Monitorování a analýza síťového provozu

Bc. Andrej Filip

Diplomová práce
2022

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektroniky a měření

Akademický rok: 2021/2022

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Andrej Filip**
Osobní číslo:	**A20161**
Studijní program:	**N1032A020003 Bezpečnostní technologie, systémy a management**
Specializace:	**Bezpečnostní technologie**
Forma studia:	**Prezenční**
Téma práce:	**Monitorování a analýza síťového provozu**
Téma práce anglicky:	**Network Traffic Monitoring and Analysis**

Zásady pro vypracování

1. Seznamte se s principy monitorovacích systémů.
2. Proveďte analýzu dostupných řešení.
3. Porovnejte a zhodnoťte možnosti jednotlivých řešení.
4. Vybrané řešení aplikujte na sledování provozu v síti.
5. Vyhodnoťte výsledky zkušebního provozu.

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. WOLAND, Aaron T., Vivek SANTUKA, Jamie SANBOWER a Chad MITCHELL. *Integrated security technologies and solutions: Cisco security solutions for network access control, segmentation, context sharing, secure connectivity and virtualization*. Indianapolis: Cisco Press, [2019], xxi, 665 s. ISBN 9781587147074.
2. WOLAND, Aaron T., Vivek SANTUKA, Mason HARRIS a Jamie SANBOWER. *Integrated security technologies and solutions: Cisco security solutions for advanced threat protection with next generation firewall, intrusion prevention, AMP, and content security*. Indianapolis: Cisco Press, [2018], xxvi, 564 s. ISBN 9781587147067.
3. COLLINS, Michael. *Network security through data analysis: from data to action*. Second edition. Beijing: O'Reilly Media, 2017. ISBN 1491962844.
4. SANTOS, Omar. *Network security with NetFlow and IPFIX: big data analytics for information security*. Indianapolis: Cisco Press, [2016]. Cisco Press networking technology series. ISBN 1-58714-438-7.
5. GUPTA, Brij a Srivathsan SRINIVASAGOPALAN. *Handbook of research on intrusion detection systems*. Hershey, PA: IGI Global, an imprint of IGI Global, [2020]. ISBN 9781799822431.

Vedoucí diplomové práce: **Ing. Jiří Korbel, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce: **3. prosince 2021**
Termín odevzdání diplomové práce: **23. května 2022**

doc. Mgr. Milan Adámek, Ph.D. v.r.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

Ing. Milan Navrátil, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 7. února 2022

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 18. 4. 2022

Bc. Andrej Filip v.r.
podpis studenta

ABSTRAKT

Cieľom tejto práce je zhodnotiť možnosti v oblasti hĺbkového monitoringu počítačových sietí za účelom zvýšenia viditeľnosti a bezpečnosti siete. Teoretická časť opisuje spôsoby a princípy monitorovania počítačových sietí aj najčastejšie využívané protokoly z tejto oblasti. Praktická časť je zameraná na porovnanie dostupných komerčných riešení a ich funkcionalít, stručný opis firemnej počítačovej siete a funkčné požiadavky navrhovaného nástroja. Je popísaný postupu inštalácie navrhovaného nástroja a jeho základná konfigurácia. Sú tu taktiež uvedené vzorové nastavenia systému a jednotlivých modulov, ktoré boli žiadané zo strany firemného správcu siete. V závere praktickej časti sú uvedené zistené výsledky monitoringu z daného časového obdobia. Taktiež sú v tejto časti uvedené zistené bezpečnostne anomálie a sú hlbšie vysvetlené.

Kľúčové slová: monitoring, IP tok, počítačová sieť, kybernetická bezpečnosť, NetFlow, IPFIX, Flowmon

ABSTRACT

The aim of this work is to evaluate the possibilities in the field of deep monitoring of computer networks in order to increase the visibility and security of the network. In the theoretical part, the methods and principles of computer network monitoring are described. Also, the most commonly used protocols in this field are presented in this section. The practical part of the thesis is focused on the comparison of available commercial solutions and their functionalities. This part contains a brief description of the corporate network and the functional requirements of the selected tool that is being deployed in the corporate network. The next section describes the actual implementation procedure of the selected tool and its basic configuration. There are as well presented use case settings of system and modules which were required by company's network administrator. The practical part concludes with the monitoring results found during the given time period. Also, detected security anomalies are listed in this section and are explained in more depth.

Keywords: monitoring, IP flow, computer network, cybersecurity, NetFlow, IPFIX, Flowmon

POĎAKOVANIE

Rád by som sa poďakoval vedúcemu práce, pánovi Ing. Jiřímu Korbelovi Ph.D., za odborné vedenie, cenné rady, jeho čas a podporu v rámci navštevovania CISCO Akadémie. Moja veľká vďaka patrí taktiež Martinovi Ševčíkovi a Romanovi Čupkovi zo spoločnosti Flowmon Networks, za technickú podporu a pomoc pri spracovávaní praktickej časti tejto práce. Taktiež by som sa chcel poďakovať nemenovanej firme, za dôveru a možnosť spracovať túto tému v ich firemnej sieti.

Ďakujem aj profesorom a spolužiakom z FAI UTB za nezabudnuteľné zážitky počas štúdia. V neposlednom rade ďakujem svojej rodine za podporu a trpezlivosť, ktorú so mnou mali počas môjho štúdia.

OBSAH

ÚVOD

Nárast počtu uzlov v Internete priniesol so sebou aj nárast rizikových používateľov, ktorí sa snažia škodiť nelegálnou činnosťou (napr. útokmi na citlivé údaje). Rozširovaním Internet of Things (IoT), presunu technológii čoraz viac do prostredia cloud, alebo s používaním vlastných zariadení Bring Your Own Device (BYOD) sa výrazne mení pohľad na správu a monitorovanie sietí. S narastajúcim počtom aplikácií, ktoré pracujú v cloudovom prostredí, veľké percento sieťovej komunikácie prechádza z privátneho intranetu na verejný internet. Súčasne ako sa mení a vyvíja prostredie, vyvíjajú sa aj nové hrozby a typy útokov. V rokoch 2016-2017 bol zaznamenaný nárast IoT zariadení dostupných cez nezabezpečený prístup. Väčšina takýchto zariadení bola dostupná pomocou výrobcom prednastavených (default login password) prihlasovacích údajov (admin-admin). Táto zraniteľnosť bola veľmi rýchlo zneužitá na vytvorenie siete v službách útočníka (botnet). Pre zmienku stojí spomenúť aj malware Mirai, ktorý zneužil spomenutú zraniteľnosť na masívny útok Distributed Denial-of-Service (DDoS), kedy obeť útoku prijala necelých 1 TB komunikácie za sekundu.

Bývalý výkonný riaditeľ spoločnosti Cisco raz povedal: *„Sú len dva typy firiem. Tie, ktoré už boli napadnuté kybernetickým útokom, a tie, ktoré o tom ešte nevedia".* Potencionálne ciele útokov nie je tak komplikované nájsť. Dá sa na to využiť napr. online nástroj Shodan, ktorý skenuje verejne dostupné internetové adresy (IP) a protokoly (TCP, UDP). Dobíjanie sa do sietí je natoľko lukratívne pre útočníkov, že by sa dalo povedať, že ide o prácu na plný úväzok. Skupina zaoberajúca sa skúmaním kybernetickej bezpečnosti Cisco Talos pozoruje pravidelný vzor útokov počas pracovnej doby medzi 9.00-17.00 hod. Pre predstavu ransomware CryptoLocker vybral za prvé dva mesiace od vydania približne $27 miliónov na výkupnom (ransome) [1].

Monitorovanie sieťovej prevádzky poskytuje správcom sietí mnohé výhody. Ide predovšetkým o včasnú detekciu narušenia bezpečnosti siete a odhalenie prípadných skrytých anomálií. Monitoring taktiež poskytuje lepšiu viditeľnosť prevádzky siete, a tým umožňuje odhalenie prípadných problémov. Pre niektoré subjekty vyplýva povinnosť implementovať nástroj na monitorovanie siete priamo z legislatívy. Cieľom tejto diplomovej práce je poskytnúť čitateľovi v teoretickej časti informácie a technické možnosti z oblasti monitorovania počítačových sietí. V tejto časti sú uvedené a hlbšie popísané protokoly, ktoré sa najčastejšie využívané v oblasti monitoringu. Posledná kapitola teoretickej časti porovnáva funkcie troch navrhovaných riešení, ktoré poskytujú hĺbkový monitoring siete s využitím strojového učenia, behaviorálnych analýz a reputačných databáz. Firemná infraštruktúra je opísaná v prvej

kapitole praktickej časti. Následne je popísaná samotná implementácia a konfigurácia systému a prídavných modulov. Pri tomto procese sú do úvahy brané funkčne požiadavky správcu firemnej siete na monitorovací nástroj. Zahrnuté boli všetky požiadavky správcu firemnej siete na monitorovací nástroj. V závere praktickej časti sú interpretované výsledky za sledované časové obdobie. Sú taktiež demonštrované možnosti vizualizácie nazbieraných dát vo forme grafov, štatistík, reportov alebo prehľadových obrazoviek (dashboardov).

I. TEORETICKÁ ČASŤ

1 KYBERNETICKÁ BEZPEČNOSŤ

Táto kapitola sa zaoberá problematikou kybernetickej bezpečnosti. V prvej podkapitole sú uvedené najčastejšie kategórie útočníkov aj s príkladmi jednotlivých útokov. V druhej podkapitole sú vymedzené pojmy ako threat, vulnerability, risk alebo mitigation, v spojitosti s ochranou kybernetického priestoru.

1.1 Kategorizácia útočníkov

Za účelom zabezpečenia konkrétnej siete je nutné mať celkový nadhľad nad všetkými potencionálnymi hrozbami a určité technické povedomie o ich funkcionalite. Je potrebné vedieť, pred kým sa počítačová sieť zabezpečuje. Vo väčšine prípadov potencionálny útočník spadá do jednej z týchto kategórií:

Black-Hat hacker - termín "hacker" predstavuje osobu, ktorá zneužíva zraniteľnosti určitého systému alebo chyby programu v duchu objavovania alebo zvedavosti, čo nebýva až tak časté. Táto osoba alebo organizácia viacerých osôb vykonáva túto činnosť hlavne za účelom zisku, a to dokonca aj na objednávku. Pri tejto činnosti využívajú rôzne spôsoby ako napr. dostupne známe zraniteľnosti, sociálne inžinierstvo, útoky ako phishing alebo rootkity alebo trójske kone. Vo všeobecnosti je týmto termínom označená osoba, ktorá vykonáva škodlivú a nelegálnu činnosť v kybernetickom priestore.

Script kiddies - je to hanlivé označenie pre black-hat útočníka, ktorý používa voľne dostupné scripty alebo programy na útočenie. Je možné tvrdiť, že ide o neskúsenú osobu, ktorá nie je schopná si vytvoriť vlastné nástroje z dôvodu nedostatku skúsenosti alebo zručnosti. Takáto osoba využíva napr. jednoduchý Denial-of-Service (DoS) útok alebo Structured Query Language (SQL) injections.

Organizované kriminálne skupiny - tieto organizované skupiny sú si dobre vedomé, ako vysoké sú potencionálne zisky z takejto trestnej činnosti. Sú to veľmi dobre organizované skupiny, vybavené potrebnými technológiami a prostriedkami na útočenie. Celosvetovo známy príklad takejto skupiny je napr. Business Club, ktorý je zodpovedný za GameOver-Zeus malware.

Štátni aktéri - pravdepodobne najviac sofistikovaná skupina útočníkov. Útočníci sú financovaní vládou. Medzi ich hlavné aktivity patria cielené špionáže, útoky na konkrétne infraštruktúry alebo sledovanie osôb. Tieto aktivity sú vykonávané na podnet vlády daného štátu, za finančnú odmenu. Využívajú najnovšie a doposiaľ neodhalené sofistikovaný malware

(zero-day) alebo prepracované praktiky, v oblasti sociálneho inžinierstva. Dobrým príkladom útoku na fyzickú infraštruktúru na podnet štátnych orgánov je napr. malware Stuxnet.

Hacktivist – jedná sa o internetových aktivistov, alebo skupiny hackerov, ktorí svojími aktivitami chcú šíriť nejakú politickú propagandu. Ich činnosť je smerovaná na pritiahnutie pozornosti médií, a vo veľa prípadoch sa skupiny ku konkrétnym útokom aj samé prihlásia. Medzi najčastejšie praktiky tejto skupiny patrí DDoS útok a zverejňovanie údajov z databáz, emailovej komunikácie alebo utajovaných dokumentov. V súčasnej dobe najznámejšie skupiny hacktivistov sú Anonymous a LulzSec.

Cyber teroristi - ich primárny cieľ je vytvoriť pomocou svojich aktivít pocit nebezpečia v spoločnosti. Tieto skupiny bývajú často motivované politickými organizáciami alebo náboženskými názormi. Najčastejšie využívajú útoky mierené na Information Technology (IT) infraštruktúru, odcudzenie citlivých informácií, ako napr. osobné údaje štátnych zamestnancov, alebo zmenenie obsahu webových stránok za účelom určitej propagandy. Ich technická zručnosť pri útokoch sa môže pohybovať na úrovni script kiddies, až po veľmi skúsených black hat hackerov. Zo skúsenosti sa potvrdilo, že nie sú až tak sofistikovaní, ako štátmi podporovaní útočníci.

Vnútorné hrozby - sú útoky, ktoré pramenia z vnútra organizácie alebo nejakého celku. Často za takýmito útokmi stoja nespokojní zamestnanci, ktorí sa chcú pomstiť organizácií alebo jej nejako uškodiť. Môže ísť o súčasných, ale aj bývalých zamestnancov. Útočníci spadajúci do tejto kategórie nemusia byť veľmi skúsení v útočení na IT infraštruktúru alebo počítačovú sieť, nakoľko zneužívajú už získanú dôveru alebo prístupy do rôznych systémov. Príkladom môže byť napr. správca počítačovej siete, ktorý môže počas posledného pracovného dňa zmeniť konfiguráciu routrov alebo swtichov, a tým znefunkčniť celú sieť. Podobný príklad by sa dal aplikovať na správcu databázového systému, ktorý môže zmazať všetky záznamy popr. aj zálohy, a tým spôsobiť masívne škody pre danú organizáciu. Takéto vnútorné hrozby sú viac pravdepodobné ako tie vonkajšie a majú oveľa väčšie dopady v prípade ich vzniku.

Tento list potencionálnych útočníkov nie je kompletný, ale poskytuje obecný náhľad nad možnými hrozbami v kybernetickom priestore. Je nutné mať ale na pamäti, že útočníci a ich metódy sa nepretržite vyvíjajú v rýchlom tempe, a preto aj prostriedky na ochranu by mali byť adaptované aktuálnym hrozbám a používaným technikám.

1.2 Posúdenie aktív

Pri posudzovaní aktív, ktoré sa snažíme chrániť v kybernetickom prostredí je nutné definovať základne prvky analýzy, sú to:

- **threat (hrozba)** - je to osoba alebo nástroj, ktorý môže spôsobiť nejakú ujmu na stráženom aktíve. Do hrozieb spadajú jednotlivé kategórie útočníkov, ktoré boli rozobraté v predošlej časti tejto práce, ale taktiež sem patria aj nástroje ako vírusy, červy (worms) alebo iný malware. Všetko toto je možné klasifikovať ako potenciónálnu hrozbu v kybernetickom priestore.
- **vulnerability (zraniteľnosť) -** predstavuje to určitú slabosť alebo zraniteľnosť stráženého aktíva alebo systému, ktoré môže byť zneužité hrozbou. Dobrým príkladom zraniteľnosti môže byť absencia zabezpečenia koncovej stanice s heslom, čo vytvára príležitosť pre hrozbu získať prístup napr. k určitým dokumentom na zariadení.
- **risk** - potencionálna strata alebo ujma, ktorá vyplýva z hrozby v dôsledku zraniteľnosti. Napríklad, ak hrozba zapríčiní nefunkčnosť webového obchodu, tak risk predstavuje stratu tržby počas a po skončení takejto udalosti.
- **mitigation (opatrenie)** - sú to všetky opatrenia podniknuté za účelom redukovania pôsobenia rizika na strážené aktívum. Všetky opatrenia znižujú riziko a menia možné hrozby. Napríklad použitie hesla na zabezpečenie koncovej stanice predstavuje opatrenie voči riziku zneužitia zariadenia neoprávnenou osobou [1], [2].

2 MONITORING POČÍTAČOVÝCH SIETÍ

Na začiatku tejto kapitoly by bolo vhodné položiť si otázku, či je naozaj potrebné monitorovať určitú počítačovú sieť? Odpoveďou na túto otázku nemusí byť vždy áno, v prvom rade je dôležité posúdiť, o akú počítačovú sieť sa jedná. Ako príklad je možné použiť sieťovú komunikáciu v internetovej kaviarni. Monitorovanie takejto siete nie je potrebné, pokiaľ používatelia majú zabezpečený prístup do Internetu a koncové stanice sa vždy vo večerných hodinách preinštalujú pôvodnou verziou operačného systému. V ostatných prípadoch monitorovanie siete už je potrebné, a to hlavne z dôvodu efektívneho riadenia a spravovania siete, ochrany pred potencionálnymi hrozbami a anomáliami alebo dohľadanie napr. konfiguračných chyb, ktoré sa môžu vyskytnúť. Je preto nutné, aby bol zvolený vhodný nástroj, ktorý umožňuje hĺbkový monitoring celej siete.

V súčasnej dobe existuje široké spektrum nástrojov na monitorovanie napr. sieťového výkonu, dostupnosti jednotlivých zariadení ako sú switche alebo routre, monitorovanie aplikačného výkonu, kontrola vyťaženia jednotlivých hardwarových parametrov (Central Processing Unit - CPU, Random Access Memory - RAM) a pod.) a iné. Veľa dostupných nástrojov je distribuovaná pod General Public License (GPL) alebo Berkeley Software Distribution (BSD) licenciou, čo znamená, že sú voľne dostupné k používaniu aj v komerčnom prostredí a nie je nutná žiadna ďalšia licencia. Ostatné produkty sú komerčné a na ich dlhodobú funkčnosť je nutné zakúpenie licencie, v niektorých prípadoch aj hardware.

Existuje niekoľko možných techník a prístupov k monitorovaniu počítačových sieti. V tejto kapitole sú popísané jednotlivé princípy ktoré sa aktuálne využívajú v praxi. Taktiež sú v tejto kapitole uvedené protokoly, ktoré sa využívajú v oblasti monitorovania [3].

2.1 Princípy monitorovania

Spôsoby monitorovania predstavujú proces získavania informácií o danom zariadení. Ide o informácie o stave, v ktorom sa zariadenie nachádza, alebo štatistík týkajúcich sa využitia CPU alebo RAM a ďalšie. Existuje spôsob odosielania týchto inflácií s agentom, alebo bez agenta.

Variant **bez agenta** využíva štandardné protokoly na poskytovanie týchto informácii o sledovanom zariadení - Simple Network Management Protocol - SNMP, Windows Management Instrumentation - WMI alebo NetFlow. Tento spôsob monitoringu je veľmi jednoduchý a častokrát tieto protokoly sú povolené vo výrobných nastaveniach serverov alebo

zariadení. V prípade špeciálneho hardwaru ako napr. routre, switche alebo load balancere varianta monitorovania bez agenta predstavuje jedinú dostupnú možnosť.

Druhý variant je **s agentom**. V tomto prípade je na zariadenie nasadený program, ktorý zbiera jednotlivé informácie a následne ich odosiela do centrálneho monitorovacieho zariadenia. Tento variant zabezpečuje širokú škálu rôzných informácií o sledovanom zariadení a poskytuje zvýšenie flexibility.

Je samozrejmé, že každá metóda má svoje výhody a nevýhody, a preto je vhodné mať vytvorený prehľad o oboch možnostiach, pretože častokrát sa implementujú v kombinácií. Tieto dva spôsoby monitorovania poskytujú veľa výhod, ale aj nevýhod v rámci širokého spektra IT oblasti. Pred konečným rozhodnutím je nutné zváženie týchto bodov:

Bezpečnosť

- bez agenta - monitorovanie bez agentov zvyčajne vyžaduje iba jediné administratívne ID s globálnym prístupom na nepretržité zhromažďovanie údajov, ktoré môže vytvoriť slabé miesto v zabezpečení celého systému. Z tohoto dôvodu sa monitorovanie bez agentov zvyčajne neodporúča organizáciám, ktoré majú vyššie bezpečnostné požiadavky.
- s agentom - agenti, ktorí sú nainštalovaní jednotlivo, nemajú globálny prístup k sieti, čo znamená, že ak je kompromitovaný jeden z nich, nie je ohrozená celá sieť. Vďaka tomu je monitorovanie s agentov bezpečnejšie a lepšie pre prostredie s vysokými nárokmi na zabezpečenie.

Flexibilita

- bez agenta - monitorovacie systémy bez agentov sú zvyčajne jednoduché a menej rušivé ako systémy s agentom pre daný operačný systém, a preto poskytujú väčšiu flexibilitu. Okrem toho využívajú Application Programming Interface (API) a WMI čo znamená, že monitorovanie je nezávislé od poskytovateľa a možno ho použiť vo veľmi rôznorodých prostrediach IT.
- s agentom - aj keď sú moderné monitorovacie systémy založené na agentoch pomerne jednoduché, často stále využívajú niektoré systémové prostriedky nadmerným spôsobom na zariadeniach na ktorých sú nainštalované. Okrem toho, v závislosti od výrobcu, niektorí agenti nemusia fungovať so špecifickými zariadeniami alebo operačnými systémami.

