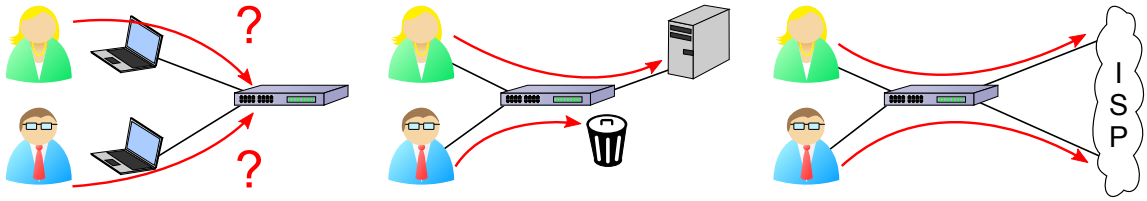
Excel@FIT 2015
http://excel.fit.vutbr.cz

SDN riadené pomocou identity používateľov

Martin Holkovič*



Abstrakt
Jedným z posledných trendov firemných počítačových sietí je možnosť zapojiť si vlastné zariadenie do siete. Tento trend otvára nové výzvy pre sieťových administrátorov. Jedným z prístupov ako sa k problému so správou veľmi dynamických sietí vysporiadať je správa pomocou identít používateľov. Namiesto vytvárania konfigurácie sieťových prvkov na základe pripojených koncových staníc (MAC adresa, IP adresa) sa konfigurácia vytvára podľa identity užívateľov, využívajúcich koncové stanice (meno užívateľa, pracovná skupina). Výsledkom práce je rozšírenie riadenia SDN sietí o znalosť identít používateľov pomocou systému pre detekciu a správu identít. Takto rozšírené riadenie umožňuje administrátorovi konfigurovať a spravovať sieť prostredníctvom identity používateľov. Súčasťou práce je taktiež vytvorenie prípadu použitia znázorňujúceho výhody tohto prístupu.

Kľúčové slová: SDN — dynamická identita — Pyretic — OpenFlow

Priložené materiály: *N/A*

*xholko00@stud.fit.vutbr.cz, *Fakulta informačních technologií, Vysoké učení technické v Brně*

1. Úvod

Počítačové siete sa rovnako ako všetky iné oblasti IT vyvíjajú a neustále čelia novým trendom, technológiám a výzvam. Aktuálne je veľmi diskutovaná nová architektúra SDN (z anglického Software Defined Networking). Jedná sa o úplne nový prístup k sieťam, jej správe a možnostiam nasadenia nových technológií. Siete SDN umožňujú veľmi efektívne prepojenie ľubovoľnej aplikácie s riadením počítačovej siete. Vďaka tomuto prepojeniu je na základe znalosti počítačovej siete možné zlepšiť funkcionalitu aplikácií alebo je možné zlepšiť samotnú funkcionalitu siete zo strany aplikácií. Jednou z oblastí zlepšenia siete na základe informácií od aplikácií je správa siete.

Ak zoberieme do úvahy skutočnosť, že do počítačovej siete sú zapojované ľubovoľné zariadenia používateľov siete, ktoré nie sú pod správou administrátorov siete, správa počítačovej siete je komplikovaná činnosť. Pre uľahčenie správy siete by bolo vhodnejšie sieť riadiť na základe identity používateľov. Namiesto vytvorenia pravidiel pre každé pripojené zariadenie by sa vytvorili pravidlá pre každého používateľa. V prípade zapojenia nového zariadenia používateľom by stačilo toto zariadenie prepojiť s identitou používateľa a nebolo by tak nutné vytvárať pravidlá pre každé zariadenie zvlášť.

Článok popisuje vytvorenie rozhrania medzi systémom pre správu identít a riadením siete SDN, ktoré bolo pre tento účel rozšírené. Pomocou znalosti identít v riadení siete sa pakety používateľov budú označovať na základe identity používateľov. Vďaka označeniu bude možné využívať znalosť identít pri vývoji aplikácií pre správu siete. Článok zobrazuje výhodu tohto prístupu na aplikácii pre filtrovanie a smerovanie dátovej prevádzky.

