovej siete nie je jednoduchá
  - veľké množstvo zariadení v sieti
  - používatelia zapájajú vlastné zariadenia do siete
- Architektúra SDN správu siete zjednodušuje
  - centrálna konfigurácia zariadení
  - aplikáciami riadená sieť
- Rozšírenie SDN siete o identity používateľov
  - správa na základe identity používateľa
  - konfigurácia siete na vyššej úrovni



Návrh

- Systém SIMS
  - vyvinutý v rámci projektu Sec6Net
  - deteguje používanie identifikátorov a spojuje ich
- Prepojenie SIMSu so sieťou SDN
  - SIMS odosiela identifikátory riadeniu SDN
- Detekcia identity
  - používateľ sa autentifikuje
  - zistenie skupiny do ktorej patrí používateľ
  - pakety sú označené zistenou skupinou



Implementácia

- použitý kontrolér Pyretic
- názov skupiny je v paketoch uložený formou VLAN tagu
- sieťová politika definovaná if-then pravidlami
- aplikácie vytvárajú pravidlá podľa užívateľských skupín

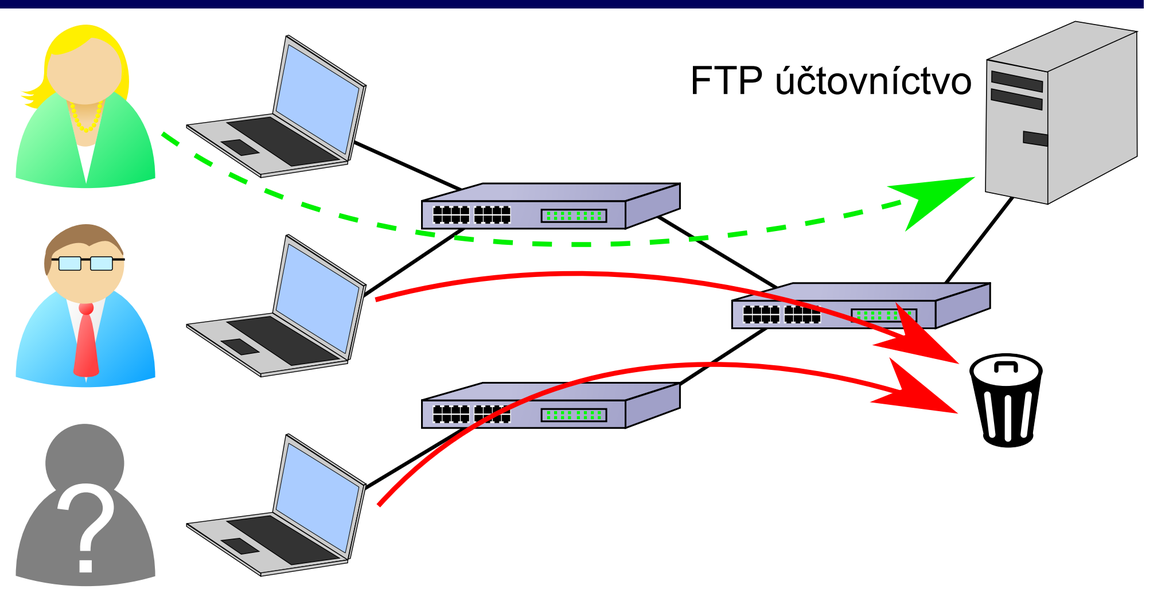
Používateľ	Názov skupiny	VLAN tag
Araňa	manažment	1
Dezider	vývoj	2
Etela	vývoj	2
*	default	1000

Prípad použitia: filtrovanie

- Zabezpečenie prístupu ku zdrojom
- Konfigurácia aplikácie

Služba	Parametre	Oprávnené skupiny
Web	192.168.1.1:TCP 80	*
FTP-účtovníctvo	192.168.1.2:TCP 210	manažment
FTP-projekty	192.168.1.2:TCP 21	manažment, vývoj

- Špecifické pravidlá sa nastavujú iba na prvkoch, kde je priamo pripojený niektorý zo zdrojov
  - pre oprávnené skupiny sa vytvoria povolovacie pravidlá
  - ostatná komunikácia sa bude zahadzovať

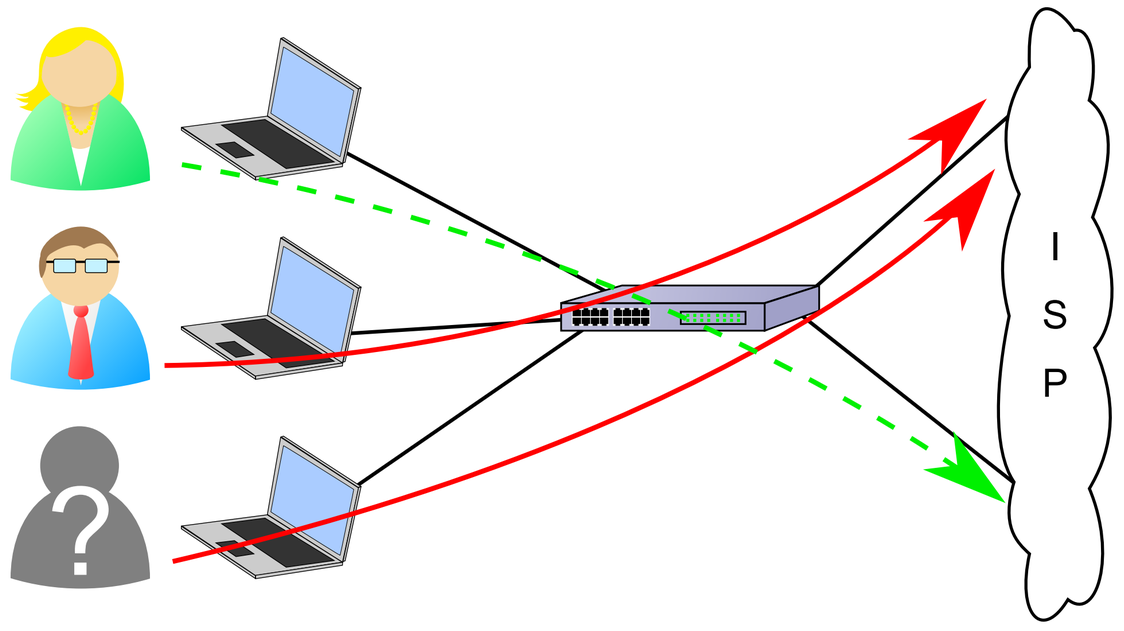


Prípad použitia: smerovanie

- Výber smerovacej topológie podľa odosielateľa
- Konfigurácia aplikácie

Linka	Skupina	Podmienka použitia
s1-1	manažment	žiadna
s1-1	vývoj	keď s1-2 nefunguje
s2-2	manažment	keď s1-1 nefunguje
s2-2	*	žiadna

- Pre každú skupinu sa vytvorí graf siete
  - z grafu sa odstránia linky pre ktoré nemá skupina oprávnenie
  - algoritmom Dijkstra sa z grafu vytvoria smerovacie pravidlá
  - smerovacie pravidlá sa nastavia na prvky v sieti



Vyhodnotenie

- Prednosti riešenia
  - nezávislosť na konkrétnom výrobcovi sieťových prvkov
  - možnosť tvorby ľubovoľnej aplikácie
- Možné rozšírenia práce
  - zohľadniť čas, typ a polohu zariadenia pri voľbe politiky
  - súčasné použitie viacerých autentifikáčných metód
  - podpora IPv6