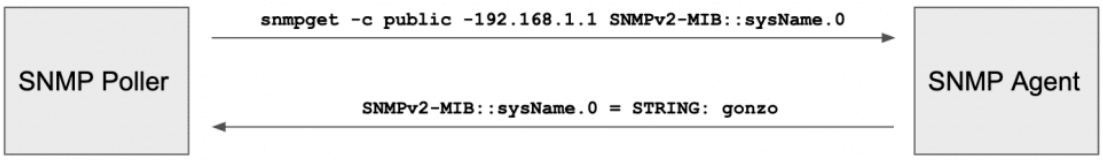
Získané dáta

- bez agenta - monitorovanie bez agentov funguje dobre pre niektoré systémy, ale nedisponuje niektorými hĺbkovými metódami na získavanie určitých typov informácií. Je možné tvrdiť, že dáta získané monitoringom bez agenta nie sú častokrát tak robustné a hĺbkové ako tie získane pomocou nástrojov, ktoré využívajú agentov.
- s agentom - monitorovanie s agentom je možné získať podrobné údaje, ktoré sú oveľa bohatšie, ako poskytuje monitorovanie bez agentov. Špeciálne aplikácie ktoré je nutné monitorovať sú obvykle ľahšie monitorované pomocou agentov kvôli hlbším dátovým možnostiam [4].

2.1.1 SNMP monitoring

SNMP je protokol využívaný na získavanie informácii zo zariadení ako switch, router alebo server o aktuálnom stave vyťaženosti CPU, operačnej pamäti, aktuálnom stave sieťových rozhraní alebo počet prijatých a odoslaných bytov daného rozhrania. Tento protokol ale nie je schopný zobraziť štruktúru sieťovej komunikácie a neumožňuje hĺbkový pohľad do komunikácie jednotlivých používateľov a hľadanie potencionálnych anomálii v sieťovej komunikácií. Pokiaľ nastane situácia, že monitorovaný prvok je nedostupný, alebo jeho hardwarové zdroje sú preťažené, monitorovací nástroj generuje upozornenie, a tým informuje administrátora o tomto probléme.

Do tejto kategórie spadá veľa dostupných riešení, medzi najznámejší open source (voľne dostupné na používanie a zdieľanie) nástroj je považovaný Nagios, z komerčných je vhodné spomenúť napr. riešenie SolarWinds alebo IBM Tivoli. Hlavné rozdiely v jednotlivých riešeniach sú vo funkcionalite, a taktiež v maximálnom počte spravovaných uzlov.



Obr. 1 - Princíp komunikácie SNMP protokolu [5]

Druh informácií, ktoré možno získať z konkrétneho sieťového zariadenia, sa líši v závislosti od výrobcu daného zariadenia a modelu. Každý výrobca sieťových zariadení publikuje súbor Management Information Base (MIB). MIB popisujú konkrétne informácie alebo zdroje,

ktoré je možné dopytovať zo sledovaného zariadenia (SNMP agent). Väčšina riešení SNMP umožňuje import súborov MIB za účelom integrácie s konkrétnym zariadením určitého výrobcu.

- **výhody** - vhodné na monitorovanie sieťových zariadení ako routre, switche a taktiež serverov
- **nevýhody** - tento spôsob sa nevyužíva na overenie funkčnosti a výkonnosti danej siete [6], [7]

2.1.2 Full packet inspection - hĺbková kontrola packetov

Tento prístup je založený na kontrole obsahu packetov. Ide o zachytenie a spracovanie všetkých dát z packetov, t. j. nielen metadát o sieťovej komunikácií. Tento prístup poskytuje veľmi dobrú viditeľnosť sieťovej komunikácie, ale má vysoké požiadavky na ukladanie a spracovávanie takýchto dát. Tento spôsob monitoringu je implementovaný veľmi zriedkavo, a to hlavne z dôvodov vysokých nákladov na obstaranie takéhoto systému. Ako príklad je vhodné uviesť, že pri sledovaní siete s priemernou rýchlosťou 250 Mb/s je dátové zaťaženie približne 31 MB za sekundu, 1,8 (Gigabyte) GB za minútu, 108 GB za hodinu a 2,6 Terabyte (TB) za deň. V prípade sietí s rýchlosťou 10 Gb/s sa tieto čísla môžu pohybovať okolo 100 TB uložených dát za deň. Je nutné poznamenať, že vysoký objem ukladaných dát nie je jediná nevýhoda tohoto spôsobu monitorovania. Ďalším obmedzením pre full packet inspection je šifrovaná sieťová komunikácia. Bez šifrovacieho kľúča nie je možné vidieť obsah jednotlivých správ, dokonca ani typ použitého protokolu alebo aplikácie. V súčasnej dobe objem šifrovanej komunikácie neustále rastie, napr. pre Spojené Štáty Americké percento šifrovanej komunikácie je 92 %, pre Rusku Federáciu 85 %, Japonsko 80 % alebo pre Indonéziu 74 % [8].

Aj napriek nevýhodám takéhoto spôsobu monitorovania, full packet inspection má svoje miesto v každodennej rutine správcov sietí. V prípade zistenia problému v sieti je komunikácia zachytená a následne je manuálne analyzovaná v nástroji ako je napr. Wireshark. Takýmto spôsobom je možné zistiť veľké množstvo informácií o sieti, ale aj zachytiť veľa problémov, ktoré môžu byť ľahko identifikované, s vysokou presnosťou. Tento spôsob ale spolieha hlavne na znalosti a skúsenosti správcov, ktorí musia mať obstojne technické znalosti v oblasti sieťových protokolov a princípov fungovania sieťových služieb.

Aktuálne veľa monitorovacích riešení využíva tzv. hybridný princíp, kedy sa využíva prioritne monitorovanie jednotlivých flows komunikácie (podrobnejšie je toto riešenie opísané

v ďalšej podkapitole). V prípade potreby je možné zaznamenávať všetky packety prechádzané sieťou a následne ich analyzovať. Obvykle je možné nastaviť určité pravidlá, kedy ma byť zapnuty full packet capture.

Je vhodné taktiež definovať, čo je packet. Packet je základná jednotka pre dáta v sieťovej komunikácii. Packet je zložený z hlavičky packetu (packet header), s riadiacimi informáciami a payloadom, čo predstavuje používateľské dáta. Sú známe dve kategórie nástrojov, ktoré umožňujú zachytiť a analyzovať packety. Prvú kategóriu nástrojov je možné ovládať iba pomocou príkazového riadku (napr. tcpdump). Druhá skupina nástroj už disponuje grafickým rozhraním a poskytuje pohodlnejšie ovládanie (napr. Wireshark) [9], [10].

2.1.3 Monitoring na základe flows

Tento spôsob monitorovania na rozdiel od hĺbkovej kontroly packetov nespracúva jednotlivý payload (payload označuje konkrétne dáta prenášane v packete) správ. Analyzuje hlavičky jednotlivých paketov a vytvára z nich flows na základe spoločných atribútov. Na nižšie priloženom obrázku je možné vidieť príklad zobrazenia flows pomocou nástroja nfdump.

Terminal File Edit View Search Terminal Help

```
$ nfdump -R /var/cache/nfdump/
Date first seen          Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Packets    Bytes Flows
2019-10-01 18:51:06.726     0.013 TCP    193.190.205.209:443   ->     192.168.0.14:42438        3      187     1
2019-10-01 18:51:06.726     0.002 TCP       192.168.0.14:42438 ->  193.190.205.209:443          2      104     1
2019-10-01 18:51:15.843     0.000 UDP     192.168.0.100:5353  ->      224.0.0.251:5353          1      155     1
2019-10-01 18:51:08.044     7.730 UDP       192.168.0.14:5353  ->      224.0.0.251:5353          2      162     1
2019-10-01 18:51:30.381     6.389 TCP       192.168.0.14:42504 ->  193.190.205.209:443          20     6279    1
2019-10-01 18:51:30.392     6.389 TCP    193.190.205.209:443   ->     192.168.0.14:42504        21     7486    1
2019-10-01 18:51:49.061     0.043 TCP     192.168.0.100:6690  ->     192.168.0.14:59660        31     9971    1
2019-10-01 18:51:49.059     0.045 TCP       192.168.0.14:59660 ->    192.168.0.100:6690        17     5497    1
2019-10-01 18:51:45.465     7.238 TCP       192.168.0.14:38968 ->       10.67.1.60:3128        4      240     1
2019-10-01 18:51:49.659     3.001 UDP       192.168.0.14:59044 ->  239.255.255.250:1900        4      800     1
2019-10-01 18:51:32.223    24.580 TCP       192.168.0.14:38112 ->    67.202.110.12:443         3      120     1
2019-10-01 18:51:55.528     3.031 TCP       192.168.0.14:38992 ->       10.67.1.60:3128        3      180     1
2019-10-01 18:51:32.327    24.576 TCP     67.202.110.12:443   ->     192.168.0.14:38112        4      206     1
2019-10-01 18:52:01.399     6.168 TCP    193.190.205.209:443   ->     192.168.0.14:42574        22     7538    1
2019-10-01 18:52:01.391     6.166 TCP       192.168.0.14:42574 ->  193.190.205.209:443          19     6227    1
2019-10-01 18:51:19.919    62.567 UDP       192.168.0.14:45062 ->     109.88.203.3:53           3      186     1
2019-10-01 18:51:19.935    62.568 UDP       109.88.203.3:53    ->     192.168.0.14:45062        3      618     1
2019-10-01 18:51:19.919    62.567 UDP       192.168.0.14:45062 ->   62.197.111.140:53           3      186     1
2019-10-01 18:51:19.919    62.567 UDP       192.168.0.14:45062 ->          8.8.8.8:53           3      186     1
2019-10-01 18:51:19.939    62.564 UDP            8.8.8.8:53    ->     192.168.0.14:45062        3      282     1
2019-10-01 18:51:54.333    28.169 UDP     62.197.111.140:53    ->     192.168.0.14:45062        2      412     1
2019-10-01 18:51:28.128    60.395 TCP       192.168.0.14:47118 ->     54.154.86.41:443          13     556     1
2019-10-01 18:52:28.442     0.000 UDP       192.168.0.14:46582 ->  239.255.255.250:1900        1      154     1
2019-10-01 18:51:28.162    60.361 TCP       54.154.86.41:443   ->     192.168.0.14:47118        12     887     1
2019-10-01 18:52:31.383     8.121 TCP       192.168.0.14:42636 ->  193.190.205.209:443          20     7115    1
```

Obr. 2 - príklad spracovania flows pomocou nástroja nfdump [11]

Tento spôsob monitorovania prináša niekoľko výhod ako napr. zníženie objemu ukladaných dát a zvýšenie súkromia používateľov. Pri procese ukladania jednotlivých flows je potrebné, aby bola zabezpečená možnosť ukladať dáta, ktoré prechádzajú jednotlivými sieťovými zariadeniami. Aby bolo toto možne je potrebné zabezpečiť uniformnosť informácií vo flows tak, aby ich bolo možné odosielať z rôznych sieťových prvkov a následne ich ukladať na

ukladacie zariadenia. Za týmto účelom bolo vytvorených niekoľko typov protokolov, ktoré sú popísané v 3. kapitole [12], [13].

2.2 Kvalitatívne parametre sietí

V sieťach s prepínaním packetov je monitorovanie založené na sledovaní hlavných atribútov, a to rýchlosť siete a výkonnosť siete.

Z pohľadu výkonnosti siete je možné sledovať nasledovné parametre:

- bandwidth (šírka pásma) - určuje množstvo bitov, ktoré je možne preniesť daným médium za jednotku času (bit/s)
- throughput - (priepustnosť) - hovorí o množstve úspešne prenesených dát medzi jednotlivými uzlami za jednotku času
- utilization (využitie) - predstavuje aktuálne využívanú časť z bandwidthu (udávaná v %)
- latency - delay (oneskorenie) - je to čas, ktorý je potrebný pre správu aby bola doručená do svojho cieľa
- response time (doba odozvy) - je to čas, ktorý uplynie medzi začiatkom a ukončením daného požiadavku
- packet loss (strata packet) - nastane vtedy, keď jeden alebo viacero packetov, ktoré sú prenášané cez počítačovú sieť, nedorazí do cieľa, môže to byť spôsobená chybami pri prenose dát alebo preťažením siete

Rýchlosť siete je charakterizovaná dvoma atribútmi:

- modulačná rýchlosť - predstavuje počet zmien signálov za sekundu, nehovorí o rýchlosti prenosu, meria sa v jednotkách Baud (Bd)
- prenosová rýchlosť - určuje maximálny počet množstvo dát, ktoré môže byť prenesených za jednu sekundu, udávaná je v bitoch za sekundu (bps, kbps) [9], [14]

2.3 Aktívny a pasívny monitoring

Aktívne monitorovanie (nazývané aj syntetické monitorovanie) simuluje správanie používateľa s cieľom určiť potenciálny výkon siete. Aktívny monitoring výkonu sa nezameriava na skúmanie skutočných používateľov a ich dát, ale namiesto toho simuluje, ako sa skutoční používatelia správajú v sieti. Táto emulácia prebieha v reálnom čase, v nastavených intervaloch, čo znamená, že monitorovací nástroj vždy analyzuje simulované dáta.

Hlavnou výhodou aktívneho monitorovania je schopnosť udržiavať úplnú viditeľnosť v sieti. Aj keď aktívny monitoring nemeria reálne toky komunikácie, umožňujú zobrazenie potencionálnych problémových oblasti skôr, ako môžu ovplyvniť užívateľov. Vďaka analýze v reálnom čase je možné okamžite eliminovať slepé miesta získaním informácií o výkonnosti konkrétnych častí siete. Nástroje aktívneho monitoringu využívajú proaktívny prístup k odstraňovaniu problémov v sieti tým, že upozorňujú na potenciálne problémové oblasti ešte pred negatívnym dopadom na koncového užívateľa.

Tento spôsob monitorovania siete taktiež pomáha pri určovaní výkonnosti novo implementovaného hardwaru v sieti. Veľa aktívnych monitorovacích nástrojov je možné nakonfigurovať tak, aby bolo možné presne definovať časť siete, ktorú je potrebné sledovať. Následne je možné napr. vidieť, ako nové pripojenia ovplyvňujú výkon siete, a či sa niekde na trase nenachládajú tzv. bottlenecks ("úzke hrdlá" predstavujú stav, kedy dátový tok je oneskorený v dôsledku obmedzenia kapacity šírky pásma - bandwidth). Je potrebné eliminovať takéto bottlenecks ešte pred tým, ako majú negatívny dopad na koncového používateľa.

Keďže aktívny monitoring je výlučne založený na prediktívnych dátach, nie vždy poskytuje 100 % presné informácie o výkonnosti siete. Je vhodný hlavne na analyzovanie jednej určitej a konkrétnej metriky (napr. odozva siete alebo packet loss) ale nie je schopný zahrnúť každý aspekt siete naraz. Tento spôsob monitoringu je taktiež veľmi náročný na zdroje z dôvodu vytvárania dát v reálnom čase a ich následnej analýze.

Aktívny monitoring sa zaoberá nasledujúcimi metrikami siete:

- bandwidth
- packet delay
- packet loss
- throughput
- dostupnosť zariadení

Medzi hlavné výhody aktívneho monitoringu patri:

- proaktívna detekcia a najlepší spôsob odstraňovania problémov koncových používateľov
- detekcia degradácie kvality siete
- stále monitorovanie (24/7)
- dokáže uchovávať veľké množstvo historických údajov
- nevyžaduje reálnu komunikáciu používateľov na generovanie Key Performance Indicators (KPIs)
- testovanie sieťovej infraštruktúry vo fáze pred nasadením
- overenie zmien v konfigurácií

Ako nevýhody je vhodné spomenúť:

- pri vykonávaní skutočného dátového prenosu tieto nástroje konzumujú značné sieťové a aplikačné zdroje
- aby aktívny monitoring mohol byť úspešne implementovaný, musí byť v sieti nasadených niekoľko hardvérových alebo softvérových agentov
- náročný na zdroje

Pasívny monitoring zhromažďuje aktuálne užívateľské dáta a analyzuje ich v rámci určitého časového intervalu. Monitorovací nástroj skúma výsledky analýzy dát a následne ich prezentuje užívateľovi monitorovacieho nástroja. Na rozdiel od aktívneho monitorovania pasívny monitoring nevkladá umelo testovacie dáta do siete za účelom sledovania správania jednotlivých užívateľov siete. Namiesto toho sa využívajú pri monitorovaní skutočné údaje, prenesené dáta od užívateľov z konkrétnych bodov v sieti.

Pasívny monitoring je schopný zhromažďovať a generovať veľké množstvo dát, ktoré popisujú výkonnosť danej siete. Tieto dáta poskytujú holistický pohľad na výkonnosť siete a sú pokryté široké spektrá sledovaných metrík. Keďže pasívny monitoring zhromažďuje skutočné dáta, tieto systémy informujú o problémoch, ktoré priamo ovplyvňujú užívateľov siete. Upozorňujú na problémy, s ktorými sa aktuálne užívatelia potýkajú, a preto je potrebné včasnú reakciu na tento stav. V porovnaní s aktívnym monitoringom, pasívny monitoring nepredstavuje až takú záťaž na sieťové zariadenia.

Niektoré spoločnosti poskytujú len čisto pasívny monitoring alebo len aktívny. Je samozrejmé, že je prínosne využiť taký nástroj, ktorý kombinuje oba tieto spôsoby do jedného

riešenia. Každý z vyššie spomenutých spôsobov monitorovania je dôležitý. Aktívny monitoring generuje prediktívne dáta, ktoré sa využívajú pri upozornení, v prípade zistenia problému naprieč celou sledovanou sieťou. Pasívny monitoring dopĺňa pohľad na sieť z perspektívy koncového používateľa pomocou údajov o skutočnom výkone. Využitím kombinácie týchto dvoch prístupov je zabezpečený hĺbkový pohľad na celú monitorovanú sieť, čo napomáha administrátorom robiť rýchle a účinné rozhodnutia v prípade vzniknutých problémov.

Medzi hlavné výhody je možné zaradiť:

- možnosť identifikovať užívateľov alebo aplikácie v sieti, ktoré spotrebúvajú vysoké percento bandwidthu siete
- je to menej náročný monitoring na hardwarové a sieťové zdroje
- získava skutočné užívateľské dáta z konkrétnych bodov v sieti
- poskytuje ucelený pohľad na výkonnosť siete pomocou rôznych metrík

Ako nevýhody je vhodné spomenúť napr.:

- pasívny monitoring zvyčajne analyzuje tok dát, ktoré prechádzajú cez špeciálne zariadenia, a preto je potrebný špecializovaný hardvér
- nástroje pasívneho monitorovania musia byť neustále aktualizované, aby zohľadňovali meniaci sa charakter služieb

V nižšie priloženej tabuľke je možné vidieť porovnanie a oblasti použitia týchto dvoch spôsobov monitoringu [15], [16].

Tab. 1 - porovnanie aktívny a pasívny monitoring [15]

Aktívny monitoring	**Pasívny monitoring**
Prediktívny prístup, ktorý simuluje skutočné správanie používateľov	Analyzuje skutočné údaje používateľov
Úplný prehľad o výkone sledovanej siete	Meria výkonnosť v danom čase
Generuje komplexnú analýzu, zvyčajne pre jednu metriku.	Generuje veľké množstvo údajov pre holistický pohľad na rôzne metriky
Zameranie na kvalitu služieb Quality of Service (QoS)	Vhodné na sledovanie hĺbkovej komunikácie a analýzu protokolov, najmä po incidente
Vhodné pre údaje v reálnom čase, ako je strata packetov, latencia atď.	Zamerané na Quality of Experience (QoE)

3 VYUŽÍVANÉ PROTOKOLY

V tejto kapitole sú rozobraté najčastejšie používane protokoly v oblasti monitoringu počítačových sieti, a to konkrétne protokol SNMP a NetFlow. V jednotlivých podkapitolách sú popísané princípy fungovania týchto protokolov, a taktiež aj rozdiely v jednotlivých dostupných verziách týchto protokolov.

3.1 SNMP

Ako už bolo uvedené v tejto práci, protokol SNMP sa využíva na monitorovanie a správu sieťových zariadení predovšetkým v Local Area Network (LAN). Ide o protokol, ktorý pracuje na aplikačnej vrstve modelu TCP/IP. Umožňuje štandardizovaným spôsobom zhromažďovať informácie o zariadeniach pripojených k sieti v rámci širokého množstva výrobcov a typov produktov.

Architektúra SNMP je založená na princípu klient-server a skladá sa z týchto častí:

- **SNMP manager** - je to softvérová platforma, ktorá funguje ako centralizovaná konzola, do ktorej sú agentmi posielané informácie. Agenti sú aktívne žiadaní managerom o zasielanie aktualizácií v pravidelných intervaloch. Rozsah získaných informácií závisí vo veľkej miere od toho, ako je daný monitorovací nástroj bohatý na funkcie.
- **SNMP agent** - ide o softvér, ktorý je spustený na monitorovanom hardwari alebo službe a zhromažďuje údaje o diskovom priestore, využívaní šírky pásma a ďalších dôležitých ukazovateľoch výkonu siete. Ak nastane dopyt na určité informácie zo strany SNMP managera, agent odošle tieto informácie do monitorovacieho nástroja. Agent je schopný proaktívne upozorniť na výskyt chyby v kontrolovanom zariadení.
- **MIB** - je to databáza vo forme textového súboru (.mib), ktorý obsahuje všetky objekty konkrétneho zariadenia, ktoré je možné vyhľadávať alebo ovládať pomocou protokolu SNMP. Každej položke MIB je priradený Object Identifier (OID).

SNMP manager vystupuje ako klient, SNMP agent ako server a MIB ako servera databáza. Keď manager SNMP odošle dopyt na nejakú otázku agentovi, agent použije MIB na poskytnutie odpovede. Tento protokol je natoľko populárny, že väčšina sieťových zariadení je dodávaná už s predinštalovanými SNMP agentmi. Je nutné vykonať zmenu v predvolených nastaveniach agenta, aby bola zabezpečená komunikácia s lokálnym monitorovacím systémom. Protokol SNMP je súčasťou pôvodného IP balíku, ktorý bol konkrétne definovaný

organizáciou The Internet Engineering Task Force (IETF). V súčasnej dobe existuje viacero verzií protokolu SNMP. Najnovšia verzia, SNMPv3, obsahuje bezpečnostné mechanizmy na autentifikáciu, šifrovanie a riadenie prístupu.