2. Súvisiace práce

Firmy HP, Cisco a Juniper ponúkajú ako riešenie produkty Identity Driven Management (IDM) [1], Identity Service Engine (ISE) [2] a Identity and Policy Control [3]. Riešenie spočíva v autentifikácii klienta prostredníctvom protokolu 802.1x alebo prostredníctvom webovej autentifikácie a následnom kontaktovaní proprietárnej centrálnej aplikácie od príslušnej firmy, ktorá sa stará o konfiguráciu sieťových prvkov.

Druhým možným prístupom je autentifikácia tokov pomocou riadenia SDN siete [4]. Na rozdiel od riešenia uvedených spoločností, toto riešenie nevyžaduje sieťové prvky od konkrétneho výrobcu k čomu využíva architektúru sietí SDN. Každý nový užívateľ sa prostredníctvom webovej stránky autentifikuje, čím riadiaca logika SDN deteguje identitu používateľa. Každý nový tok od užívateľa prejde riadiacou logikou SDN siete a tá určí, či je tok možné povoliť alebo je nutné ho zakázať. Pretože každé nové spojenie musí najprv prejsť riadiacou logikou SDN kontroléra, zvyšuje sa doba spracovania každého nového spojenia.

Obidve riešenia majú ten nedostatok, že sa zameriavajú iba na filtrovanie prevádzky (firewall). Moje riešenie spočíva vo vytvorení univerzálnej platformy prostredníctvom architektúry SDN nad ktorou by bolo možné vytvoriť rôzne aplikácie pre riadenia siete. Príklad takýchto aplikácií môže byť už spomenuté filtrovanie, monitorovanie, smerovanie a ďalšie. Ďalším nedostatkom oboch riešení je, že systém pre kombináciu a spracovanie identít používateľov spájajú so samotnou realizáciou funkcie filtrovania prevádzky. Súčasťou môjho riešenia je využitie systému na správu identít z projektu Sec6Net označovaného ako SIMS [5].

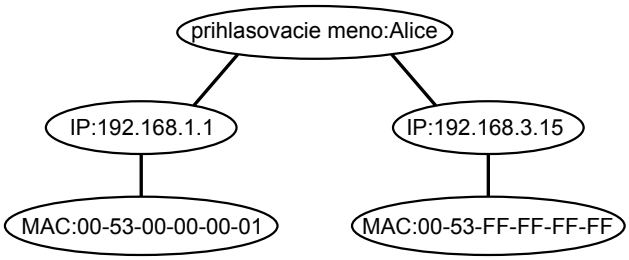
3. Návrh

3.1 Softwarovo definované siete

Aby sme mohli sieťové prvky riadiť na základe identity je nutné, aby sieťové prvky mohli byť konfigurovateľné adaptívne, automaticky a centralizovane. Klasická architektúra sietí nám takéto možnosti priamo neposkytuje a preto je vhodné využiť architektúru SDN sietí [6]. Siete SDN sú spravované centrálnym prvkom nazývaným kontrolér, ktorý okrem podnetov zo strany administrátora reaguje na každú zmenu v počítačovej sieti. Kontrolér tak na základe informácií o aktuálne pripojených zariadeniach do siete a na základe konfigurácie zo strany administrátora výkonáva správu sieťových prvkov.

3.2 Systém SIMS

Pre detekciu používateľských identít je použitý systém SIMS (Sec6net Identity Management System) vyvinutý v rámci projektu Sec6Net. Pre detekciu identít SIMS vykonáva dve hlavné funkcie:



Obrázok 1. Reprezentácia identity používateľa s prihlasovacím menom *Alice* pomocou grafu.

1. Detegovanie identifikátorov zo siete.
2. Spojovanie identifikátorov pre vytvorenie celkového pohľadu na identity používateľov.