3.1.1 Princíp fungovania SNMP

Monitorovaná sieť má zvyčajne aspoň jeden počítač alebo server s monitorovacím nástrojom. Predstavuje to riadiaci subjekt. Sieť má s vysokou pravdepodobnosťou viacero zariadení, ktoré je potrebné monitorovať, sú to napr.: routre, switche, pracovné stanice, tlačiarne alebo čokoľvek iné. Tieto všetky zariadenia predstavujú spravované zariadenia. Správy SNMP sú posielané a prijímané medzi SNMP managerom a SNMP agentom. Zvyčajne je SNMP manager v sieti nainštalovaný na riadiacom subjekte a agenti SNMP sú nainštalovaní na riadených zariadeniach.

Prenos správ v SNMP protokole je možné prirovnať ku komunikácii, ktorá je založená na modeli klient-server, ktorá vychádza z pull a push technológie. Pull (alebo poll) technológia, pri ktorej klient (napr. monitorovací nástroj na správu siete v riadiacom subjekte), vyšle požiadavku na vyžiadanie odpovede od servera alebo riadeného zariadenia. Druhá časť komunikácie predstavuje push technológiu, ktorá inštruuje riadené zariadenie ku odoslaniu SNMP odpovede na riadiace zariadenie. V terminológii SNMP sa napríklad požiadavka GET od SNMP managera riadi modelom pull, zatiaľ čo SNMP trap spáva je "vytlačená" agentom SNMP (napr. routrom) bez predchádzajúcej požiadavky.

Obr. 3 - princíp protokolu SNM [17]

Sú známe tieto typy SNMP správ:

- GetRequest - ide o najbežnejšiu správu, ktorú odosiela SNMP manager za účelom vyžiadania údajov z monitorovaného zariadenia.
- GetNextRequest - takéto správy môžu byť odoslané od SNMP managera za účelom zistenia všetkých dostupných informácií z monitorovaného zariadenia. Začínajúc od OID 0 je SNMP manager schopný pokračovať v odosielaní požiadaviek na ďalšie dostupné údaje zo zariadenia. Týmto spôsobom používatelia sú schopní zistiť všetky dostupné údaje o určitom zariadení, aj keď nemajú žiadne predchádzajúce znalosti o odpovedajúcom systéme alebo zariadení.
- GetBulkRequest - predstavuje to novšiu, optimalizovanú verziu funkcie GetNextRequest, ktorá bola pridaná vo verzii SNMP v2. Vyžiadaná odpoveď obsahuje toľko údajov, koľko povoľuje požiadavka. V podstate ide o spôsob ako je možné vykonať niekoľko GetNextRequests správ naraz, čo umožňuje používateľom vytvoriť zoznam všetkých dostupných údajov a parametrov o sledovanom zariadení.
- SetRequest - tento príkaz je iniciovaný managerom za účelom nastavenia alebo zmeny hodnoty parametrov prostredníctvom protokolu SNMP na zariadení, kde je spustený SNMP agent. Tento typ správ je využívaný pri správe alebo aktualizácií konfiguračných nastavení, alebo iných parametrov. Je potrebné dbať na pozornosť pri tomto type správ pretože nesprávny SetRequest môže vážne poškodiť systémovú konfiguráciu alebo sieťové nastavenia.
- Response - je to správa, ktorú SNMP agent odošle na základe požiadavky managera. Keď je odoslaná táto správa ako odpoveď na správu typu GetRequest, packet obsahuje požadované údaje alebo hodnoty. Pokiaľ ide o správu typu SetRequest, packet odpovedá novo nastavenými hodnotami ako potvrdenie, že SetRequest bol úspešne uskutočnený.
- Trap(v2) - SNMP agent odošle ("vytlačí") SNMP trap správu bez toho, aby bola vyžiadaná zo strany managera. Trap správy sú posielané na základe určených podmienok, napr. v prípade výskytu určitej chyby alebo po prekročení vopred stanovených hraničných hodnôt. Ak používateľ chce využiť výhody trap správ v oblasti monitorovania, je potrebné takéto správy najskôr nakonfigurovať pomocou SNMP managera.

- InformRequest - tento typ správy bol pridaný v SNMP v2 aby bol manager schopný potvrdiť, že bola prijatá trap správa od agenta. Niektorí agenti sú nakonfigurovaní tak, aby pokračovali v odosielaní trap správy pokiaľ nie je prijatá potvrdzujúca správa.
- Report - na použitie tejto správy je potrebná SNMP v3. Umožňuje SNMP manažérovi určiť, aký druh problému bol zistený vzdialeným SNMP agentom. Na základe zistenej chyby je protokol SNMP schopný odoslať opravenú SNMP správu. Ak to nie je možné, tento typ správy je schopný odoslať informáciu o chybe aplikácii, z ktorej bola inicializovaná neúspešná požiadavka SNMP [18].

3.1.2 OID a MIB

OID jednoznačne identifikuje spravované objekty, ktoré sú definované v súboroch MIB. Ako príklad je možné spomenúť napr. tlačiareň v ktorej sú sledované jednotlivé stavy kaziet s farbou alebo počet vytlačených strán. V prípade routra sú typickými objektmi záujmu prichádzajúca a odchádzajúca komunikácia, miera straty packetov alebo počet packetov, ktoré sú adresované na broadcastovú adresu. Hierarchia OID objektov sa zvyčajne zobrazuje ako strom s rožnými úrovňami. Každý OID má adresu, ktorá nasleduje po úrovniach stromu OID. Príklad štruktúry OID je možné vidieť nižšie:

```
Iso(1).org(3).dod(6).internet(1).private(4).transition(868).pro-
ducts(2).chassis(4)
.card(1).slotCps(2)-cpsSlotSummary(1).cpsModuleTable(1).cpsModuleEn-
try(1)
.cpsModuleModel(3).3562.3
```

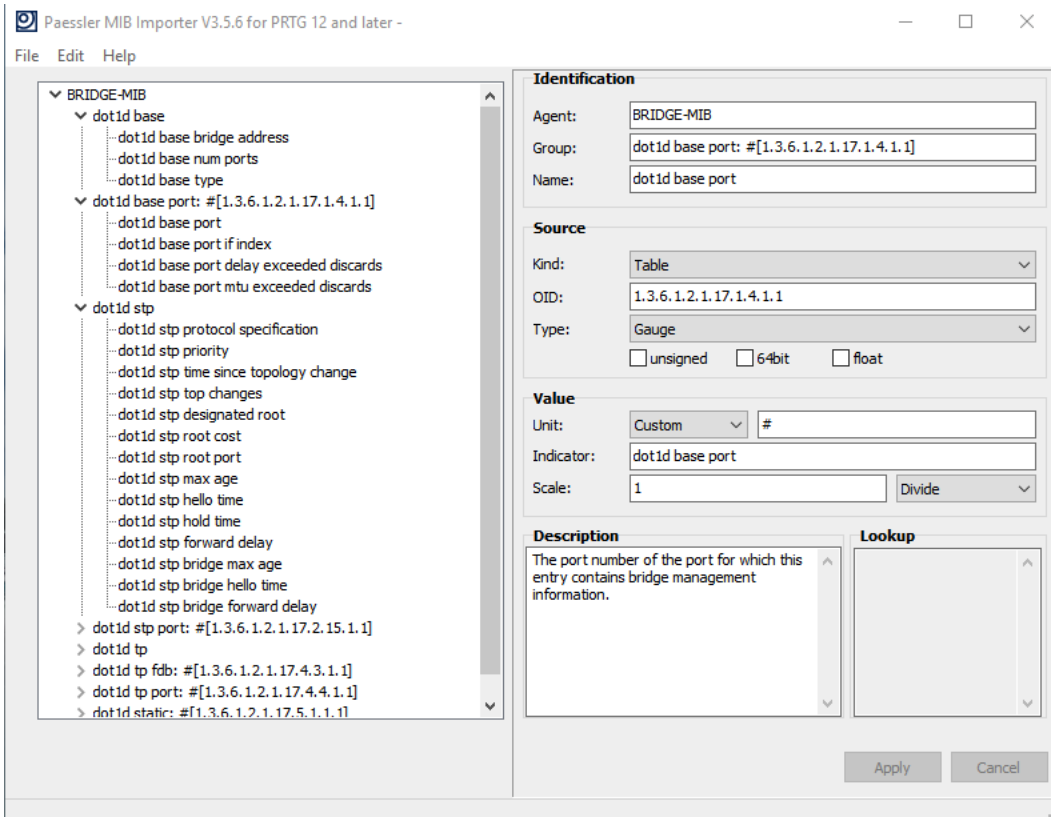
Táto štruktúra môže byť zapísaná aj ako:

```
1.3.6.1.4.868.2.4.1.2.1.1.1.3.3562.3
```

ID objektov najvyššej úrovne a všeobecných objektov MIB sú prideľované rôznymi štandardizačnými organizáciami, ako napríklad International Organization for Standardization (ISO). Dodávateľmi sú definované OID pre svoje vlastné produkty v súkromných vetvách stromu OID.

MIB označuje nezávislý formát na definovanie informácií na monitorovanom zariadení. V MIB sú popísané jednotlivé parametre, ktoré sú predmetom sledovania v danom zariadení. K týmto údajom sa následne pristupuje pomocou protokolu SNMP. Aby bola zabezpečená úspešná komunikácia v sieti medzi monitorovaným zariadením a monitorovacím nástrojom musia oba subjekty vedieť, aké OID sú dostupné. To je dôvod, prečo existujú MIB databáze a prečo sú vyžadované správcami siete. Každá hodnota, ktorú je potrebné monitorovať na

zariadení musí byť zahrnutá v MIB databáze. Je potrebné zaistiť, aby všetky potrebné MIB databázy boli uložené na SNMP agentoch, ako aj v SNMP managerovi (monitorovací nástroj). Výrobcovia zariadení zvyčajne dodávajú potrebné súbory MIB spolu so svojimi produktmi, ktoré podporujú protokol SNMP. V závislosti od použitého monitorovacieho riešenia môže byť niekedy nutné konvertovať MIB na inú podporovaná verziu daného zariadenia [19], [20], [21].



Obr. 4 - MBI importér pre PRTG monitorovací nástroj [18]

3.2 NetFlow

Flow je charakterizovaný ako jednosmerná sekvencia packetov, ktoré majú určité spoločné vlastnosti a prechádzajú cez sieťové zariadenie. Každý flow je identifikovateľný na základe týchto hodnôt:

- zdrojová IP adresa
- cieľová IP adresa
- IP protokol
- zdrojový port
- cieľový port

Je možné tvrdiť, že v jednotlivých flows nie sú žiadne informácie o paylode packetov. Protokol NetFlow zaznamenáva pre každý flow dobu jeho vzniku, dĺžku trvania, počet prenesených packetov, bajtov a ďalšie údaje. Je vhodný na použitie aj v multi gigabitových sieťach. Každý flow je tvorený ako agregácia sieťovej komunikácie, ktorá obsahuje informácie z L3 a L4 vrstvy modelu Open Systems Interconnection (OSI). Protokol NetFlow sa "pozrie" do hlavičky paketu a vytvorí záznam o dátovom toku. Táto technológia je jednosmerná, čo znamená, že akonáhle server odosiela odpoveď na užívateľovu požiadavku, je vytvorený ďalší záznam o tejto komunikácii. Následne packety s rovnakými atribútmi aktualizujú predchádzajúce flows (napr. trvanie komunikácie alebo počet prenesených bajtov). Akonáhle je komunikácia ukončená, jednotlivé flows sú odoslané na collector, kde sú tieto dáta uložené a spracované za účelom ďalšej vizualizácie.

Pri využívaní flows k monitoringu sa predchádza ukladaniu veľkého množstva dát z prevádzky siete, tým je tento spôsob menej náročný na hardwarové vybavenie a úložné zariadenia. Zároveň všetky potrebné informácie ktoré sú potrebné na ďalšie analyzovanie sieťovej komunikácie sú vo flows uchované. Informácie o obsahu jednotlivých správ z paylodu nie sú uchovávané, a tým pádom nie je možné identifikovať konkrétny obsah komunikácie používateľov.

Spoločnosť Cisco počas posledných rokov predstavila viacero verzií protokolu NetFlow. Postupom času aj iní výrobcovia začali vytvárať svoje verzie protokolu NetFlow a v súčasnej dobe sú známe viaceré využívané verzie tohoto protokolu. V nižšie priloženej tabuľke sú popísané hlavné rozdiely jednotlivých protokolov. Je nutné ale podotknúť, že tabuľka obsahuje iba súčasné, najviac používané a rozšírené verzie protokolu. Verzie ako NetFlow v1 alebo NetFlow v7 nie sú uvedené z dôvodu, že sú už veľmi zastaralé, alebo už nie sú podporované.

Tab. 2 - verzie protokolu NetFlow [13]

NetFlow v5	Originálny Cisco štandard na monitorovanie flows, ktorý je podporovaný veľkým množstvom routrov a switchov. Má fixovaný formát a atribúty sú špecializované na informácie z L3 a L4 vrstvy modelu OSI. Za hlavnú nevýhodu sa dá považovať absencia podpory IPv6 a Virtual Local Area Network (VLAN). Tento formát je podporovaný vo veľkom množstve monitorovacích nástrojoch a aplikáciách.

NetFlow v9	Táto verzia je založená na tzv. šablónach a je možné flexibilne nastaviť aké konkrétne informácie zo sieťovej komunikácie majú byť sledované. Rieši absenciu podpory IPv6 z predošlej verzie, a taktiež umožňuje monitorovať informácie z L2 modelu OSI ako napr. Media Access Control (MAC) adresy alebo VLAN tagy. Bližšie je tento protokol popísaný v Request for Comments (RFC) 3954. Je Cisco proprietárny.
NetFlow v10 (IPFIX)	Je to nezávislý medzinárodný štandard, ktorý umožňuje výrobcom monitorovacích nástrojov, ktorý využívajú technológiu flow definovať vlastné nadstavby protokolov. Je založený na predošlej verzií NetFlow v9, ale už nie je proprietárny. Vďaka tomuto je možné exportovať do flow v podstate akékoľvek informácie z L2 až L7 modelu OSI. Táto technológia prináša unikátny pohľad do sieťovej komunikácie bez potreby full packet inspection. Je popísaný v RFC 7011, RFC 7015 a RFC 5103. Je predpokladané, že Internet Protocol Flow Information Export (IPFIX) nahradí pôvodný NetFlow protokol v plnej miere v blízkej budúcnosti.
jFlow	Je to štandard firmy Juniper na monitorovanie flows, je dostupný vo verzii v5 a v9. Hlavný rozdiel v porovnaní s NetFlow je ten, že timestamp jednotlivých flows sú uchované počas celého sieťového prenosu, čo si vyžaduje iný prístup pri spracovaní flows na strane collectoru. Tento štandard je kompatibilný s NetFlow.
NetStream	Štandard firmy Huawei na monitorovanie flows dostupný vo verzii v5 a v9. Tento štandard je kompatibilný s NetFlow.
sFlow	Je to priemyselný štandard na monitorovanie vysokorýchlostných prepínaných sietí. Na rozdiel od NetFlow táto technológia nepracuje s konceptom flow catche a agregáciou metadát z paketov do flows. Vzorové hlavičky packetov sú zakódované do formátu podobného NetFlow a exportované do collectora. V dôsledku vysokej vzorkovacej frekvencii (zvyčajne 1:1000) tieto dáta nie sú presné na využitie v troubleshootingu, alebo pri detekcie anomálii v sieti. Tento protokol je podporovaný v širokom spektre podnikových sieťových zariadení.

[13], [22], [23]

3.2.1 Technické riešenie

Protokol NetFlow bol prvýkrát predstavený spoločnosťou Cisco v roku 1996, ktorý umožňuje zaznamenávať sieťovú komunikáciu ktorá vstupuje, alebo opúšťa konkrétne sieťové rozhranie. Na základe týchto dát správca je schopný určiť zdroj a cieľ komunikácie typ služby alebo príčiny nedostupnosti určitých služieb. Obvyklý monitorovací nástroj využívajúci protokol Netflow sa skladá z týchto častí:

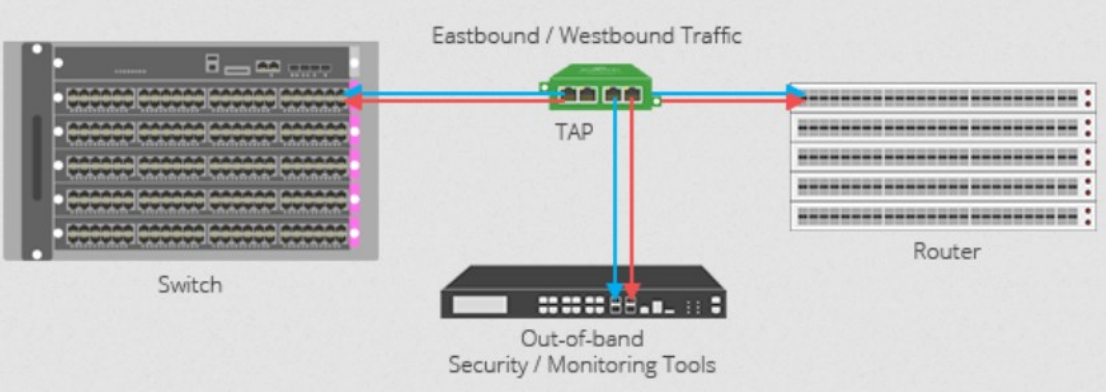
Exportér jednotlivých flows - hlavnou úlohou exportéra je agregovať pakety do jednotlivých flows a následne ich posielať na jeden, alebo viacero collectorov. Exportér pridelí unikátnu časovú otlačku (timestamp) a extrahuje dôležité časti z hlavičky packetu. Je veľmi dôležité vhodne nastaviť exportér na základe požiadaviek konkrétnej sledovanej siete. Existujú dva dôležité parametre, ktoré ovplyvňujú vytváranie a exportovanie zachytených flows, sú to:

- **active timeout** - je to časový limit, ktorý ak uplynie, a packety stále prechádzajú cez záchytne zariadenie, exportér výmaze flow z pamäte cache a vyexportuje tento flow do collectora
- **inactive timeout** - je to časový limit, ktorý ak uplynie a záchytne zariadenie medzičasom neprijalo žiadne nové packety, ktoré by patrili do daného flow, tak sa vymaže flow z pamäte cache a exportuje sa do collectora

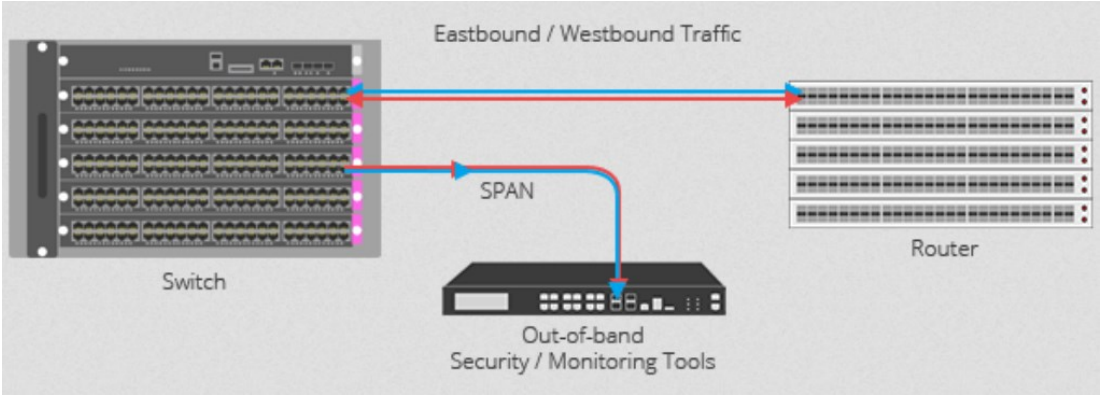
V súčasnej dobe sú známe dva hlavné typy exportérov, a to:

- **exportér ako súčasť sieťového zariadenia** - sú to zariadenie, ktorých hlavnou úlohou nie je exportovanie flows za účelom monitoringu. Ich primárna funkcia spočíva napr. v smerovaní komunikácie - routre.
- **sieťové sondy** - routre a switche nie je možné považovať ako vhodné zariadenia na zachytávanie sieťovej komunikácie a vytváranie flows, pretože ich primárna funkcia je iná. Za týmto účelom sú vytvárané jednoúčelové zariadenia, ktoré zabezpečujú výlučne spracovávanie komunikácie - sieťové sondy. Tieto sondy sú umiestnené na vstupnom, alebo výstupnom bode sledovanej siete, alebo na kritických bodoch siete. Sondy môžu byť pripojené pomocou Switch Port Analyzer (SPAN) portu (rozhranie, na ktorý je odzrkadlená všetka komunikácia siete), alebo pomocou Test Access Point (TAP) zariadenia (špeciálne hardwarové zariadenie, ktoré je umiestnené medzi switchom a routrom, ktoré sprístupňuje zrkadlenie komunikácie). Využívanie TAP alebo

SPAN zapojenia ma niekoľko výhod. Monitorovacie zariadenie je účinne skryté na sieťovej a spojovacej vrstve modelu OSI pred potencionálnymi útočníkmi. Na dvoch nižšie priložených obrázkoch je možné vidieť schématické zapojenie oboch spôsobov.



Obr. 5 - zapojenie pomocou TAP zariadenia [24]



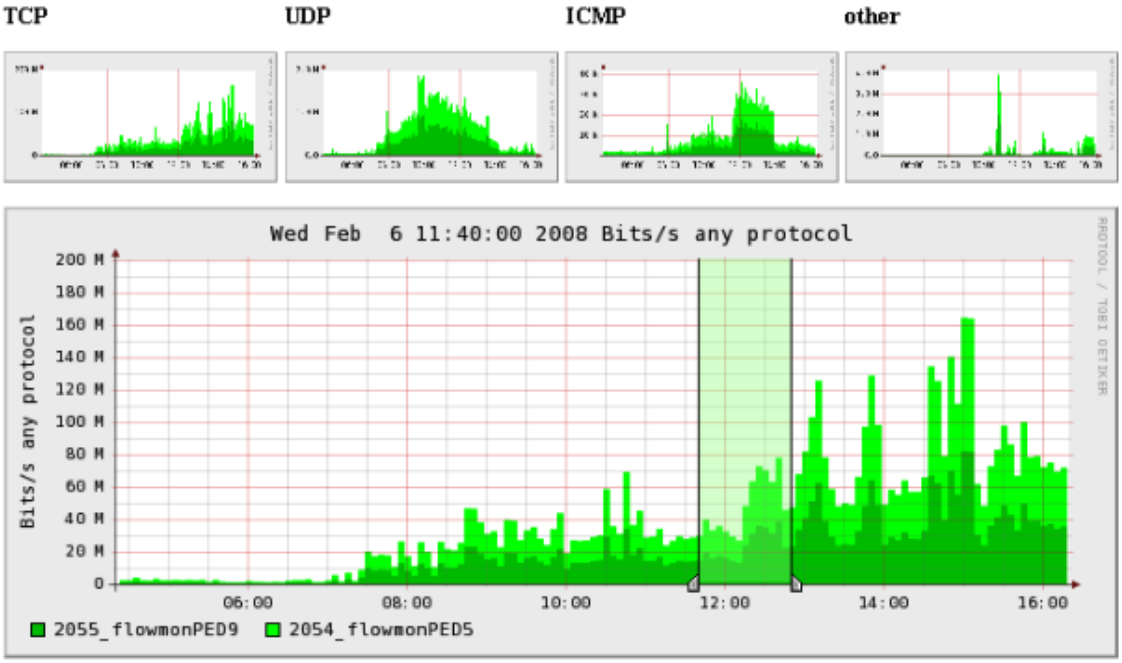
Obr. 6 - zapojenie pomocou SPAN portu [24]

Hlavnou úlohou monitorovacieho nástroja je schopnosť obsiahnuť celú snímanú sieť alebo aspoň jej kritické časti. V praxi je bežné, že sú častokrát stavané monitorovacie systémy na zariadeniach, ktoré nie sú primárne na to určené. Je odporúčané, aby monitorovací systém bol vybudovaný vyhradené jednoúčelovo, tak aby bol schopný poskytovať dostatočný výkon a neovplyvňoval iné komponenty siete. Jednotlivé požiadavky na takýto systém sa odvíjajú od rozsahu monitorovanej siete a počtu užívateľov a iných faktorov.

Flow úložisko - collector - zodpovedá za prijatie, ukladanie a predpracovanie jednotlivých prijatých flows z exportéra, spôsob ukladania sa môže líšiť v závislosti od collectora, ale obvykle sú dáta ukladané do štandardných databáz (napr. MySQL). Odhadovaný objem NetFlow dát z vyťaženej 100 Mb/s siete za jednu hodinu predstavuje približne 300 MB a približne 600 MB pri priemerne vyťaženej 1 Gb/s sieti. Collector by mal disponovať

dostatočným objemom úložného miesta aby bolo možné ukladať flows na potrebné časové obdobie (týždeň, mesiac alebo rok). Dáta, ktoré sú ukladané na collectore, sú analyzované nástrojom ako napr. nfdump, alebo nástrojmi, ktoré podporujú užívateľsky pohodlnejšie prostredie pomocou Graphical User Interface (GUI).

Vyhodnocujúca aplikácia - analyzuje prijaté flows a profiluje komunikáciu za účelom odhalenia možného narušenia bezpečnosti. Takéto systémy umožňujú vytváranie rožných pohľadov, grafov alebo zobrazovať informácie o užívateľoch. Jeden z možných príkladov využitia takejto aplikácie je identifikovanie užívateľa v sieti, ktorý nadmerne vyťažuje sieť odosielaním dát z lokálnej siete do Internetu. Ako prvé je zvolený časový úsek, ktorý je predmetom analýzy (Obr 7.) Následne je zvolená agregácia flows na základe zdrojovej IP adresy a počtu prenesených bytov. Obr. 8 zobrazuje tabuľku používateľov, ktorí počas nadviazaných spojení preniesli najväčší objem dát v danom časovom rozmedzí.



Obr. 7 - objem komunikácie v časovom horizonte [25]

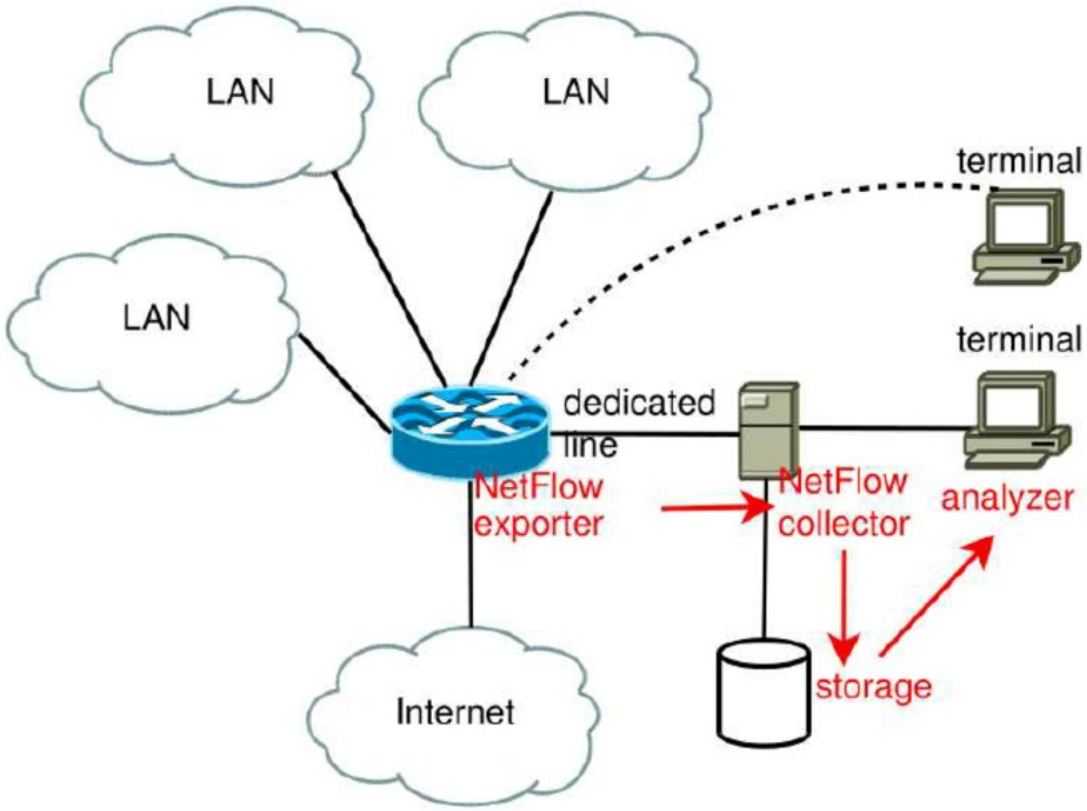
```
Top 10 Src IP Addr ordered by bytes:
Date first seen          Duration Proto      Src IP Addr    Flows  Packets    Bytes      pps      bps   bpp
2008-02-06 05:49:41.984   334.976 any    121.201.189.240      953     6064    6.4 M       18   159998  1104
2008-02-06 05:49:58.512   297.457 any      142.241.112.8       77     1850    2.1 M        6    59766  1201
2008-02-06 05:50:09.069   299.911 any      51.20.192.101       10     8148   350643       27     9353    43
2008-02-06 05:50:07.102   235.578 any       172.58.120.1       93      881   319750        3    10858   362
2008-02-06 05:50:00.831   291.591 any      204.145.193.9       39      422   235179        1     6452   557
2008-02-06 05:52:34.667    58.697 any       205.191.73.7       10      142   151929        2    20706  1069
2008-02-06 05:52:34.999    53.128 any      205.191.78.32        4      114   136503        2    20554  1197
2008-02-06 05:52:26.652    62.278 any      205.191.76.89        6      120   113490        1    14578   945
2008-02-06 05:52:35.758    48.410 any      205.191.72.51       51      381   112531        7    18596   295
2008-02-06 05:50:14.209   274.068 any      204.69.181.16        9     2470   106226        9     3100    43

IP address anonymized
Summary: total flows: 3240, total bytes: 10.9 M, total packets: 29113, avg bps: 272216, avg pps: 86, avg bpp
Time window: 2008-02-06 05:49:41 - 2008-02-06 05:55:16
```

Obr. 8 - prehľad užívateľov s najväčším objemom komunikácie [25]

Protokol Netflow je aktuálne považovaný za najviac využívaný štandard pre získavanie štatistík o dátovej prevádzke siete. Jednotlivé flows sú generované špeciálnymi sieťovými zariadeniami ako sú routre a switche, ale taktiež aj hardwarovými alebo virtuálnymi sondami (probes). Tieto sondy sú implementované v sledovanej sieti ako pasívne zariadenia, ktorých úlohou je vytvárať flows z kópie sieťovej komunikácie. Tento prístup s použitím hardwarovej alebo virtuálnej sondy sa používa na prekonanie hardwarových obmedzení a funkcií routra, v prípade ak by jeho výkon nebol dostačujúci na smerovanie packetov a aj generovanie flows [23], [25].

Na nižšie priloženom obrázku je možno vidieť architektúru zaznamenávania flows pomocou protokolu NetFlow



Obr. 9 - architektúra protokolu NetFlow [22]

4 DOSTUPNÉ MONITOROVACIE RIEŠENIA

Táto kapitola sa zaoberá popisom jednotlivých vybraných nástrojov na monitorovanie a bezpečnosť siete. Riešenia, ktoré sú nižšie rozobraté poskytujú hĺbkovú viditeľnosť v sieti, čo znamená, že nesledujú len či je napr. daný prvok v sieti dostupný (pomocou napr. ping echo request a reply), alebo ako moc je na danom sieťovom zariadení aktuálne vyťažené CPU. Skúmajú celkovú komunikáciu a sledujú prípadne anomálie správania jednotlivých staníc za využitia behaviorálnych analýz, čo napomáha v detekcii bezpečnostných problémov. Súčasťou jednotlivých podkapitol je aj krátka história firiem a prehľad aktuálne dostupných technických riešení. Aktuálne je na trhu veľké množstvo obdobných nástrojov. Hlavným dôvodom výberu monitorovacích nástrojov pochádzajúcich z Českej republiky bol nezáujem zahraničných dodávateľov konkurenčných produktov o poskytnutie Proof of Concept (PoC) a ďalších technických informácií.

4.1 GreyCortex

Firma GreyCortex bola založená v roku 2009 v Brně, dvoma študentmi, popri ich doktorandskom štúdiu na Vysokém učení technickém. Spoločnosť sa zaoberá výskumom sieťovej prevádzky a analýzou malwaru. Ich produkt Mendel, je nástroj, ktorý využíva umelú inteligenciu a strojové učenie na identifikáciu počítačových hrozieb a útokov. Softvér poskytuje podrobnú viditeľnosť sieťovej prevádzky pre forenznú a obranu proti rôzným poškodeniam infraštruktúry.

Mendel monitoruje a analyzuje sieťovú prevádzku, pomáha odhaľovať známe aj neznáme hrozby vrátane únikov dát, anomálie v prevádzke, škodlivé aktivity užívateľov a ďalšie ťažko odhaliteľné hrozby. K analýze sieťovej komunikácie je využívaná odzrkadlená komunikácia zo SPAN portu alebo TAP zariadenia (najčastejší model implementácie). Pri spracuvávaní údajov nástroj Mendel prioritne využíva vlastný protokol Advanced Security Network Metrics (ASNM), a to hlavne z dôvodu nevyhovujúcich vlastností agregácie dát v protokolu IPFIX. Je samozrejmé, že sú podporované aj iné formy vstupných dát. Využitie vlastného protokolu umožňuje hĺbkovú viditeľnosť do dát, ktoré prechádzajú sieťou. V porovnaní s riešeniami založenými len na protokole NetFlow spracúva MENDEL oveľa väčšie objemy údajov, čo je predpokladom spoľahlivého strojového učenia v oblasti detekcie anomálii. Tento nástroj preto dokáže rozlíšiť štandardnú sieťovú komunikáciu od potenciálnej, alebo priamo škodlivej komunikácie. Nástroj pracuje na princípe zachytávania všetkých packetov, ktoré prechádzajú sieťou - Deep Packet Inspection (DPI). DPI hĺbkovo skúma

kompletný rozsah údajov a metadát spojených s jednotlivými packetmi. Pri DPI nie sú skúmané len informácie z hlavičky packetu (ako napr. zdrojová / cieľová IP adresa, číslo portu), ale aj jednotlivý obsah z payload packetu. Všetky údaje o komunikácií sú komprimované za účelom zníženia nárokov na ukladanie a následne indexované v databáze, čím je zabezpečená rýchla odozva na požiadavky [26], [27]

4.1.1 Popis funkcionality

Ako už bolo uvedené, GreyCortex Mendel je nástroj na analýzu sieťovej prevádzky, monitorovanie výkonnosti a hrozieb, a teda predstavuje riešenie pre hĺbkovú viditeľnosť siete, hlavne pre podniky, verejnú správu a kritickú infraštruktúru. Na nižšie priloženom obrázku je možné vidieť štruktúru tohoto nástroja aj s popisom jednotlivých častí.

Obr. 10 - štrukúra nástroja Mendel [26]

Vstupy (inputs) predstavujú všetky zdroje, s ktorými nástroj Mendel pracuje pri vyhodnocovaní bezpečnostných hrozieb a anomálií v sieti. Konkrétne sú to:

Sieťové dáta

- odzrkadlená komunikácia (pomocou TAP zariadenia, SPAN portu alebo iného spôsobu zrkadlenia portu)
- z iných zariadení Mendel (senzor alebo collector)
- podpora L2-L4 vrstvy TCP/IP modelu zahrnujúc podporu IPv6 protokolov
- protokoly založené na flows (Netflow - IPFIX)

Bezpečnostná inteligencia

- rôzne zdroje IDS signatúr (napr. súbor pravidiel Emerging Threat alebo Proofprint)
- ostatné relevantné databázy (IP reputácia, doménová reputácia, GEO IP, WHOIS, ...)

- databáza škodlivých súborov (napr. ESET Threat Intelligence)
- definícia udalosti podľa Mitre ATT&CK Enterprise a Mitre ATT&CK ICS rámcov

Znalosť siete

- definícia funkčných sieťových segmentov - podsietí, ktoré majú rovnaké vzory správania, napr. oddelenie managementu, obchodu alebo servery, WiFi sieť, tlačiarne a pod.
- spojenie IP s názvom hostiteľa (pomocou Domain Name System - DNS záznamov)

Znalosť užívateľov

- spojenie IP adresy s doménou pomocou logov z doménových kontrolérov - Lightweight Directory Access Protocol (LDAP)

Po vstupných dátach nasleduje **spracovanie a analyzovanie komunikácie**, čo obsahuje:

Analýza sieťového chovania - Network Behavior Analysis (NBA)

- analýza sieťovej komunikácie na základe flows prostredníctvom strojového učenia
- možnosti detekcie konkrétnej aktivity malwaru (šírenie, sťahovanie malwaru alebo spamovanie)
- detekcia aktivít útočníka (skenovanie, brute-force, exploitácia)
- detekcia Command & Controll (boti, rootkity, červy a pod.)

Detekcia na základe signatúr - Signature-Based Detection

- monitorovanie interakcií s internou sieťou alebo v rámci internej siete
- detekčné signatúry pre známy malware, útoky a iné aktivity
- niekoľkých rôznych zdrojov databáz známych signatúr
- detekcia škodlivých súborov pomocou hashovania
- detekcia komunikácie s hostiteľom, ktorý sa nachádza na nejakom blackliste
- možnosť pridať užívateľsky definované signatúry - pravidlá podľa potreby

Poslednou súčasťou analyzovania komunikácie predstavuje monitorovanie výkonu - Performance Monitoring, zhŕňa to:

- analyzovanie výkonu siete a aplikácií pomocou flows

- poskytuje všeobecný prehľad o aplikáciách využívaných v sieti
- sledovanie aktuálnej a priemernej šírky pásma
- monitorovanie metrík, ktoré hovoria o výkonu danej aplikácie (odozva, roud trip time, user experience)
- automatická detekcia na základe zistení anomálií v aplikáciách

Posledným krokom je **prezentácia získaných a analyzovaných dát** vo forme výstupov a reportov a prípadná ďalšia integrácia so sieťovými zariadeniami alebo systémami. Patrí sem:

GUI

- webové užívateľské rozhranie podporované širokou škálou webových prehliadačov založené na Jave
- umožňuje vytváranie prispôsobiteľných dashboardov
- ponúka rýchle a široké možnosti filtrovania
- užívateľ ma dostupnú kontextovú nápovedu a užívateľskú dokumentáciu

Reporty a notifikácie

- reporty sú generované na základe definovaných podmienok
- formáty výstupov sú vhodné pre koncového užívateľa - odoslanie priamo cez e-mail vo forme Portable Document Format (PDF)

Integrácia

- podporované Security Information and Event Management (SIEM) formáty sú CEF (Common Event Format), LEEF (Long Extended Event Format) alebo Syslog
- možnosť exportovať zachytené flows vo formáte IPFIX
- integrácia s firewallmi (MikroTik, Juniper, FortiGate, Palo Alto, Checkpoint)
- možnosť doplniť identitu užívateľa pomocou Active Directory alebo Cisco ISE
- výstupný formát je možné prispôsobiť

4.1.2 Možnosti implementácie

Riešenie od firmy GreyCortex sa skladá z týchto komponentov, ktoré sú aktuálne dostupné:

Senzor (sonda) - je dostupná v prevedení Hardware (HW) alebo Virtual Appliance (VA), je možné ju nasadiť do siete s priepustnosťou až 100 Gbps. Senzor v hardvérovom prevedení môže mať až 8x 1 Gbit/s rozhraní, 4x 10 Gbit/s rozhraní alebo 2x 100 Gbit/s. V režime virtualizácie alebo nasadenia v cloude je možné komunikáciu spracovať až v rýchlosti 4 Gbit/s.

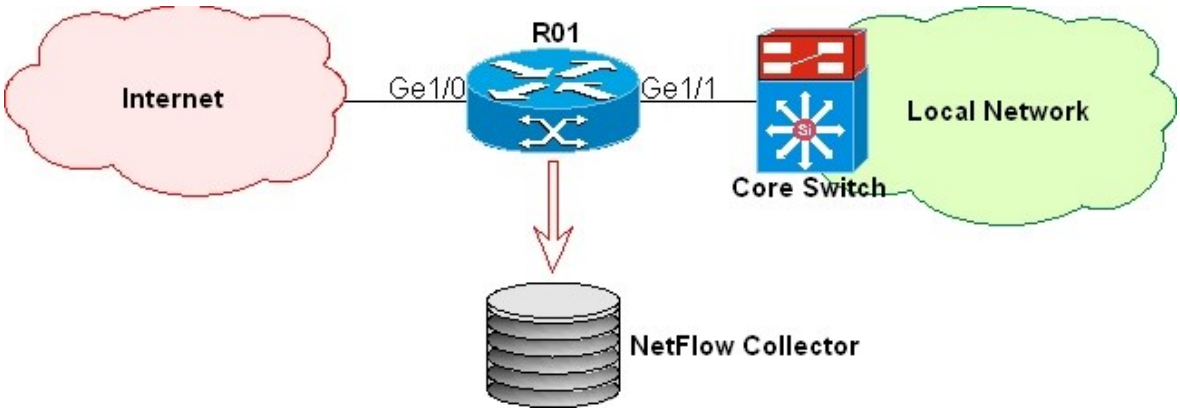
Collector - je taktiež dostupný v prevedení HW alebo VA. HW prevedenie ponúka monitorovanie 40 a viac senzorov na jeden collector, až 50 000 monitorovaných sieťových uzlov a historické dáta dostupné od mesiaca až po niekoľko rokov. VA spoločne s nasadením v cloud je schopné pripojiť 20 senzorov na jeden collector. Collector disponuje úložiskom s viacerými oddielmi s podporou rýchlych diskov Solid-State Drive (SSD).

All-in-One riešenie - predstavuje spojenie senzora a collectoru do jedného zariadenia, ktoré je dostupné v prevedení HW alebo VA. All-in-One riešenie ponúka monitorovanie siete s priepustnosťou až 100 Gbps, môže obsahovať 8x 1 Gbit/s rozhranie, 4x 10 Gbit/s alebo 2x 100 Gbit/s rozhranie. Podporuje pripojenie až 20-tich ďalších senzorov na jedno All-in-One zariadenie a až 50 000 monitorovaných sieťových uzlov. Taktiež toto zariadenie podporuje viacej diskových oddielov a rýchle disky [26].

4.2 Caligare

Caligare s.r.o je súkromná spoločnosť založená v roku 2004 v Prahe. Spoločnosť je zameraná na vývoj softvérových nástrojov v oblasti monitoringu počítačových sietí. Tieto produkty sú zamerané na malé a stredne-veľké podniky. V roku 2004 spoločnosť predstavila inovatívny produkt - Caligare Flow Inspector (CFI) softvérový monitorovací nástroj pracujúci v operačnom prostrední Linux, ktorý umožňuje sledovanie a analyzovanie sieťovej komunikácie s využívaním technológie flows. Tento nástroj poskytuje efektívne riešenie v oblasti monitorovania a zabezpečenia počítačových sietí. CFI analyzuje dáta vo formáte NetFlow, ktoré sú exportované z routerov, alebo iných sieťových zariadení. Podporuje verzie protokolu NetFlow 1,5,6,7 a 9. Tento nástroj poskytuje riešenie v oblasti monitoringu počítačovej siete v reálnom čase, široké možnosti inteligentného filtrovania jednotlivých flows a následná agregácia a vytváranie štatistík. Na nižšie priloženom obrázku je vidno schému zapojenia, kde sú údaje o flows odosielané priamo z hraničného routra na NetFlow

collector, na ktorom je nainštalovaný nástroj na analyzovanie komunikácie. V tomto prípade zapojenia monitorovacieho nástroja nie je implementovaná zvlášť hardvérová alebo virtuálna sonda a využíva sa export komunikácie priamo zo sieťových zariadení.