Identifikátor je unikátna hodnota používaná aplikáciami pre jednoznačnú identifikáciu používateľa alebo zariadenia. Príkladom identifikátoru je IP adresa používaná IP stackom alebo prihlasovacie meno do informačného systému. Detekcia používania identifikátorov je vykonávaná prostredníctvom sond, ktoré analyzujú datovú prevádzku v sieti alebo prostredníctvom modulov, ktoré sú s príslušnými aplikáciami priamo integrované. Takto definované identifikátory sú následne odoslané systému SIMS.

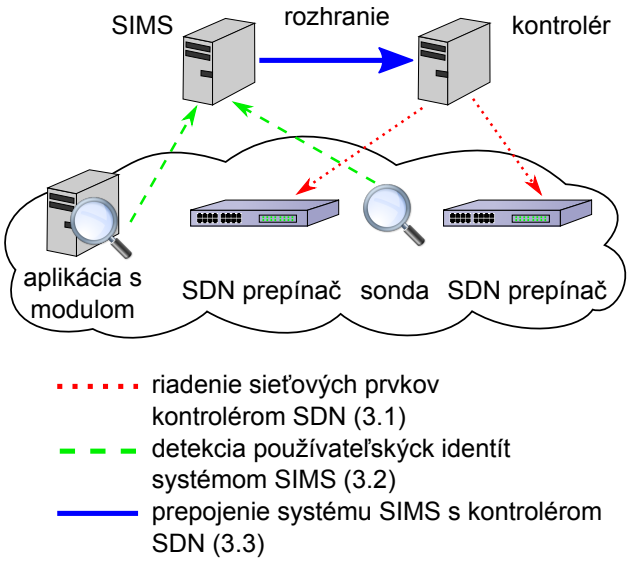
Systém SIMS pomocou grafových algoritmov vytvára zo všetkých prijatých identifikátorov graf, kde uzlami grafu sú identifikátory a hranami sú prepojené identifikátory spolu patriace. Identita používateľa sa vo výsledku skladá z množiny prepojených identifikátorov. Na obrázku č. 1 je zobrazený graf patriaci identite používateľa s prihlasovacím menom *Alice*.

3.3 Prepojenie systému SIMS so sieťou SDN

Aby bolo možné využiť znalosti identít zo systému SIMS v riadení siete SDN, je nutné dané technológie prepojiť. Súčasťou práce je vytvorenie rozhrania medzi systémom SIMS a kontrolérom siete SDN. Rozhranie využíva TCP sockety a knižnicu JSON pre serializáciu prenášaných objektov. Pomocou tochto rozhrania bude systém SIMS informovať o zmenách identít týkajúcich sa identifikátoru prihlasovacieho mena do webového informačného systému. Konkrétne sa jedná o zmeny:

1. prihlásenie používateľa,
2. odhlásenie používateľa,
3. pridanie nového zariadenia k používateľovi.

Odobranie zariadenia zo siete sa neoznamuje, pretože touto informáciou už kontrolér SDN disponuje. Každá správa okrem typu zmeny obsahuje aj prihlasovacie meno používateľa a MAC adresu zariadenia.



Obrázok 2. Architektúra SDN siete zobrazujúca prepojenie so systémom SIMS.

Príjem správ kontrolérom je realizovaný prostredníctvom nového vlákna kontroléru, ktoré po príjme správy upraví lokálnu databázu MAC adries a používateľských mien a následne zavolá funkciu pre aktualizovanie používanej politiky. Kontrolér po aktualizovaní politiky prispôsobí riadenie sieťových prvkov tak, aby bola splnená politika nastavená sieťovým administrátorom. V aktuálnej verzii je rozhranie jednosmerné zo smeru od systému SIMS do kontroléru. V budúcnosti sa však rozhranie bude používať aj opačným smerom pre možnosť kontroléru zistiť aktuálnu databázu identít od systému SIMS. Rozhranie je znázornené na obrázku 2.

4. Implementácia

4.1 Detekcia identity

Prvou časťou implementácie je uloženie informácie o používateľoch siete v rámci kontroléra SDN. K tomuto účelu bol využitý kontrolér Pyretic [7], ktorý bol rozšírený o možnosť prijímať externé udalosti vyvolávajúce aktualizáciu sieťovej politiky. V rámci tejto práce je udalosť chápaná ako informovanie o zmene v znalosti identít používateľov systémom SIMS.