Obr. 11 - schéma zapojenia [28]

Vývoj tohoto monitorovacieho nástroja bol pozastavený v roku 2018. V súčasnej dobe je dostupná posledná verzia nástroja 7.2.7, ktorá ma plnú podporu výrobcu. Je samozrejmé, že tento nástroj nemôže konkurovať riešeniam, ktoré sú v súčasnej dobe pravidelne aktualizované, každopádne stále sa nájde oblasť využitia tohoto nástroja.

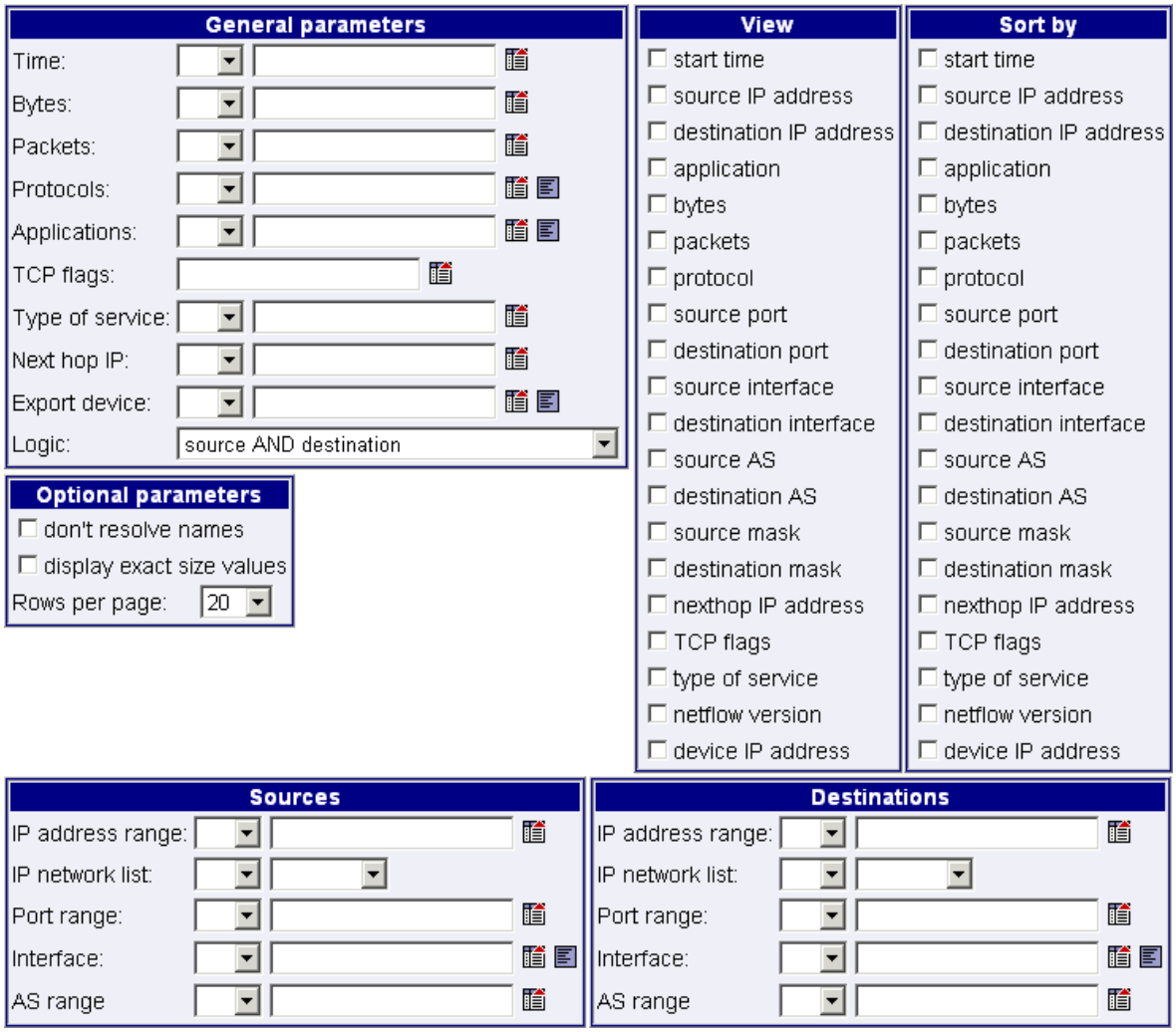
Obr. 12 - logo firmy Caligare s.r.o. [28]

4.2.1 Popis funkcionality

CFI ponúka širokú paletu funkcií, ale jedna z najpotrebnejších funkcií pre monitorovací nástroj je schopnosť analyzovať sieťovú komunikáciu. Tento nástroj umožňuje filtrovať na základe rôznych podmienok, ktoré je možné definovať vo webovom GUI. Výhodou tohto softvéru je možnosť heuristickej detekcie v rôznych typoch aplikácií (napr. Microsoft Exchange, FTP komunikácia, P2P klienti - Direct Connect, Gnutella, Kazza. Nižšie sú uvedené niektoré dostupné atribúty, podľa ktorých je možné tvoriť štatistiky komunikácie:

- celková analýza prevádzky - zobrazenie celkovej sieťovej prevádzky v monitorovanej sieti

- top source / destination host - zobrazenie zariadení v sieti, ktoré najviac využívajú sieť
- aplikácia - zobrazenie najpoužívanejších aplikácií (heuristická detekcia)
- protokoly - zobrazenie najviac využívaných protokolov (Transmission Control Protocol - TCP, User Datagram Protocol - UDP, Internet Control Message Protocol - ICMP)
- top source TCP/UDP porty
- top destination TCP/UDP porty
- top source / destination rozhranie - zobrazenie najviac využívaných zdrojových / cieľových rozhraní
- top source / destination Autonomous System (AS)



Obr. 13 - možnosti filtrovania komunikácie [28]

CFI monitorovací nástroj disponuje aj funkcionalitou detekcie anomálií v sieti. Táto detekcia pracuje na princípe, kedy je vytvorený základný model, ktorý opisuje normálnu sieťovú aktivitu v sledovanej sieti podľa určitého historického vzoru. Akákoľvek iná sieťová komunikácia, ktorá nepatrí do daného vzoru, je označená ako škodlivá. Pri analyzovaní jednotlivých flows komunikácií sa detekcia zameriava hlavne na flows, ktoré majú neobvykle vysoký objem prenesených dát, ale aj na tie, ktoré sa výrazne odlišujú od stanoveného základného modelu komunikácie. Nástroj CFI má tieto moduly detekcie anomálií:

- **skenovanie sieťových portov** - modul skenovania sieťových portov deteguje podozrivé aktivity, ako je napr. prítomnosť červov, BOTNET a iných. Ďalej deteguje stanice, ktoré skenujú sieť a hľadajú zraniteľnosti siete ako napr. Microsoft Windows Internet Name Service (WINS), NETBIOS, Microsoft SQL, MySQL alebo Virtual Network Computing (VNC).
- **skenovanie hostiteľského portu** - tento modul na detekciu siete identifikuje útočníkov, ktorí skenujú porty služieb TCP alebo UDP a hľadajú v nich zraniteľnosti. Modul podporuje iba skenovanie aplikácií, ktoré používajú nízke porty (1-1024).
- **ICMP flooding** - detekcia ICMP flooding kontroluje, koľko packetov ICMP host odosiela. Ak počet packetov prekročí nakonfigurovaný limitný prah, je systémom vytvorená nová anomália. Systém je schopný rozpoznať dlhé správy ICMP (>1000B), takže je možné nakonfigurovať rôzne limitné prahové hodnoty pre krátke správy ICMP a dlhé správy.
- **TCP/SYN flooding** - Modul TCP/SYN flooding zisťuje priame alebo distribuované zaplavenie siete požiadavkami na pripojenie TCP. Tento útok je charakteristický pre DDoS útok.
- **detekcia sieťových počítačových hier** - modul používa na detekciu sieťových hier heuristické metódy. Mnohé hry používajú rovnaký port TCP alebo UDP, takže je veľmi ťažké určiť, ktorá hra bola použitá. V aktuálnej verzií CFI nástroja sú podporované nasledujúce hry - Need for Speed, Diablo, Worms 3D, Railroad Tycoon, Athena Sword, Unreal, Team Speak, Battlefield 1942, Battle Zone, Age of Empires, Heretic, , Doom, Call Of Duty, Castle Wolfenstein, Battlefield 2142, Alien vs. Predator, America's Army, Battle.NET, Vietcong, Half-Life alebo iné [28].

	Start time End time Length	Source	Destination	Severity	Internal	State	Commands
☐	2006/11/19 17:21 2006/11/20 15:34 22 hours 42 minutes	66.235.194.19 ds194-19.ipowerweb.com	N/A	Warning	External network	New	View detail 610 anomalies network port scan
☐	2006/11/19 09:36 2006/11/20 15:34 1 day 5.97 hours	66.214.122.37 66-214-1...ca.charter.com	N/A	Warning	External network	New	View detail 1630 anomalies network port scan
☐	2006/11/13 01:31 2006/11/20 15:34 7 days 14.05 hours	204.180.198.13 esp.localis.com	N/A	Warning	External network	New	View detail 9589 anomalies 2 various network port scan
☐	2006/11/18 13:21 2006/11/20 15:34 2 days 2.21 hours	212.33.121.169	N/A	Warning	External network	New	View detail 2760 anomalies network port scan
☐	2006/11/18 19:27 2006/11/20 15:33 1 day 20.1 hours	84.19.189.163	N/A	Warning	External network	New	View detail 781 anomalies network port scan
☐	2006/11/18 04:51 2006/11/20 15:33 2 days 10.7 hours	212.107.221.34 slavda.ru	N/A	Warning	External network	New	View detail 1713 anomalies network port scan
☐	2006/11/18 23:09 2006/11/20 15:33 1 day 16.39 hours	66.135.33.20	N/A	Warning	External network	New	View detail 1100 anomalies network port scan
☐	2006/11/01 17:49 2006/11/20 15:32 18 days 21.71 hours	221.6.163.50	N/A	Warning	External network	New	View detail 2952 anomalies network port scan
☐	2006/11/16 10:43 2006/11/20 15:32 4 days 4.82 hours	67.15.16.31	N/A	Warning	External network	New	View detail 5728 anomalies network port scan
☐	2006/11/01 17:48 2006/11/20 15:30 18 days 21.7 hours	60.11.125.53	N/A	Warning	External network	New	View detail 2155 anomalies network port scan
☐	2006/11/19 05:22 2006/11/20 15:25 1 day 10.04 hours	221.208.208.212	N/A	Warning	External network	New	View detail 290 anomalies network port scan
☐	2006/11/09 14:24 2006/11/20 15:25 11 days 1.02 hour	221.10.224.253	N/A	Warning	External network	New	View detail 1114 anomalies network port scan
☐	2006/11/01 18:52 2006/11/20 15:25 18 days 20.54 hours	147.231.52.62 kronos.soc.cas.cz	N/A	Warning	External network	New	View detail 6547 anomalies 13 various network games, 4 various p2p applications
☐	2006/11/16 04:21 2006/11/20 15:24 4 days 11.05 hours	202.97.238.203	N/A	Warning	External network	New	View detail 378 anomalies network port scan

Obr. 14 - prehlaď zistených anomálií - CFI [28]

4.3 FlowMon

Začiatky firmy siahajú do roku 2002 kedy skupina vedcov v rámci združenia Czech Education and Scientific Network (CESNET) začala vykonávať aktivity v oblasti programovateľného hardvéru s názvom projektu Liberouter. Počas participovaní na vývoji projektu GENT2 bol tímom Liberouter navrhnutý prototyp sondy na monitorovanie siete s názvom FlowMon. Ten sa stal základom spoločnosti Invea-Tech, ktorá bola založená v roku 2007 pod záštitou Masarykovej univerzity a Vysoké učení technické v Brne. S týmto prototypom riešenia monitorovania siete bola spoločnosť zapojená do inkubačného programu Juhomoravského inovačného centra. V roku 2013 bola vyhlásená spoločnosťou Gartner (americká spoločnosť, ktorá sa zaoberá výskumom a poradenstvom v oblasti Information and Comunications Technologies - ICT) za jediného európskeho dodávateľa, ktorý ponúkal vo svojom

monitorovacom nástroji NBA. V roku 2016 spoločnosť kúpila firmu FerretApps, aby bola schopná doplniť funkcionalitu v oblasti merania výkonnosti aplikácii. V roku 2020 spoločnosť FlowMon bola prevzatá pod spoločnosť Kemp Technologies. Tento krok mal za následok to, že spoločnosť bola schopná doručiť klientom komplexný nástroj na sledovanie siete, detekciu hrozieb a monitorovanie výkonnosti jednotlivých aplikácií. V septembri 2021 spoločnosť Kemp bola odkúpená za $258 miliónov spoločnosťou Progress.

Riešenie na monitorovanie siete od spoločnosti FlowMon je založené na sledovaní flows (protokol NetFlow alebo IPFIX a iné), ktoré poskytuje hĺbkovú viditeľnosť do sieťovej prevádzky. Nástroj Flowmon obsahuje NBA, ktorá poskytuje správcom siete potrebné informácie o stave zabezpečenia siete a potencionálnych hrozbách. Tento nástroj môže byť implementovaný na monitorovanie fyzickej ale aj virtuálnej siete (cloudové riešenia). V nasledujúcej podkapitole sú popísané jednotlivé komponenty riešenia Flowmon [29], [30].

4.3.1 Popis jednotlivých komponentov

Flowmon Probe (sonda) - ide o vysoko výkonné zariadenie, ktoré monitoruje sieťovú prevádzku a generuje flows. Tieto flows sú následne exportované na FlowMon collector, kde sú uložené a analyzované. Sonda je neinvazívna a je pripojená pomocou SPAN portu alebo pomocou TAP zariadenia, a preto nepredstavuje žiaden potencionálny bod zlyhania a neobmedzuje výkon siete. Je transparentná z pohľadu L2/L3 vrstvy OSI. Sondy vo všeobecnosti zhromažďujú hlavne informácie z L2-L4 vrstvy ako IP adresu, protokol, čas odozvy serverov, latenciu a iné. Flowmon proprietárne rozšírenie v protokole IPFIX poskytuje ďalšie údaje z L7 modelu OSI ako napr. názov zariadenia, Uniform Resource Locator (URL), informácie o použitom prehliadači, ďalšie rozširujúce údaje z protokolov ako DNS, Dynamic Host Configuration Protocol (DHCP), Structured Query Language (SQL), Simple Mail Transfer Protocol (SMTP) ale Samba. Okrem monitorovania MAC adries na L2 modelu OSI Flowmon sonda podporuje aj rôzne protokoly a spôsoby enkapsulácie ako VLAN, Multiprotocol Label Switching (MPLS), Generic Routing Encapsulation (GRE), Overlay Transport Virtualization (OTV), Encapsulating Security Payload (ESP) a Transparent Interconnection of Lots of Links (TRILL).

Flowmon sonda ako hardvérové zariadenie - hardware appliance (HA)

Ide o vysoko výkonnú hardvérovú sondu na monitorovanie všetkých typov sietí, od 10 Mbps až 100 Gbps. Flowmon sonda je vyrábaná v dvoch výkonnostných kategóriách, sú to štandardné modely alebo pro modely s rôznym počtom monitorovacích portov. Hardvérová

sonda je vybavená dvoma Ethernet portami s rýchlosťou 10/100/1000 Mb/s (okrem modelu FP-1000-CU), ktoré je možné použiť na konfiguráciu, správu zariadenia a zber flow dát. Porty na správu je možné rozšíriť až na rýchlosť 10 Gb/s, po zakúpení rozširujúceho balíka. Implementácia hardvérovej sondy sa využíva pri rozsiahlých sieťach, s veľkým počtom užívateľov a vysokým dátovým tokom. Hardvérová sonda už v sebe obsahuje vstavaný Flowmon collector a modul Flowmon Monitoring Center (FMC). Tento modul umožňuje ukladanie, vizualizáciu, vytváranie reportov a analyzovanie flows zo sondy. Všetky hardvérové sondy spoločnosti Flowmon sú predávané vo veľkosti 1U, čo predstavuje výšku zariadenia v serverovej skrinke (rack) približne 43,6 mm.

Obr. 15 - Flowmon hardvérová sonda [30]

V nižšie priloženej tabuľke je možné vidieť porovnanie jednotlivých hardvérových modelov sondy a ich jednotlivé hardvérové špecifikácie.

P/N[1]	Model	Performance Per Port[2]	Performance Per Appliance[2]	Monitoring Port	Flow Cache[3]	RAID	Disk Type	CPU[4]	RAM	Remote Control
IFP-1000-CU	Kemp Flowmon Probe 1000	1.48 Mpps	1.48 Mpps	1 x 10/100/1000 Mbps Ethernet	0.5 M	-	1 x SATA	8	32 GB	Express
IFP-2000-CU	Kemp Flowmon Probe 2000	1.48 Mpps	2.96 Mpps	2 x 10/100/1000 Mbps Ethernet	0.5 M	-	1 x SATA	8	32 GB	Express
IFP-4000-CU	Kemp Flowmon Probe 4000	1.48 Mpps	3 Mpps	4 x 10/100/1000 Mbps Ethernet	0.5 M	-	1 x SATA	8	32 GB	Express
IFP-4000-SFP	Kemp Flowmon Probe 4000 SFP	1.48 Mpps	3 Mpps	4 x 1 Gbps Ethernet	0.5 M	-	1 x SATA	8	32 GB	Express
IFP-10000-SFP+	Kemp Flowmon Probe 10000 SFP+	1.5 Mpps	1.5 Mpps	1 x 10 Gbps Ethernet	4 M	-	1 x SATA	12	64 GB	Enterprise
IFP-20000-SFP+	Kemp Flowmon Probe 20000 SFP+	1.5 Mpps	3 Mpps	2 x 10 Gbps Ethernet	4 M	-	1 x SATA	12	64 GB	Enterprise
IFP-40000-SFP+	Kemp Flowmon Probe 40000 SFP+	5 Mpps	20 Mpps	4 x 10 Gbps Ethernet	4 M	RAID1	2 x SATA	48	64 GB	Enterprise
IFP-4000PRO-CU	Kemp Flowmon Probe 4000 Pro	1.48 Mpps	3 Mpps	4 x 10/100/1000 Mbps Ethernet	0.5 M	RAID1	2 x SATA	8	32 GB	Enterprise
IFP-4000PRO-SFP	Kemp Flowmon Probe 4000 Pro SFP	1.48 Mpps	3 Mpps	4 x 1 Gbps Ethernet	0.5 M	RAID1	2 x SATA	8	32 GB	Enterprise
IFP-20000PRO-SFP+	Kemp Flowmon Probe 20000 Pro SFP+	14.8 Mpps	29.6 Mpps	2 x 10 Gbps Ethernet	4 M	RAID1	2 x SATA	48	128 GB	Enterprise
IFP-40000PRO-SFP+	Kemp Flowmon Probe 40000 Pro SFP+	14.8 Mpps	59.2 Mpps	4 x 10 Gbps Ethernet	4 M	RAID1	2 x SATA	48	128 GB	Enterprise
IFP-200000PRO-QSFP28	Kemp Flowmon Probe 200000 Pro QSFP28	100 Mpps[5]	150 Mpps[5]	2 x 40/100 Gbps Ethernet	32 M	RAID1	2 x SATA	40[6]	256 GB	Enterprise

Tab. 3 - porovnanie hardvérových sond [30]

Flowmon sonda ako virtuálne zariadenie - virtual appliance (VA)

Flowmon sonda vo forme virtuálneho zariadenia je zariadenie na monitorovanie siete, určené na nasadenie do vybraného virtuálneho prostredia (VMware, Hyper-V, KVM). Sonda, ktorá je nasadená vo virtuálnom prostredí, poskytuje rovnakú fumcionalitu ako tie hardvérové. Hlavným rozdielom medzi virtuálnym a hardvérovým riešením je počet podporovaných monitorovacích portov a ich rýchlosť. Na rozdiel od hardvérovej sondy, virtuálna neobsahuje vstavaný Flowmon collector. Preto je potrebné použiť špecializovaný kolektor na ukladanie a analýzu komunikácie vo formáte NetFlow/IPFIX. Virtuálne sondy podporujú až dva porty pre správu (okrem modelu IFP-1000-VA, ktorý disponuje iba jedným portom pre správu), ktoré možno použiť na konfiguráciu zariadenie, správu a export flows. V nižšie priloženej tabuľke je možné vidieť porovnanie jednotlivých riešení virtuálnych sond.