Po pripojení nového zariadenia do siete vytvorí kontrolér SDN pravidlo, aby prvý odoslaný paket od daného zariadenia bol preposlaný na kontrolér pre uloženie zdrojovej MAC adresy. Po spracovaní prvého paketu je toto pravidlo odstranené a všetky nasledujúce pakety už do kontroléru nebudú preposielané. Pomocou tohto pravidla sa vytvorí mapovanie medzi MAC adresami zariadení a portami sieťových prvkov.

Zároveň s tým, ako sa zapojí koncové zariadenie do siete, vytvorí sa pravidlo pre označovanie paketov skupinou *default*. Kontrolér automaticky prevádza názvy skupín na hodnoty VLAN ID. Pre zmenu názvy skupiny do ktorej dané zariadenie patrí, je nutné sa na danom zariadení prihlásiť prostredníctvom webovej stránky. Prihlásenie na stránku je detegované systémom SIMS a prihlasovacie meno je spolu s MAC adresou odoslané kontroléru SDN. Kontrolér SDN si zistí názov skupiny do ktorej patrí používateľ s daným prihlasovacím menom. Pomocou mapovania MAC adries s portami sieťových prvkov sa nájde port do ktorého je zapojené príslušné zariadenie a vytvorí sa pravidlo pre označovanie paketov skupinou do ktorej patrí prihlásený používateľ. Predošlé pravidlo pre označovanie paketov je odstránené.

4.2 Tagovanie paketov

Aby bolo možné pri spracovaní sieťovej prevádzky rozhodovať na základe identity používateľa, sú pakety označené VLAN tagom reprezentujúcim danú identitu. Vzhľadom k tomu, že viacero užívateľov by zdieľalo tú istú sieťovú politiku (napr. zamestnanci jedného oddelenia) je z hľadiska úspory počtu vytvorených pravidiel lepšie užívateľov rozdeliť do skupín a politiku vytvárať pre celé skupiny používateľov. Výhodou VLAN tagov je možnosť ich nastaviť na ľubovoľnú hodnotu bez ovplyvnenia funkcionality SDN siete. Vzhľadom k tomu, že VLAN tagy sieťové zariadenia používajú už dnes a sú podporované hardwarovo, použitie VLAN tagov nemá negatívny dopad na výkonnosť. Kontrolér si vytvorí tabuľku VLAN tagov s názvami skupín k nim priradených podobne, ako je zobrazené v tabuľke 1.

Tabuľka 1. Mapovanie VLAN tagov

VLAN tag	Názov skupiny
1	manažment
2	vývoj
3	služby

Pomocou VLAN tagu je možné definovať až 4096 používateľských skupín, avšak v prípade potreby je možné použiť aj hodnotu priorita VLAN alebo paket rozšíriť o MPLS hlavičku. Po rozšírení paketu je možné celkovo použiť až 2^{46} požívateľských skupín.

Pakety sa označujú vždy na prvom sieťovom prvku, ktorý pakety príjme. Všetky ostatné prvky vidiac nastavený VLAN tag už označovanie robiť nemusia. Označenie paketov umožňuje vytvárať konfiguráciu sieťových prvkov bez ohľadu na polohu zdroja paketov. Ďalšou výhodou je úspora počtu pravidiel na sieťových prvkoch. Namiesto vytvárania veľkého množstva pravidiel pre každné zariadenie, je vytvorené jedno pravidlo pre každú skupinu užívateľov.

4.3 Tvorba aplikácie

Po tom ako sú pakety označené VLAN tagom, je možné vytvoriť a nasadiť aplikáciu pre riadenie siete. Kontrolér Pyretic umožňuje vytváranie aplikácií podľa základných pravidiel typu *match-action*. Funkcia *match* obsahuje políčka paketu, ktoré musí paket obsahovať aby sa vykonala funkcia *action*. Súčasťou políčok paketu, ktoré funkcia *match* prehľadáva, môže byť aj názov skupiny do ktorej je používateľ priradený. Políčko názov skupiny sa deteguje podľa tagu VLAN.

Aby bolo možné vytvárať komplexnejšie politiky pomocou pravidiel typu *match-action*, je potrebné mať prostriedok na kombináciu týchto pravidiel. Pyretic definuje tri operátory:

1. sekvenčná kompozícia + (OR),
2. paralerná kompozícia >> (AND),
3. negácia ∼ (NOT).

Hlavnou úlohou aplikácií je abstrahovanie *match-action* pravidiel od administrátora siete. Abstrahovanie spočíva vo vytvorení niekoľkých konfiguráčných súborov, ktoré budú pri každej aktualizácii niektorého konfiguračného súboru automaticky prevedené na zoznamy *match-action* pravidiel.

Niekoľko vytvorených nezávislých aplikácií môže byť prostredníctvom Pyretic operátorov spojených do jednej veľkej aplikácie. Pyretic k spojeniu aplikácii využíva sekvenčný operátor >> a paralerný operátor +. V prípade sekvečného sa vykonáva nová množina pravidiel, ktorá vytvára dojem ako by sa vykonali pôvodné dve aplikácie sériovo za sebou. Pri paralernom operátore je vytvorená množina pravidiel reprezentujúca vykonanie viacerých aplikácií naraz. Príkladom kombinácie aplikácií môže byť: detekcia_identity >>firewall >> (smerovanie + monitoring).

5. Príklady aplikácie

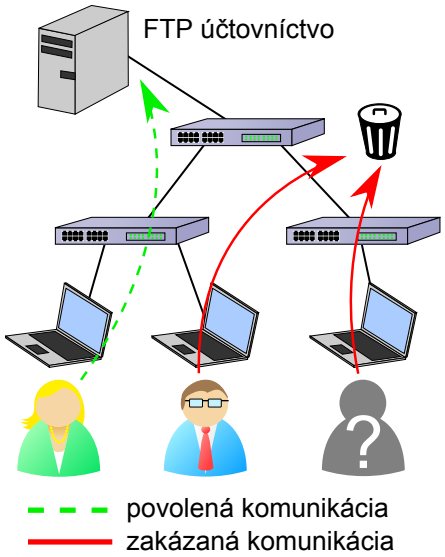
Pre otestovanie vytvorenej platformy boli vytvorené aplikácie zamerané na filtrovanie a smerovanie paketov. Cieľom aplikácií je ukázať možnosti správy siete pri použití siete SDN rozšírenej o znalosti identít. Príklady obsahujú konfiguračné súbory, ktoré poukazujú na jednoduchšiu správu konfigurácie siete. Obe aplikácie vyžadujú konfiguračný súbor priraďujúci používateľov do užívateľských skupín. Príklad takejto konfigurácie je zobrazený v tabuľke č. 2.

5.1 Filtrovanie paketov

Cieľom aplikácie je zabezpečiť prístup k zdrojom na sieti, aby k nim mohli pristupovať iba používatelia s dostatočným oprávnením tak, ako to zobrazuje obrázok č. 3. Konfigurácia aplikácie spočíva v definícií

Tabuľka 2. Definícia užívateľských skupín

Užívateľ	Skupina
Alica	manažment
Bob	vývoj
Cecilka	vývoj



Obrázok 3. Príklad aplikácie využívajucej identitu užívateľov pre filtrovanie prevádzky.

zdrojov na sieti a zoznamu skupín, ktoré k nim majú mať prístup. Zoznam zdrojov na sieti spoločne s ich parametrami (IP adresa, port, protokol) a zoznamom užívateľských skupín, ktoré majú mať k danému zdroju povolený prístup, aplikácia očakáva vo formáte zobrazenom v tabuľkách č. 3 a 4.