P/N	Model	Performance Per Port[1]	Performance Per Appliance[1]	Monitoring Interfaces	Flow Cache[2]	VMware ESXi	Microsoft Hyper-V	KVM	Recommended Configuration[3]
IFP-1000-VA	Kemp Flowmon Probe 1000 VA	Up to 0.3 Mpps	Up to 0.3 Mpps	1 x 1 Gbps Ethernet	0.5 M	5.5 and later	2012 R2 and later	KVM 3.10.0 QEMU 1.5.3 libvirt 4.5.0 and later	4 CPU cores, 8 GB RAM, min. 25 GB HDD
IFP-2000-VA	Kemp Flowmon Probe 2000 VA	Up to 0.3 Mpps	Up to 0.6 Mpps	2 x 1 Gbps Ethernet	0.5 M				4 CPU cores, 8 GB RAM, min. 25 GB HDD
IFP-4000-VA	Kemp Flowmon Probe 4000 VA	Up to 0.3 Mpps	Up to 1.2 Mpps	4 x 1 Gbps Ethernet	0.5 M				6 CPU cores, 8 GB RAM, min. 25 GB HDD
IFP-6000-VA	Kemp Flowmon Probe 6000 VA	Up to 0.3 Mpps	Up to 1.8 Mpps	6 x 1 Gbps Ethernet	0.5 M				6 CPU cores, 8 GB RAM, min. 25 GB HDD
IFP-10000-VA	Kemp Flowmon Probe 10000 VA	Up to 0.7 Mpps	Up to 0.7 Mpps	1 x 10 Gbps Ethernet	4 M				8 CPU cores, 8 GB RAM, min. 25 GB HDD
IFP-20000-VA	Kemp Flowmon Probe 20000 VA	Up to 0.7 Mpps	Up to 1.4 Mpps	2 x 10 Gbps Ethernet	4 M				8 CPU cores, 8 GB RAM, min. 25 GB HDD

Tab. 4 - porovnanie virtuálnych sond [30]

Flowmon Collector

Flowmon Collector je zariadenie na monitorovanie siete, ktoré ukladá a spracováva flow dáta. Tieto dáta sú generované zo zariadení ako napr. load balancere, swtiche alebo routre, ale taktiež môže ísť aj o dedikované sieťové sondy, alebo iné zdroje flow dát. Je nutné poznamenať, že nie vždy je nutné investovať do sondy (či už virtuálnej alebo hardvérovej). Collector spracováva dáta vo všetkých štandardných formátoch ako napr. NetFlow, IPFIX, sFlow, NetStream a iné. Na collectore sú nainštalované rôzne doplnkové moduly, ktoré rozširujú funkcionalitu v oblasti monitorovania a zabezpečovania siete. Collector ma natívne nainštalovaný v sebe modul FMC na vizualizáciu komunikácie a vytváranie definovaných pohľadov. Všetky dostupné moduly sú popísane v samostatnej podkapitole tejto práce.

Collector môže byť implementovaný do rôznych prostredí, a to ako cloudová aplikácia dostupná v riešeniach poskytovateľov cloudových služieb ako Amazon Web Services (AWS), Microsoft Azure alebo Google Cloude. Tak ako Flowmon sonda, tak isto aj collector je dostupný v prevedení HW a VA. Hardvérový collector je vybavený dvoma Ethernet portami s

rýchlosťou 10/100/1000 Mb/s, ktoré je možné použiť na konfiguráciu, správu zariadenia zber flow dát. Porty na správu je možné rozšíriť až na rýchlosť 10 Gb/s po zakúpení rozširujúceho balíka. Hardvérové collectory sú dostupné v prevedeniach 1U a 2U. V nižšie priloženej tabuľke je možné vidieť porovnanie jednotlivých hardvérových modelov collectora.

P/N	Model	Performance (fps)[1]			Storage Capacity	RAID	Disk Type	CPU[5]	RAM	Form Factor
		Peak[2]	Moderate user experience[3]	Best user experience[4]						
IFC-R5-1000	Kemp Flowmon Collector R5-1000	75 000	40 000	20 000	1 TB	HW RAID5	3 x SATA Hot Swap	8	32 GB	1U
IFC-R5-2000	Kemp Flowmon Collector R5-2000	100 000	40 000	20 000	2 TB	HW RAID5	3 x SATA Hot Swap	8	32 GB	1U
IFC-R5-3000PRO	Kemp Flowmon Collector R5-3000 Pro	150 000	80 000	40 000	3 TB	HW RAID5	4 x SATA Hot Swap	32	64 GB	1U
IFC-R10-4000PRO	Kemp Flowmon Collector R10-4000 Pro	250 000	120 000	60 000	4 TB	HW RAID10	4 x SATA Hot Swap	32	64 GB	1U
IFC-R5-6000PRO	Kemp Flowmon Collector R5-6000 Pro	150 000	80 000	40 000	6 TB	HW RAID5	4 x SATA Hot Swap	32	64 GB	1U
IFC-R5-12000PRO	Kemp Flowmon Collector R5-12000 Pro	200 000	120 000	60 000	12 TB	HW RAID5	4 x SATA Hot Swap	64	128 GB	1U
IFC-R10-16000PRO	Kemp Flowmon Collector R10-16000 Pro	300 000	160 000	80 000	16 TB	HW RAID10	4 x SATA Hot Swap	64	128 GB	1U
IFC-R5-24000PRO	Kemp Flowmon Collector R5-24000 Pro	200 000	120 000	60 000	24 TB	HW RAID5	4 x SATA Hot Swap	64	128 GB	1U
IFC-R6-48000PRO	Kemp Flowmon Collector R6-48000 Pro	250 000	120 000	60 000	48 TB	HW RAID6	8 x SATA Hot Swap	72	128 GB	2U
IFC-R6-96000PRO	Kemp Flowmon Collector R6-96000 Pro	250 000	120 000	60 000	96 TB	HW RAID6	14 x SATA Hot Swap	72	128 GB	2U
IFC-R6-192000PRO	Kemp Flowmon Collector R6-192000 Pro	250 000	120 000	60 000	192 TB	HW RAID6	18 x SATA Hot Swap	72	128 GB	2U
IFC-R5-2880SSD	Kemp Flowmon Collector R5-2880 SSD	400 000	200 000	100 000	2.88 TB	HW RAID5	4 x SATA Hot Swap	72	256 GB	1U
IFC-R5-11400SSD	Kemp Flowmon Collector R5-11400 SSD	400 000	200 000	100 000	11.4 TB	HW RAID5	4 x SATA Hot Swap	72	256 GB	1U
IFC-MU	Kemp Flowmon Collector – Master Unit	–			6 TB	HW RAID5	4 x SATA Hot Swap	32	64 GB	1U
IFC-PU	Kemp Flowmon Collector – Proxy Unit	–			6 TB	HW RAID5	4 x SATA Hot Swap	32	64 GB	1U

Tab. 5 - porovnanie hardvérových chcollectorov [30]

Ako už bolo už spomenuté pri virtuálnej Flowmon sonde, tak isto aj pri virtuálnom collectore platí, že poskytuje rovnakú funkcionalitu ako hardvérové riešenie. Jediný rozdiel je v dostupnom výkonne zariadenia a veľkosti úložného miesta pre dáta. Virtuálny collector disponuje dvoma portami na konfiguráciu, správu zariadenia zber flow dát. Okrem toho virtuálny collector podporuje až dva 1 Gbps monitorovacie porty, ktoré umožňujú monitorovanie sieťovej prevádzky a vytváranie flows.

P/N	Model	Performance (fps)[1,2]	Storage Capacity[3]	VMware ESXi	Windows Hyper-V	KVM	Minimum Configuration[3]
IFC-500-VA	Kemp Flowmon Collector 500 Virtual Appliance	up to 75 000	0.5 TB	5.5 and higher	2012 R2 and higher	KVM 3.10.0 and higher QEMU 1.5.3 and higher libvirt 4.5.0 and higher	2 CPU cores, 8 GB RAM, 500 IOPS
IFC-1000-VA	Kemp Flowmon Collector 1000 Virtual Appliance	up to 75 000	1 TB				2 CPU cores, 8 GB RAM, 500 IOPS
IFC-2000-VA	Kemp Flowmon Collector 2000 Virtual Appliance	up to 75 000	2 TB				2 CPU cores, 8 GB RAM, 500 IOPS
IFC-3000-VA	Kemp Flowmon Collector 3000 Virtual Appliance	up to 150 000	3 TB				4 CPU cores, 8 GB RAM, 1000 IOPS
IFC-6000-VA	Kemp Flowmon Collector 6000 Virtual Appliance	up to 150 000	6 TB				4 CPU cores, 8 GB RAM, 1000 IOPS
IFC-12000-VA	Kemp Flowmon Collector 12000 Virtual Appliance	up to 200 000	12 TB				8 CPU cores, 16 GB RAM, 2000 IOPS
IFC-24000-VA	Kemp Flowmon Collector 24000 Virtual Appliance	up to 200 000	24 TB				8 CPU cores, 16 GB RAM, 2000 IOPS
IFC-48000-VA	Kemp Flowmon Collector 48000 Virtual Appliance	up to 200 000	48 TB				8 CPU cores, 16 GB RAM, 2000 IOPS
IFC-64000-VA	Kemp Flowmon Collector 64000 Virtual Appliance	up to 200 000	64 TB				8 CPU cores, 16 GB RAM, 2000 IOPS

Tab. 6 - porovnanie virtuálnych collectorov [30]

4.3.2 Flowmon moduly

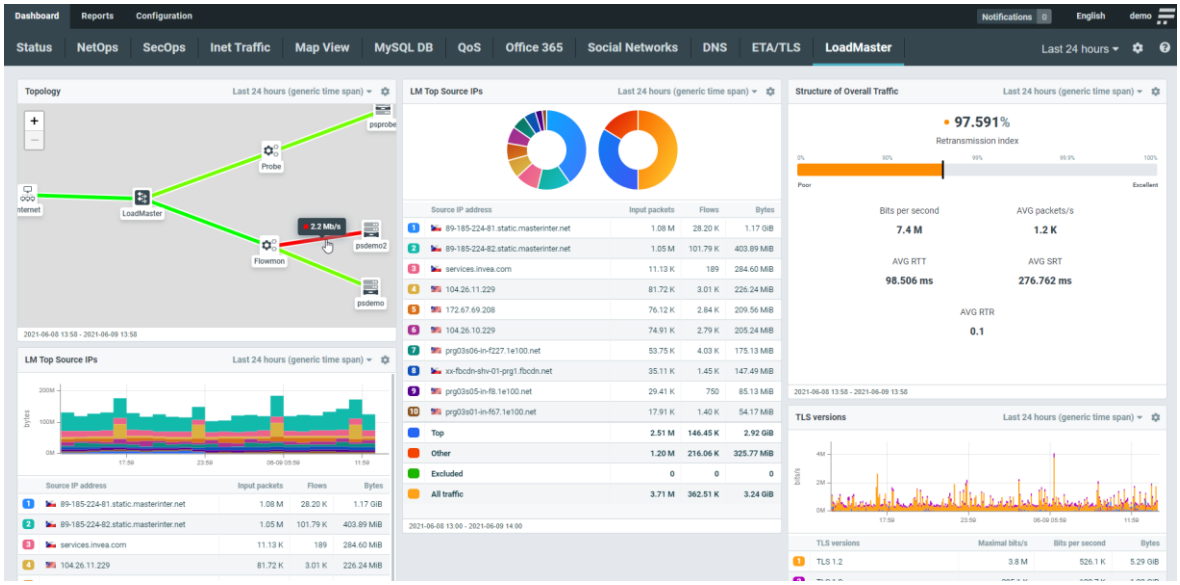
Na collectore môžu byť nainštalované rôzne moduly v závislosti od potreby konkrétnych používateľov. Tieto moduly je možné zaradiť do dvoch hlavných kategórií, a to moduly ktoré sa využívajú pri sledovaní sieťovej prevádzky alebo moduly zabezpečujúce sieťovú bezpečnosť. Moduly môžu byť nainštalované do collectora na základe zakúpenej licencie.

V tejto podkapitole sú popísane jednotlivé dostupné moduly spoločnosti Flowmon. Na nižšie priloženom obrázku je možno vidieť GUI nástroja Flowmon so všetkými dostupnými modulmi, ktoré sú nainštalované na collectore. V prípade, že určitý modul nie je nainštalovaný na collectore, jeho ikona je vyobrazená v šedom prevodní.

Obr. 16 - GUI rozhranie nástroja Flowmon [30]

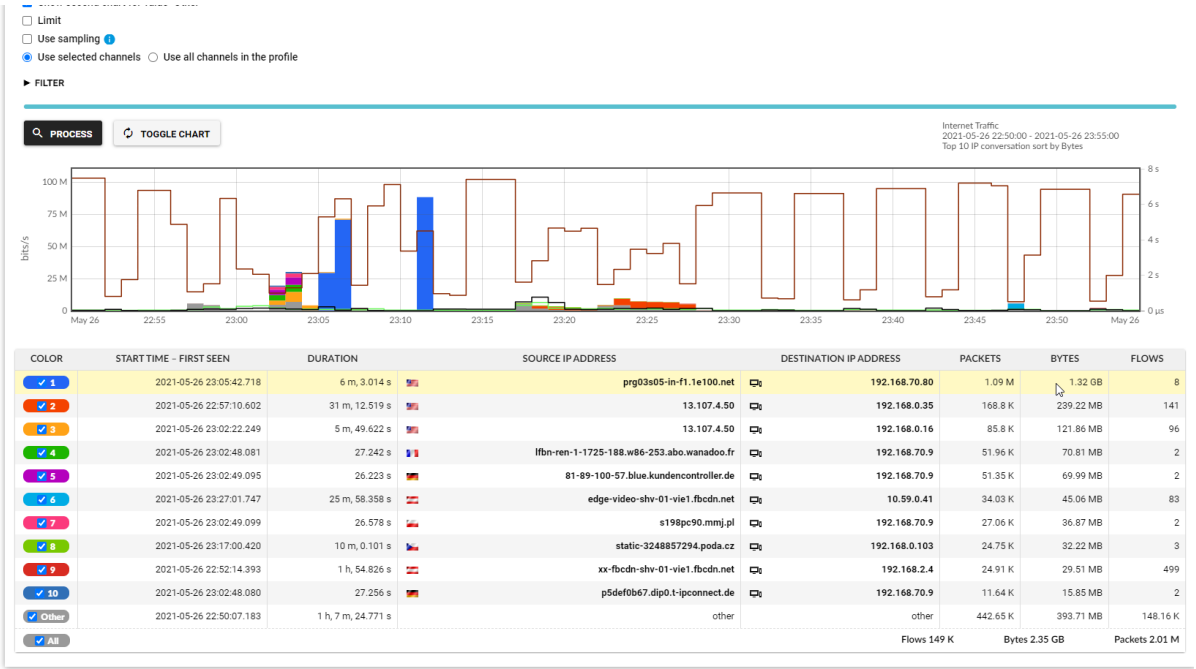
Flowmon Monitoring Center (FMC)

Tento modul je natívne nainštalovaný na collecotre (či už na HW alebo VA) a nie je potrebné k nemu zakupovať špeciálnu dodatkovú licenciu. Poskytuje vizualizáciu jednotlivých dát a vytváranie analýz. Všetky telemetrické údaje o sieti sú vyobrazované vo vysoko prispôsobiteľnom dashboarde, ktorý umožňuje hĺbkovú vizualizáciu dát a vytváranie používateľom definovaných štatistík. Toto umožňuje používateľom presne, rýchlo a efektívne odstrániť problémy, optimalizovať sieť a zvýšiť jej bezpečnosť. V module sú predpripravené šablóny s najpoužívanejšími službami na monitorovanie napr. Office 365, G-Suite, sociálnych sietí, DNS alebo DHCP.



Obr. 17 - Flowmon dashboard [30]

Jednotlivé udalosti je možné v prípade potreby podrobne skúmať až na úroveň jednotlivých dátových tokov a packetov. Je možné zobraziť aj veľmi špecifické podrobnosti ako sú informácie o zariadeniach, výrobcoch alebo jednotlivé zdroje flows. Užívateľ má možnosť ďalšieho filtrovania podľa protokolov, časových intervalov, zdrojovej alebo cieľovej IP adresy, alebo iných parametrov.

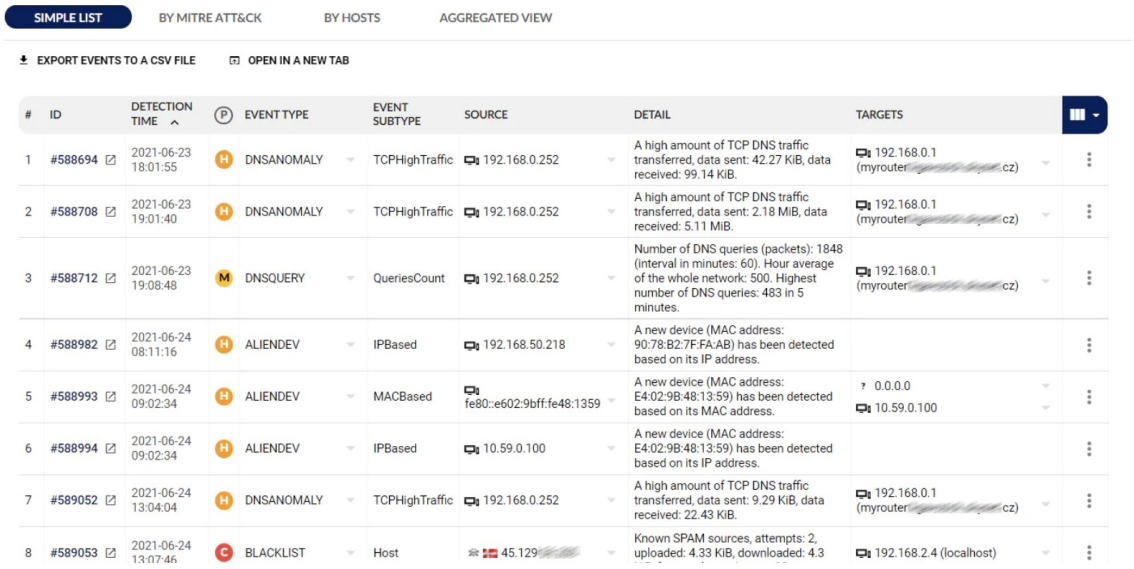


Obr. 18 - filtrovanie komunikácie v modul FMC [30]

Anomaly Dedection System (ADS)

Ide o bezpečnostný modul, ktorý využíva umelú inteligenciu a strojové učenie na zisťovanie skorých anomálii v sieťovej komunikácií. Hlavným cieľom tohoto modulu je odhaliť

podozrivé správanie, útoky na kritické aplikácie, únik dát alebo upozorniť na možné kompromitácie. Tento modul upozorňuje na vnútorné hrozby, ktoré nie je možné odhaliť pomocou ochrany koncových staníc. Modul poskytuje viac ako 40 detekčných metód, ktoré využívajú umelú inteligenciu a približne 200 algoritmov. Pracuje na základe NBA, čiže sleduje a upozorňuje na podozrivé spávanie v monitorovanej sieti. Systém má povedomie o obvyklom bežnom správaní jednotlivých koncových staníc, serverov a pod. a upozorňuje na jednotlivé odchýlky v tomto správaní. Nevyhľadáva v známych a už popísaných databázach Common Vulnerabilities and Exposures (CVE), ale identifikuje neobvyklé správanie. Modul ADS v sebe obsahuje Intrusion Detection System (IDS) nadstavbu, ktorá umožňuje prijímanie upozornení zo Suricata IDS. Vďaka tomuto tento modul poskytuje kompletné riešenie, ktoré zahŕňa aj tzv. signature based detekciu. (porovnávanie komunikácie už voči databáze popísaných a známych hrozieb). Je možné odhaliť neznáme hrozby, malware, ransomeware alebo zneužitie určitej zraniteľnosti konkrétneho systému. Tento modul je možné prepojiť napr. s firewallom alebo iným bezpečnostnými zariadeniami, za účelom včasnej reakcie na vzniknutý incident.



Obr. 19 - detekcia anomálii v module ADS [30]

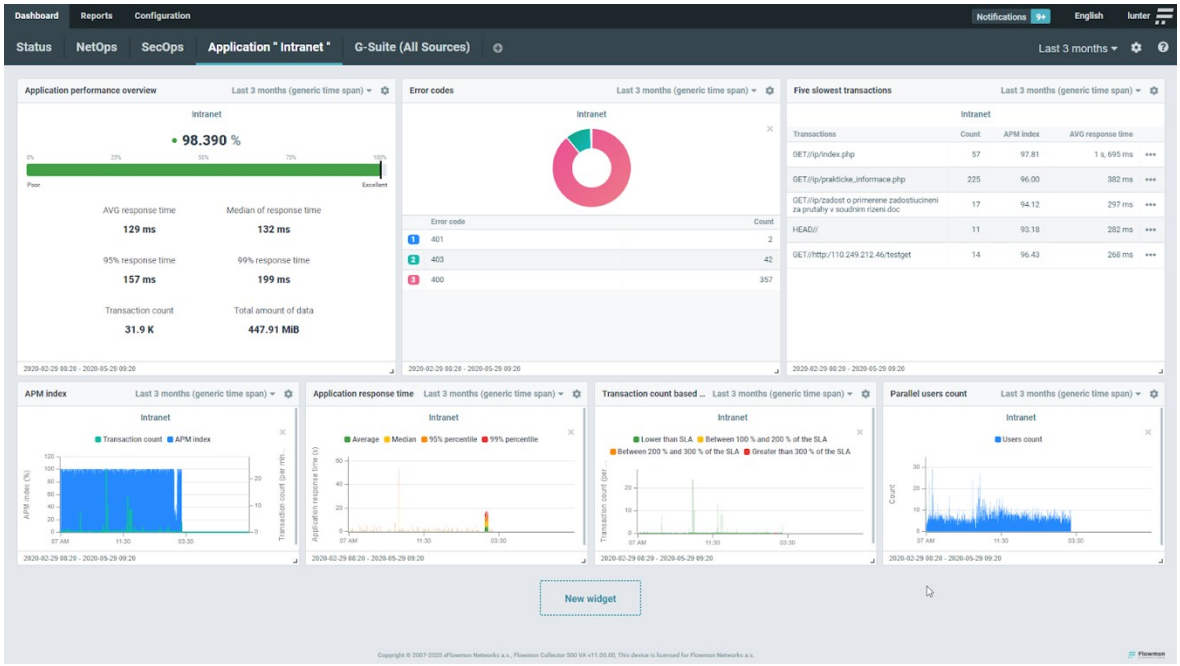
Application Performance Monitoring (APM)

Je to bezagentný modul, ktorý meria používateľskú skúsenosť a výkonnosť dôležitých podnikových aplikácii. Zobrazuje spoľahlivé dáta o využívaní siete, kapacite a chybovosti. APM poskytuje prehľad na celkový reťazec monitorovaných aplikácií a interakcií medzi

užívateľom a aplikačným serverom. Táto komunikácia umožňuje rýchle riešenie problémov a analyzovanie príčiny vzniku takýchto problémov. Zbierané metriky sú spracovávané za účelom presného určenia sieťového prvku, ktorý je zodpovedný za problémy napr. s latenciou alebo bottlenecks. Vysoko užívateľsky prispôsobiteľný dashboard poskytuje okamžité informácie o užívateľskej skúsenosti s danou aplikáciou, jej výkonnosti a súčasne kľúčových metrík v čase alebo počet najpomalších transakcií v sieti.