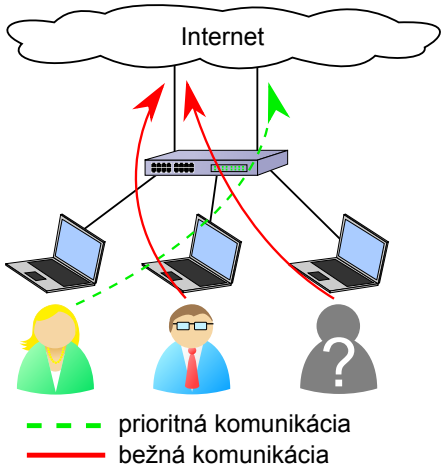
Tabuľka 3. Definícia zdrojov

Služba	Parametre
Web	192.168.1.1:80 (TCP)
FTP-účtovníctvo	192.168.1.2:210 (TCP)
FTP-projekty	192.168.1.2:21 (TCP)

Tabuľka 4. Definícia oprávnení ku zdrojom

Služba	Skupina
Web	*
FTP-účtovníctvo	manažment
FTP-projekty	vývoj

Aplikácia pre každý zdroj vyhľadá sieťový prvok do ktorého je daný zdroj zapojený a na ktorom vytvorí sadu pravidiel typu *match-action*. Tieto pravidlá budú podľa názvu skupiny (ktoré kontrolér SDN preloží na hodnoty VLAN ID) rozlyšovať, ktoré pakety sa prepošlú na zdroj a ktoré sa zahodia. Vytvorená sada sa skladá z dvoch častí:



Obrázok 4. Príklad aplikácie využívajucej identitu užívateľov pre smerovanie prevádzky.

1. **Povolenie prístupu:** Obsahuje pravidlo pre každú skupinu, ktorá má mať právo pristupovať k zdroju v tvare - match(group=názov skupiny) >> identity, kde identity reprezentuje povolenie komunikácie bez jej modifikácie.
2. **Zakázanie prístupu:** Všetka ostatná komunikácia je zakázaná prostredníctvom východzieho pravidla - drop, ktoré neobsahuje žiadny match() a teda je podmienka splnená vždy.

Ako príklad si zoberiem FTP server určený pre projekty. Aplikácia pre sieťový prvok do ktorého je daný FTP server zapojený vytvorí sadu pravidiel:match(group=”manažment”) >> identity + match(group= ”vývoj”) >> identity + drop.

5.2 Smerovanie paketov

Aplikácia slúži pre smerovanie paketov na základe odosielateľa paketu, vďaka čomu je možné využitie niektorých liniek obmedziť na vybrané skupiny používateľov. Obrázok č. 4 zobrazuje situáciu, kedy časť užívateľov využíva inú linku do Internetu ako zvyšný používatelia. Aplikácia je konfigurovaná prostredníctvom zoznamu liniek, názvu skupiny a podmienky určujúcej kedy daná skupina môže príslušnú linku využívať. Príklad konfigurácie je znázornený v tabuľke č. 5.

Tabuľka 5. Definícia liniek a podmienok použitia

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

Konfigurácia z tabuľky č. 5 odráža politiku, kedy linku s1-1 využíva manažment siete a linku s1-2 všetci ostatný používatelia. V prípade, že linka s1-1 vypadne, manažment siete začne využívať linku s1-2 spoločne s ostatnými používateľmi. Ak však vypadne linka s1-2, iba používatelia skupín manažment a vývoj začnú požívať linku s1-1. Ostatný používatelia nebudú využívať žiadnu linku (na linku s1-1 nemajú právo a s1-2 je nedostupná). Súčasťou konfigurácie aplikácie (v tabuľke nie je znázornené) je aj označenie niektorej linky, resp. liniek na sieti ako linky s prístupom na sieť 0.0.0.0/0 (východzia brána).

Aplikácia funguje na základe vytvorenia sieťovej topológie pre každú používateľskú skupinu. Podľa aktuálne dostupných liniek a pravidiel sú z danej topológie odstránené tie linky, pre ktoré príslušná skupina nemá oprávnenie používať alebo sú nedostupné. Pre vytvorie smerovacej topológie sa na takto vytvorenú topológiu použije Dijkstrov algoritmus [8]. Výslednú smerovaciu topológiu aplikácia prevedie na pravidlá typu *match-action*.

Z dôvodu úspory počtu vytvorených pravidiel je smerovacia topológia, ktorú využíva najviac používateľských skupín označená za východziu. Pre východziu topológiu je vytvorená iba jedna sada pravidiel, ktorá sa použije ak neexistuje špecifická topológia pre skupinu používateľov. Príklad pravidiel pre jeden sieťový prvok a jednu skupinu: match(group= vývoj,dstip= IPPrefix(’10.0.1.0/24’)) >> fwd(1) + match(group= vývoj,dstip=IPPrefix(’10.0.2.0/24’)) >> fwd(2) + fwd(3).

Problémom aplikácie je, že v prípade väčšieho množstva rôznych smerovacích topológií sa vytvorí veľké množstvo pravidiel. Ďalším nedostatkom aplikácie je absencia logických operátorov pri podmienkach použitia linky.

6. Vyhodnotenie

Cieľom článku je rozšírenie riadenia SDN sietí o znalosť identít zariadení. Takto rozšírené riadenie umožňuje administrátorovi vykonávať správu siete na základe identity používateľov používajúcich pripojené zariadenia. Článok popisuje riešenie pomocou prepojenia SDN kontroléru so systémom pre správu používateľských identít SIMS. Prepojenie bolo realizované prostredníctvom soketového TCP spojenia, ktoré vyvoláva aktualizáciu konfigurácie sieťových prvkov pri príjme udalosti od systému SIMS.

Implementácia počíta s použitím kontroléru Pyretic, ktorý bol rozšírení pre podporu prijímania externých udalostí. Kontrolér umožňuje rozdelenie sieťovej politiky na viacero menších častí, ktoré prostredníctvom operátorov kombinuje. Prvá časť politiky sa stará o označovanie paketov VLAN tagmi hraničnými

sieťovými prvkami. Pomocou VLAN tagu dokáže následne ľubovoľné sieťové zariadenie zistiť názov skupiny, do ktorej odosielateľ paketu patrí. Ďalšie časti sieťovej politiky predstavujú aplikácie pre správu siete, ktoré znalosť identity môžu ale aj nemusia používať.

Správa siete na základe identít umožnuje jednoduchšiu a pohodlnejšiu správu siete, ktorá zároveň znižuje riziko chybnej konfigurácie. Okrem implementácie ďaľších aplikácií by rozšírenie práce by mohlo spočívať v rozšírení možnosti nastavení politík, napr. na základe polohy zariadenia alebo aktuálneho času.

Poďakovanie

Chcel by som poďakovať môjmu vedúcemu Ing. Liboru Polčákovi za jeho pomoc.

Literatúra

[1] Hewlett-Packard. Identity driven management: technical brief. web (anglicky), 2015. http://www.hp.com/rnd/pdf_html/IDM_technical_brief.htm.

[2] Cisco. Cisco identity services engine. web (anglicky), 2015. http://www.cisco.com/c/en/us/products/security/identity-services-engine/.

[3] Juniper Networks. Identity and policy control. web (anglicky), 2015. http://www.juniper.net/us/en/products-services/ipc/.

[4] Vainius Dangovas and Feliksas Kuliesius. Sdn-driven authentication and access control system. In *DINWC2014*, pages 20–23. SDIWC, 2014.

[5] Libor Polčák, Tomáš Martínek, Radek Hranický, Stanislav Bárta, et al. Zákonné odposlechy v moderních sítích - shrnutí výsledků skupiny pro zákonné odposlechy projektu moderní prostředky pro boj s kybernetickou kriminalitou na internetu nové generace. Technical report, 2014.

[6] Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, et al. Openflow: enabling innovation in campus networks. *ACM SIGCOMM Computer Communication Review*, 38(2):69–74, 2008.

[7] Joshua Reich, Christopher Monsanto, Nate Foster, Jennifer Rexford, and David Walker. Modular sdn programming with pyretic. *Communications Magazine, IEEE*, 38(5):128–134, 2013.

[8] S Skiena. Dijkstra's algorithm. *Implementing Discrete Mathematics: Combinatorics and Graph Theory with Mathematica, Reading, MA: Addison-Wesley*, pages 225–227, 1990.