Oblasti použitia:

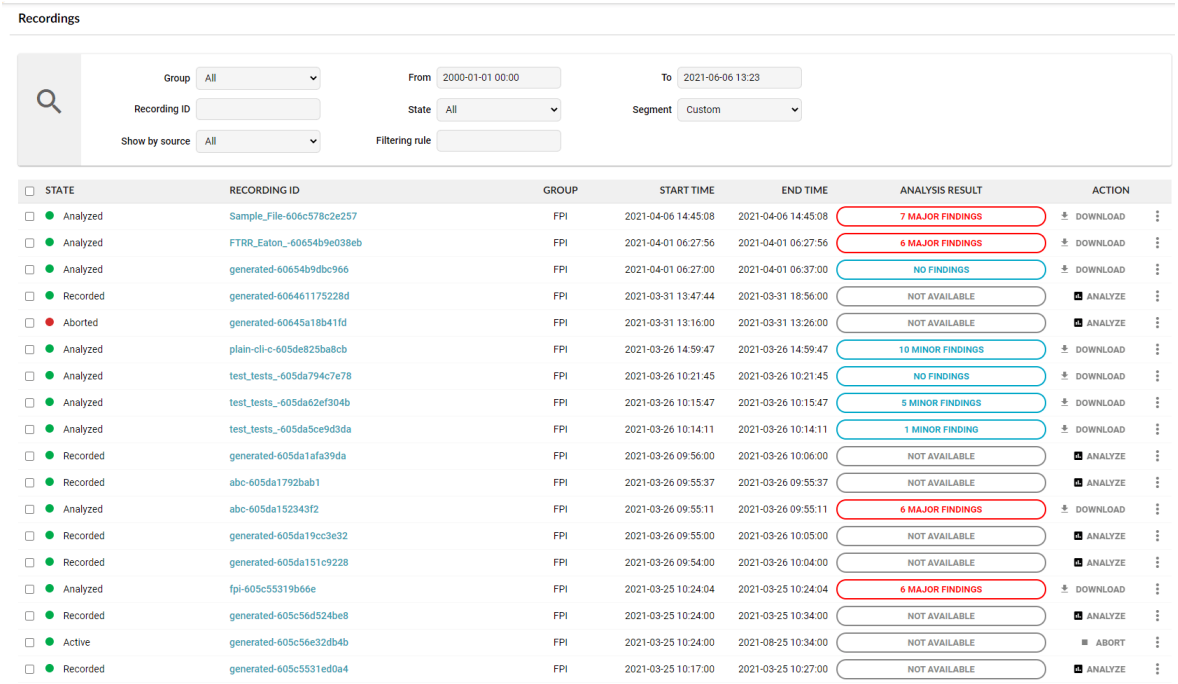
- **migrácia do cloudu** - modul ma natívnu podporu cloud riešeniach ako AWS, Azure a Google Cloud
- **plánovanie kapacity** - bohaté štatistiky a hlásenia poskytujú správcom jasný pohľad o používaní aplikácii a je možné vytvoriť pevný základ pre účelne využitie a alokovanie zdrojov
- **dostupnosť aplikácii** - tento modul sleduje dostupnosť aplikácií, identifikuje bottlenecks, monitoruje chybné kódy, flowmon APM funguje na princípe bez agenta a poskytuje informácie o príčinách problémov bez akéhokoľvek vplyvu na výkon
- **používateľská skúsenosť** - tento modul monitoruje aplikácie z pohľadu používateľa a poskytuje jednoduché riešenia problémov a analýzy hlavných príčin vzniku



Obr. 20 - dashboard modulu APM [30]

Flowmon Packet Investigator (FPI)

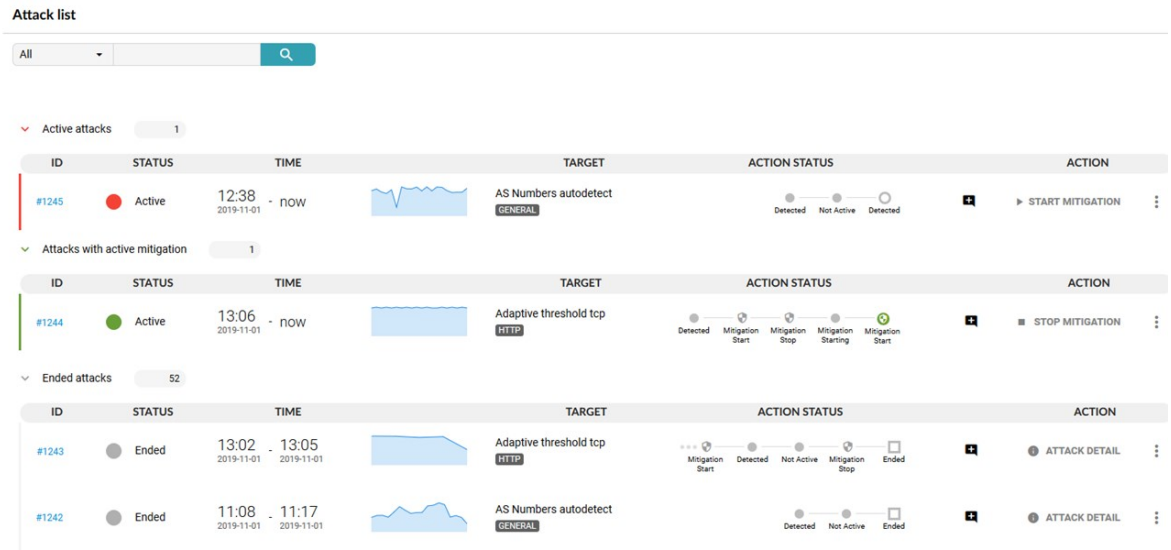
Rozširuje funkčnosti Flowmon sondy o zachytávanie celej komunikácie (Full Packet Capture), je možné vykonávať odposluch celkovej komunikácie alebo nastaviť špeciálne pravidlá, pri ktorých sa spustí nahrávanie komunikácie. Tento modul vykonáva automaticky audit sieťovej prevádzky a následne ho analyzuje. FPI vykonáva analýzu jednotlivých protokolov, sleduje ich závislosti a RFC špecifikácie z PCAP súboru a poskytuje jednoduchú detekciu problémov a kategorizovanie v závislosti na ich závažnosť. Packety je možné analyzovať viacerými spôsobmi, a to manuálne (manuálne zapnutie nahrávania), nahratím vlastného PCAP súboru s odchytenou komunikáciou, alebo modul FPI je schopný vykonať automatické zachytávanie packetov na základe vopred definovaných pravidiel, alebo pri detekcii anomálie z modulu ADS. Hlavnú výhodou tohoto modulu je to, že poskytuje automatickú analýzu zachytenej komunikácie, a preto nie sú potrebné dlhodobé skúsenosti správcov v tejto problematike. FPI je vytvorený tak, aby pokrýval široké spektrum protokolov, ktorých počet sa neustále zvyšuje. Identifikuje poruchy, alebo nesprávnu konfiguráciu kritických sieťových služieb (Address Resolution Protocol - ARP, DNS, DHCP, ICMP, Netowrk Time Protocol - NTP) a dokáže odhaliť nekompatibilitu šifrovania klient/server (verzie Secure Sockets Layer - SSL a Transport Layer Security - TLS) a mnoho ďalších bezpečnostných parametrov.



Obr. 21 - zachytená komunikácia v FPI module [30]

Flowmon DDoS Defender

Ide o modul na detekciu a zmiernenie volumetrických útokov, ako DoS alebo DDoS. Bez potreby akýchkoľvek zmien v konfigurácii, zmeny topológie alebo dodatočných investícií do sieťových komponentov je možné odhaliť tieto volumetrické útoky, ktoré sú smerované proti IT infraštruktúre, alebo na určitú konkrétnu kritickú aplikáciu v reálnom čase. Nasadenie tohoto modulu je veľmi rýchle a jednoduché, vďaka univerzálnej architektúre a širokých možnostiach integrácie so sieťovými zariadeniami. Flowmon DDoS Defender umožňuje prispôsobiť detekciu DDoS útokov tým, že správcom umožňuje nastaviť rôzne prahy detekcie pre používateľov, alebo časti sieťovej prevádzky. V prípade potreby je možné prahové hodnoty upraviť aj manuálne. Pri detekcii útoku systém upozorní používateľa a je schopný dať inštrukcie iným bezpečnostným zariadeniam na zastavenie daného útoku (napr. firewall) [30].



Obr. 22 - modul Flowmon DDoS Defender [30]

II. PRAKTICKÁ ČASŤ

5 VÝBER MONITOROVACIEHO NÁSTROJA

V tejto kapitole je popísaný výber finálneho riešenia, ktoré je následne implementované do firemnej siete. V prvej podkapitole je uvedený stručný popis monitorovanej siete a sú vytýčene po konzultácii s nemenovanou firmou základne funkčné predpoklady na nástroj. Nasledujúca kapitola sa zaoberá už konkrétnym výberom a porovnávaním jednotlivých nástrojov. V závere je uvedené cenové porovnanie a možnosti, akým spôsobom jednotlivé nástroje môžu byť obstarané, a taktiež je uvedený vybraný nástroj, ktorý je implementovaný v sledovanej firemnej sieti.

5.1 Popis monitorovanej siete

Vybraný monitorovací nástroj je implementovaný do firemnej počítačovej siete. Ide o malú až strednú firmu pôsobiacu v Českej republike, ktorá pôsobí v oblasti IT technológií. V sieti je do 200 aktívnych používateľov a iné sieťové zariadenia ako napr. Voice over Internet Protocol (VOIP) telefóny, tlačiarne, wifi prístupové body, chytré telefóny a rôzne servery.

Hlavným cieľom zavedenia monitorovania firemnej sieti je zvýšenie viditeľnosti do komunikácie a včasná detegcia anomálii a útokov, či už z vnútra siete alebo z verejného Internetu. Kľúčové požiadavky firmy sú:

- možnosť implementácie nástroja v čisto virtuálnom prostredí bez nutnosti obstarávať špeciálny fyzicky hardvér,
- komplexné riešenie na hĺbkový monitoring a bezpečnosť siete,
- pravidelné aktualizácie a podpora zo strany výrobcu,
- možnosť monitorovať na základe rôznych protokolov,
- vytváranie štatistík o prenesenej komunikácii (kto komunikoval s kým, počet prenesených packetov, bytov, atd ...),
- možnosť dohľadať klienta na základe IP adresy alebo MAC adresy,
- vytváranie používateľom definovaných upozornení (alerting),
- detekcia anomálií,
- používateľsky prívetivé prostredie,

Spoločnosť, pre ktorú je spracovaná táto diplomová práca si neurčila maximálnu sumu, ktorú je ochotná investovať do vybraného riešenia. Samozrejme, pomer ceny k výkonu by mal byť primeraný veľkosti siete a pri výbere monitorovacieho nástroja zohľadnený.

5.2 Výber monitorovacieho nástroja

V kapitole č. 4 boli popísané tri veľmi podobné nástroje, ktoré sa používajú v oblasti monitorovania a zabezpečovania počítačových sietí. Všetky tieto riešenia majú počiatky v Českej Republike, aj keď napr. riešenie Flowmon už bolo odkúpené zahraničnou firmou. Všetky tri nástroje poskytujú v podstate veľmi podobné spektrum funkcionalít zameraných na monitoring a bezpečnosť siete. Nástroj Flowmon pracuje na základe flows, kedy pomocou Flowmon sondy sú tieto flows obohatené o proprietárne metadata, samozrejme umožňuje aj full packet capture, čiže záchyt komplet komunikácie na základe určených podmienok. Produkt Mendel od firmy GreyCortex je hlavne založený na zachytávaní celkovej komunikácie, ktorá je následne spracovaná za použitia ich vlastného protokolu. Riešenie od firmy Caligare pracuje rovnako výhradne s flows ako Flowmon s tým rozdielom, že sa spolieha hlavne na štandardné metadata z verzii NetFlow protokol (podporovane max. do NetFlow v9). Čo sa týka funkcionality filtrovania komunikácie na základe užívateľských nastavení sú tieto nástroje veľmi podobne, da sa konštatovať, že sa líšia len v spôsobe ovládania cez webové GUI rozhranie. Vo všetkých troch nástrojoch je možné filtrovať komunikáciu na základe zdrojovej / cieľovej IP adresy a ďalších parametrov. Ako už bolo spomenuté vyššie v tejto prací, nástroj CFI od firmy Caligare už v súčasnej dobe nie je ďalej vyvíjaný, čo sa odzrkadlilo na prevedení GUI rozhrania, ktoré nie je až tak intuitívne ako u ostatných porovnávaných nástrojoch. Taktiež nedisponuje podporou IPv6.

Čo sa týka oblasti bezpečnosti siete je možné konštatovať, že riešenie od firmy GreyCrotex a Flowmon ponúkajú obdobné funkcionality v oblasti včasnej identifikácie známych aj neznámych hrozieb. Oba tieto nástroje využívajú viaceré podobné metódy pri detekcii hrozieb ako napr. NBA, prepojenie s verejnými databázami popísaných hrozieb, detekcia s využitím umelej inteligencie a mnohé iné. Tieto dva spomenuté nástroje poskytuje obrovské množstvo funkcii, ktoré je možné prispôsobiť podľa potrieb konkrétnej sledovanej siete. Taktiež poskytujú možnosti reportovania a vizualizácie dát a informácii spoločne s možnosťou integrácie nástroja s ďalšími systémami ako napr. SIEM, LDAP a iné. Taktiež nástroje umožňujú integráciu priamo s rôznymi výrobcami firewallov, za účelom možnosti automatickej reakcie na útoky. Prostredie a prevedenie nástroja GreyCortex je viac prispôsobené a orientované

na bezpečnosť siete. Riešenie od firmy Caligare ponúka len základnú a čiastočne obmedzenú detekciu bezpečnostných hrozieb na základe vopred definovaných algoritmov, neumožňuje pokročilé behaviorálne analýzy alebo porovnávanie incidentov s databázami popísaných hrozieb. Je možné konštatovať, že toto riešenie ponúka najmenej detekčných metód v oblasti bezpečnosti z týchto troch nástrojov. Je to v dôsledku pozastavenia ďalšieho vyvíjania. Taktiež tento nástroj neumožňuje ďalšiu integráciu pomocou syslog servera na napr. firewall alebo iné podnikové systémy.

5.2.1 Cena

Cena za jednotlivé nástroje sa veľmi líši v závislosti na spôsobe implementácie a veľkosti monitorovanej siete. Výrobcovia týchto nástrojov ponúkajú široké možností výberu. Je nutné podotknúť, že v prípade riešenia od firmy Flowmon a GreyCortex nie sú verejne dostupné cenníky za tieto nástroj, a preto bolo nutné kontaktovať tieto spoločnosti priamo za účelom vytvorenia konkrétnej cenovej ponuky. Firma Caligare má cenník verejne dostupný a je ho možno vidieť na nižšie priloženom obrázku.

Part number	Product name	Base price (EUR)	
CFI-PRO1	Caligare Flow Inspector Professional for 1 collector	777,00 €	Add item
CFI-PRO2	Caligare Flow Inspector Professional for 2 collectors	957,00 €	Add item
CFI-PRO3	Caligare Flow Inspector Professional for 3 collectors	1.137,00 €	Add item
CFI-PRO4	Caligare Flow Inspector Professional for 4 collectors	1.317,00 €	Add item
CFI-PRO5	Caligare Flow Inspector Professional for 5 collectors	1.497,00 €	Add item
CFI-PRO6	Caligare Flow Inspector Professional for 6 collectors	1.677,00 €	Add item
CFI-PRO7	Caligare Flow Inspector Professional for 7 collectors	1.857,00 €	Add item
CFI-PRO8	Caligare Flow Inspector Professional for 8 collectors	2.037,00 €	Add item
CFI-PRO9	Caligare Flow Inspector Professional for 9 collectors	2.217,00 €	Add item
CFI-ENT	Caligare Flow Inspector Enterprise Edition	2.577,00 €	Add item
CFI-PRO-TECH	CFI Professional Edition - Next 1 year tech support	297,00 €	Add item
CFI-ENT-TECH	CFI Enterprise Edition - Next 1 year tech support	477,00 €	Add item
CFI-COLLUPD	CFI Additional collectors	0,00 €	Add item

Obr. 23 - Caligare Flow Inspector cenník [29]

V prípade firemnej siete, ktorá je predmetom tejto práce by postačoval 1 collector za 777€. Collector umožňuje pripojenie jeden zdroj dát - flows, čo v prípade firemnej siete predstavuje hraničný router, ktorý umožňuje exportovanie flows v protokole NetFlow. Pri tomto nástroji sa nepočíta s externou sondou. Vyššie spomenutá cena je perpetuálna (licenciu stačí kúpiť len jedenkrát - žiadne ročné poplatky). V tejto cene je už zahrnutá technická podpora

po dobu jedného roka a aktualizácie (v tomto prípade bezpredmetné, keďže vývoj je aktuálne pozastavený).

Ďalšie dva monitorovacie nástroje sa už pohybujú v iných cenových reláciách. Flowmon zvolil modulárny prístup, kedy klient ma v základe nainštalovaný na collectore modul FMC a následne ostatné moduly je možné dokúpiť podľa potreby. Jednotlivé moduly majú viacero prevedení, líšia sa hlavne vo výkonnostných parametroch ako je throughput, množstvo spracovaných flows za sekundu, počet monitorovacích portov, alebo ich rýchlosť. Ako už bolo spomenuté, riešenie firmy Flowmon je založené na modularite modulov. V tejto posudzovanej sieti bol zvolený Flowmon základný model sondy IFP-1000-VA spoločné s IFC-1000-VA collectorom. Za účelom sledovania bezpečnosti siete je collector doplnený modulom ADS. Celková perpetuálna cena aj s ADS modulom je 21 000€, alebo je možná aj ročná subskripcia vo výške 10 500€. Firma taktiež ponúka aj balík technickej podpory , ktorá zahŕňa aktualizáciu softvéru spoločne aj aktualizáciami pre modul ADS vo výške 3 150€.

Nástroj Mendel od firmy GreyCortex zvolil iný prístup k cenovej politike a možnostiam výberu. Ponúka kompletnú funkcionalitu nástroja a hlavný rozhodujúci faktor pri výbere je hodnota maximálneho trvalého prietoku na hraničnom bode - router. V sledovanej sieti je dodávaná rýchlosť od Internet Service Provider (ISP) v rýchlosti 500/100 Mbps, a preto bolo potrebné zvoliť variantu nástroja, ktorý je schopný pracovať s takouto rýchlosťou. Perpetuálna cena za all-in-one (collector + sonda) VA riešenie je 27 500€, je ponúkaná aj ročná subskripcia vo výške 17 000€. GreyCortex taktiež ako firma Flowmon ponúka softvérovú údržbu a podporu vo výške 8 130€ za 1 rok.

5.3 Zhrnutie

V tejto kapitole boli zhrnuté a porovnané dostupné riešenia na sledovanie sieťovej prevádzky a sieťovej bezpečnosti. Po konzultácii s nemenovanou firmou bolo zvolené riešenie od firmy Flowmon, a to hlavne z dôvodu vyhovujúcejšiemu užívateľskému prostrediu, cene a možnosti rozširovať funkcionalitu podľa potreby pomocou modulov. Popis implementácie do prostredia je popísaný v ďalšej kapitole tejto práce.

6 IMPLEMENTÁCIA NÁSTROJA

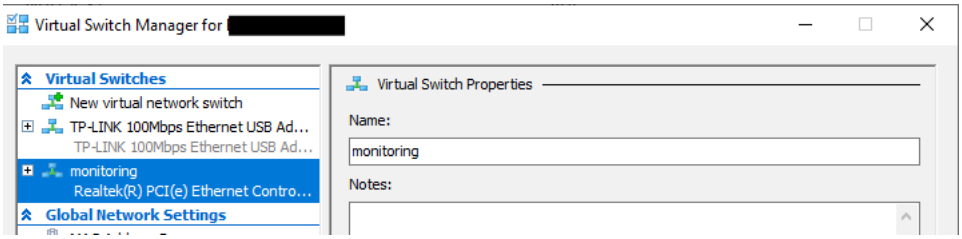
V tejto kapitole je popísaný postup implementácie a konfigurácie nástroja Flowmon na monitorovanie siete vo vybranom firemnom prostredí. Je nutné podotknúť, že niektoré údaje ako napr. IP adresy a pod. sú v tejto kapitole pozmenené a zašifrované tak, aby bol zachovaný maximálny stupeň anonymity pre danú firmu. Tento nástroj poskytuje široké spektrum možných nastavení, a preto v tejto časti sú popísane iba základne. V závere kapitoly sú uvedené vzorové nastavenia nástroja, ktoré boli požadované lokálnym správcom siete.

6.1 Inštalácia nástroja Flowmon

Ako už bolo spomenuté, monitorovací nástroj je nainštalovaný ako virtuálna zariadenie vo virtualizačnom prostredí Microsoft Hiper-V, pod operačným systémom Windows Server 2022. Zariadenie má nasledujúce hardvérové špecifikácie:

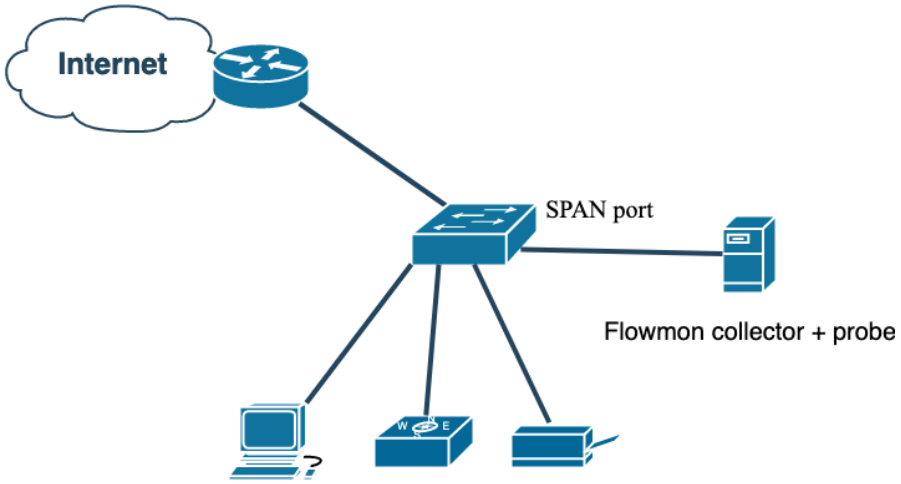
- AMD Ryzen 7 2700 Eight-Core Processor, 3.20 GHz
- 48 GB RAM
- 2 TB SSD
- 512 GB SSD - systémový disk
- 2x sieťová karta (jedná priamo na základnej doske + externá USB TP-Link 100 Mbps karta)

V prostredí Hyper-V je vytvorené nové virtuálne zariadenie, je mu pridelený názov, alokovaný pamäť RAM, v tomto prípade je to 16 GB a pridelených 8 jadier CPU. Je zvolená sieťová karta pre manažment, teda je vybratá sieťová karta, na ktorej virtuálne zariadenie dostane IP adresu, pomocou ktorej sa bude pristupovať do webového GUI rozhrania. Pre tento účel bola zvolená externá USB karta TP-Link. Ďalej je nutné pridať dva virtuálne disky vo formáte Virtual Hard Disk v2 (VHDX), ktoré je možné stiahnuť priamo zo stránok výrobca a obsahujú skúšobnú licenciu. Je potrebné upraviť ešte nastavenia virtual switch v prostredí Hyper-V, kde sú pridané obe sieťové karty (Obr. 24).



Obr. 24 - pridelenie sieťových kariet do virtual switch

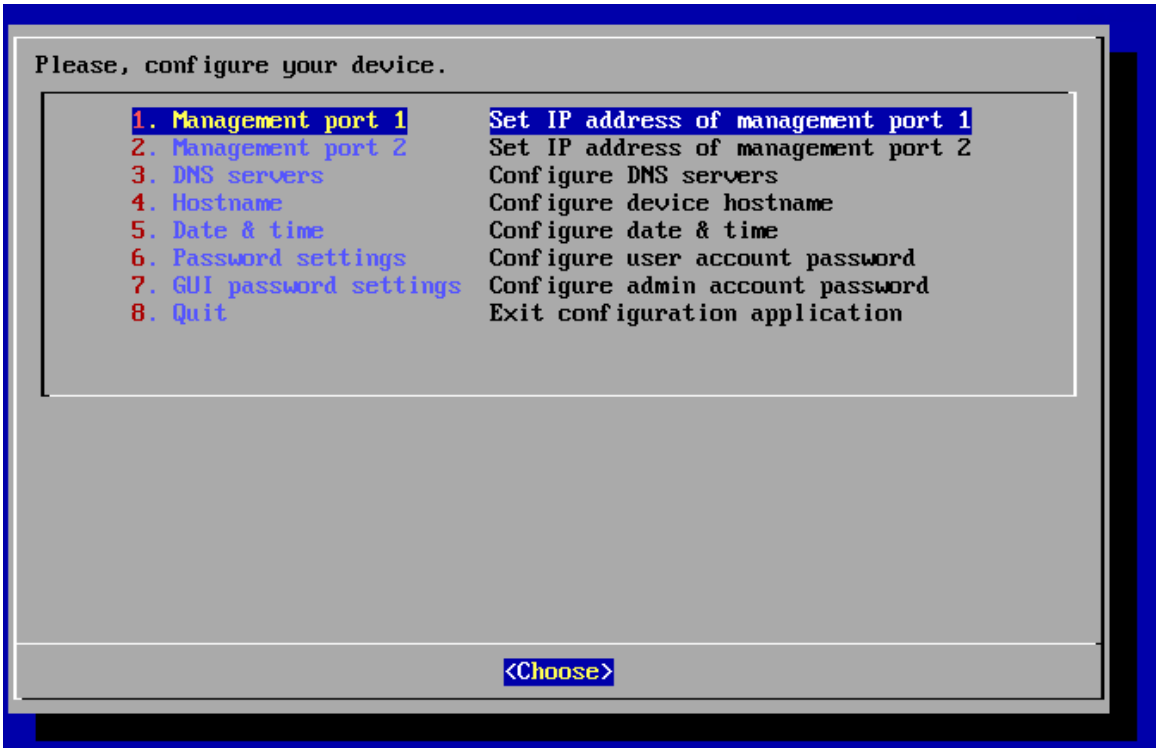
Ďalej je nutné nastaviť SPAN port na core switch, ktorý je následne prepojený so sieťovou kartou zariadenia, na ktorom je spustené virtuálne zariadenie. V tomto prípade je core switch značky Cisco, na ktorom je SPAN port je možné nastaviť príkazom - monitor session. Na nižšie priloženom obrázku je možné vidieť schému topológie.



n

Obr. 25 - schéma topológie zapojenia

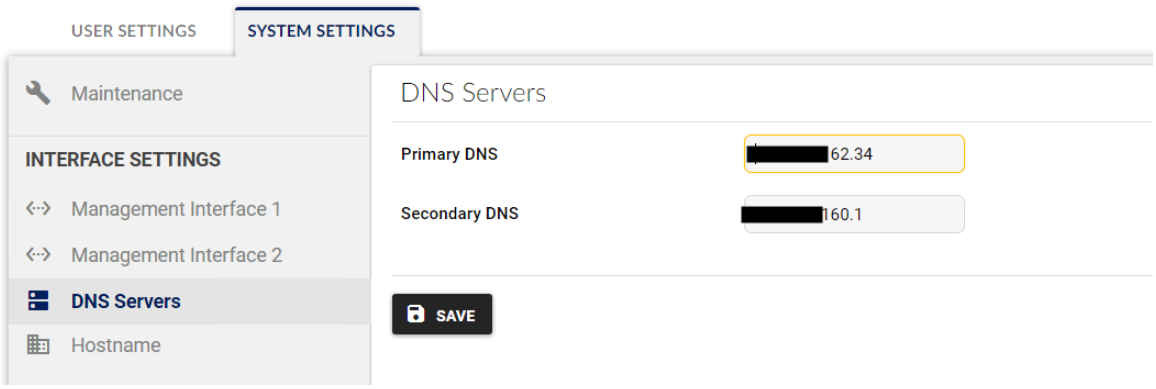
Po úspešnej inštancií je nutné sa pripojiť cez Hyper-V na virtuálne zariadenie a pomocou konzoly nastaviť IP adresu manažment portu. Pomocou príkazu sysconfig je otvorené menu, v ktorom zvolíme management port 1 a vyplníme požadovaná IP adresu, masku siete a bránu, následne cez túto IP adresu je prístupne GUI rozhranie nástroja. Taktiež je nutné nastaviť heslo pre admin účet. Ostatné údaje je možne nastaviť aj neskôr už priamo cez GUI.



Obr. 26 - nastavenie manažment IP

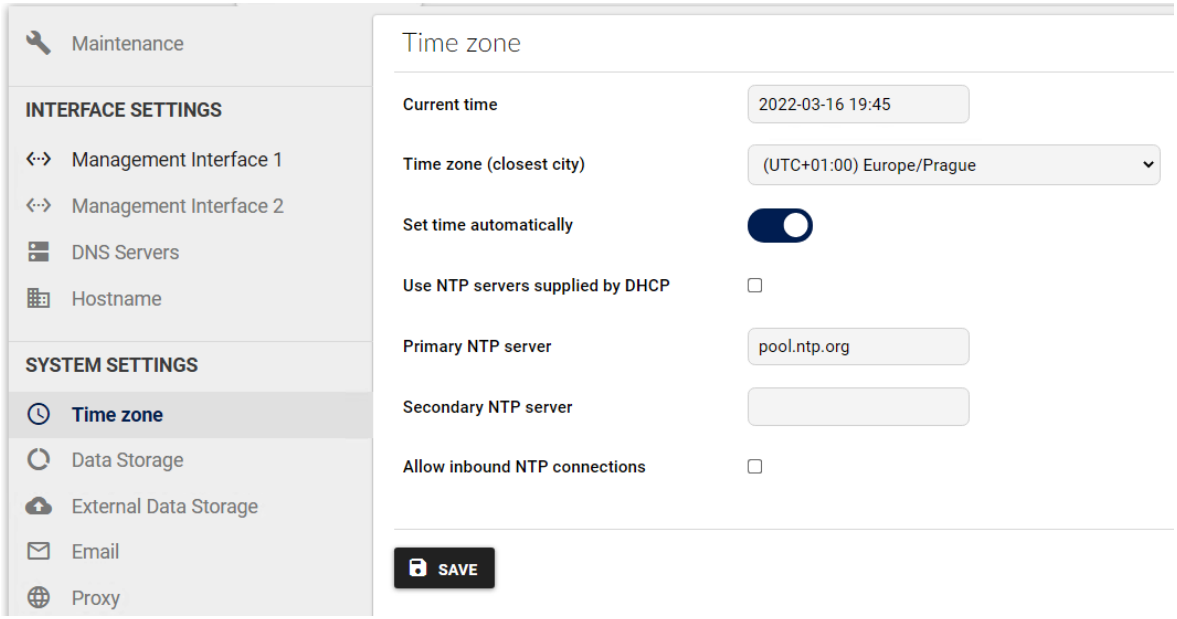
6.2 Základná konfigurácia nástroja

Po zadaní danej IP adresy z predošlého kroku do webového prehliadača je sprístupnené GUI rozhranie, cez sekciu Configuration Center je možné nastaviť systémové nastavenia. Na nižšie priloženom obrázku je vidieť definovanie DNS serverov pre danú sieť.



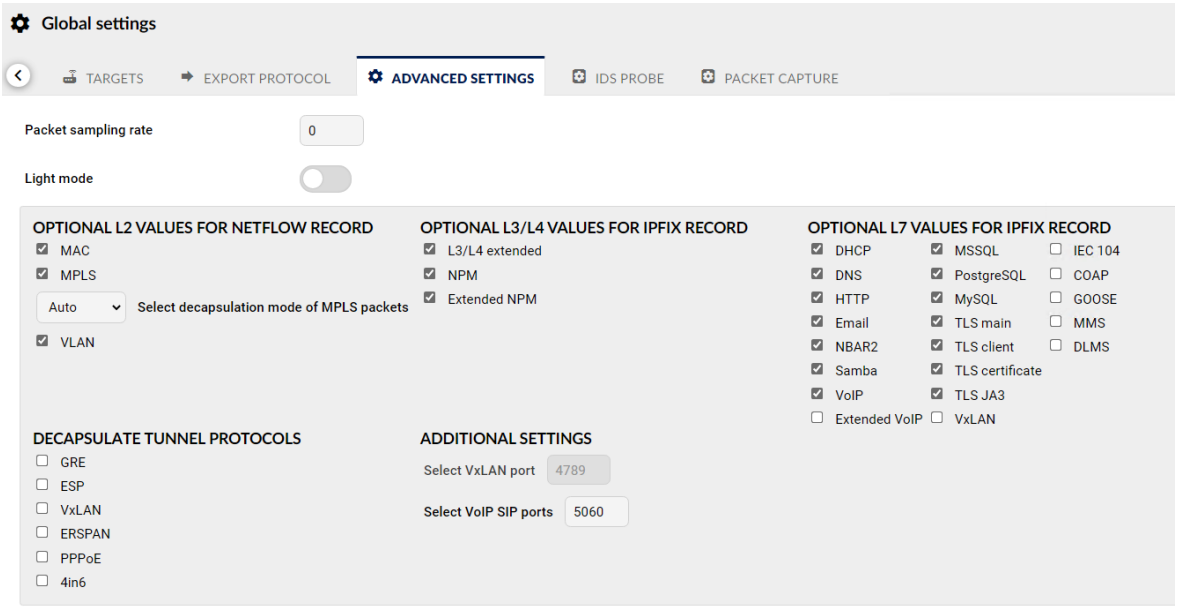
Obr. 27 - nastavenie DNS serverov

Taktiež je veľmi dôležité mať nastavaný správny systémový čas, za účelom správneho vyhodnocovania jednotlivých analýz, preto je vybrané automatické nastavenie času v správnej časovej zóne.



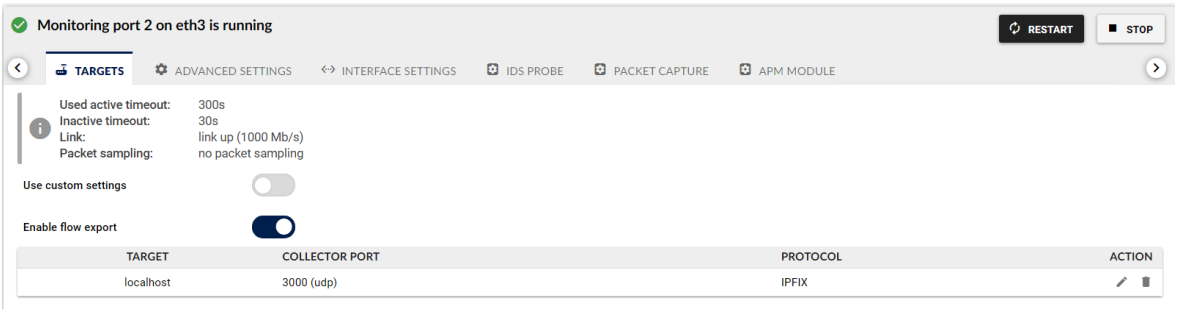
Obr. 28 - nastavenie času

V časti monitoring ports sa nachádzajú nastavenia, ktoré sa zaoberajú činnosťou monitorovacích portov. Nad každým monitorovacím rozhraním sondy je spustený jeden monitorovací port, ktorý zo zachytenej sieťovej komunikácie vytvára jednotlivé flows. V tejto časti je možné nakonfigurovať jednotlivé monitorovacie porty, alebo je možné využiť globálne nastavenia pre všetky monitorovacie porty. V časti advanced settings je možné nastaviť frekvenciu vzorkovania packetov, identifikátory tokov a zoznam autonómnych systémov. Ako je vidieť na nižšie priloženom obrázku, je možné zvoliť voliteľné hodnoty z jednotlivých vrstiev modelov OSI, ktoré je schopná sonda spracovať zo sieťovej komunikácie.



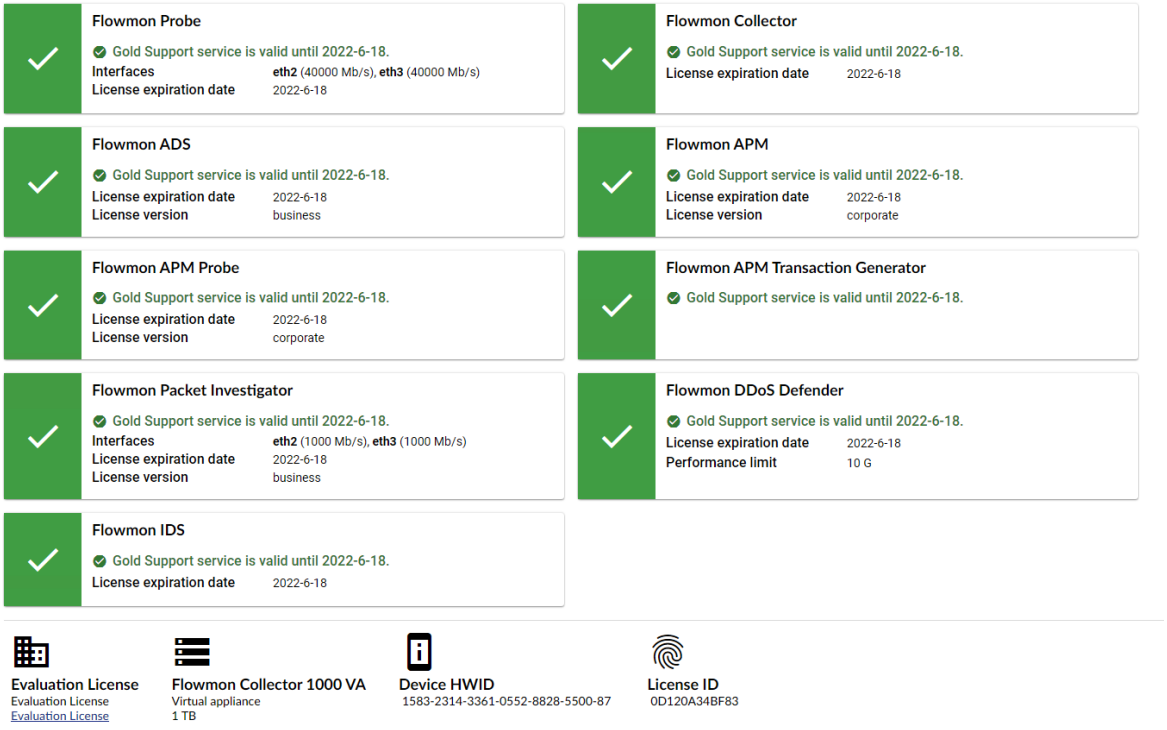
Obr. 29 - nastavenie sondy

Ďalej v tejto sekcii je vidieť konkrétne monitorovacie porty a ich dostupné nastavenia. Za účelom exportu je nutné špecifikovať hostiteľa, na ktorom je spustený collector. V tomto prípade ide o rovnaké zariadenie. Ako protokol pre export je vybraný IPFIX a cieľ je exportovania je localhost na porte 3000 UDP.



Obr. 30 - nastavenie exportu zo sondy na collector

Za účelom získania plnej funkcionality je nutné do collectora pridať potrebnú licenciu. V inštalačnom balíku v rámci 30 dňovej skúšobnej dobe licencia obsahuje všetky moduly. Licencia je vo formáte .key a je pridaná cez sekciu License (Obr. 32).

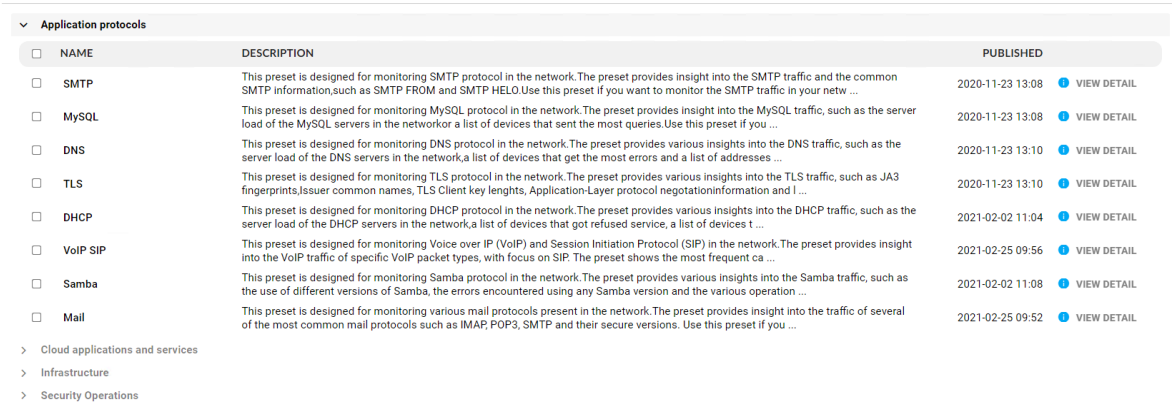


Obr. 31 - informácie o pridaných licenciách

6.3 Presets - predvoľby

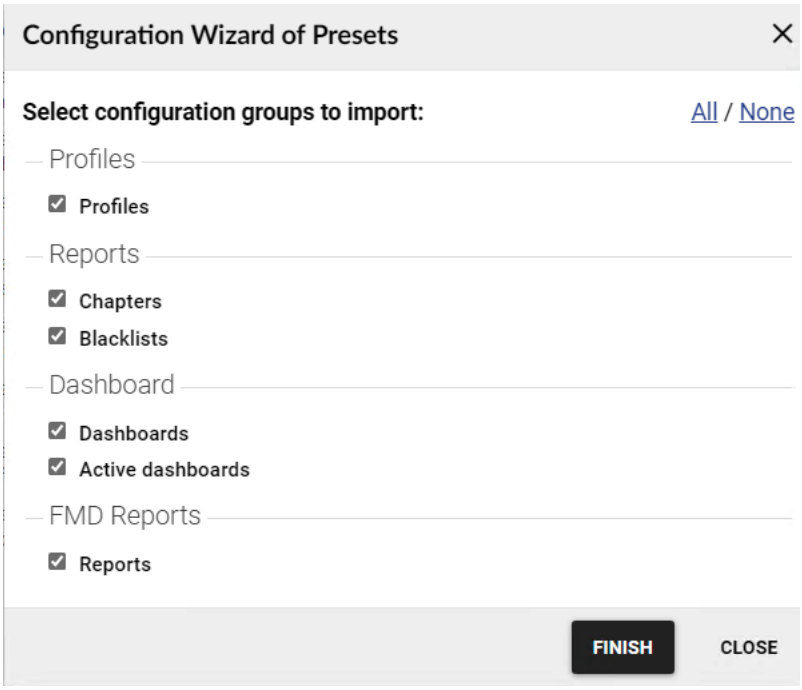
Presety umožňujú jednoducho konfigurovať nástroj Flowmon pridaním prednastavených zobrazení siete, hlavných aplikácií, alebo sieťového výkonu. Presets pozostávajú zo sady

profilov, kapitol reportu, reportov, widgetov a dashboardov. Tieto položky sú automaticky vytvorené pri pridaní konkrétneho presetu. Systém kontroluje nové alebo nedávno upravené presety a automaticky ich aktualizuje každých 12 hodín. Na nižšie priloženom obrázku je možné vidieť názov presetu, stručný popis a dátum poslednej úpravy tohoto presetu.



Obr. 32 - prehľad dostupných presetov

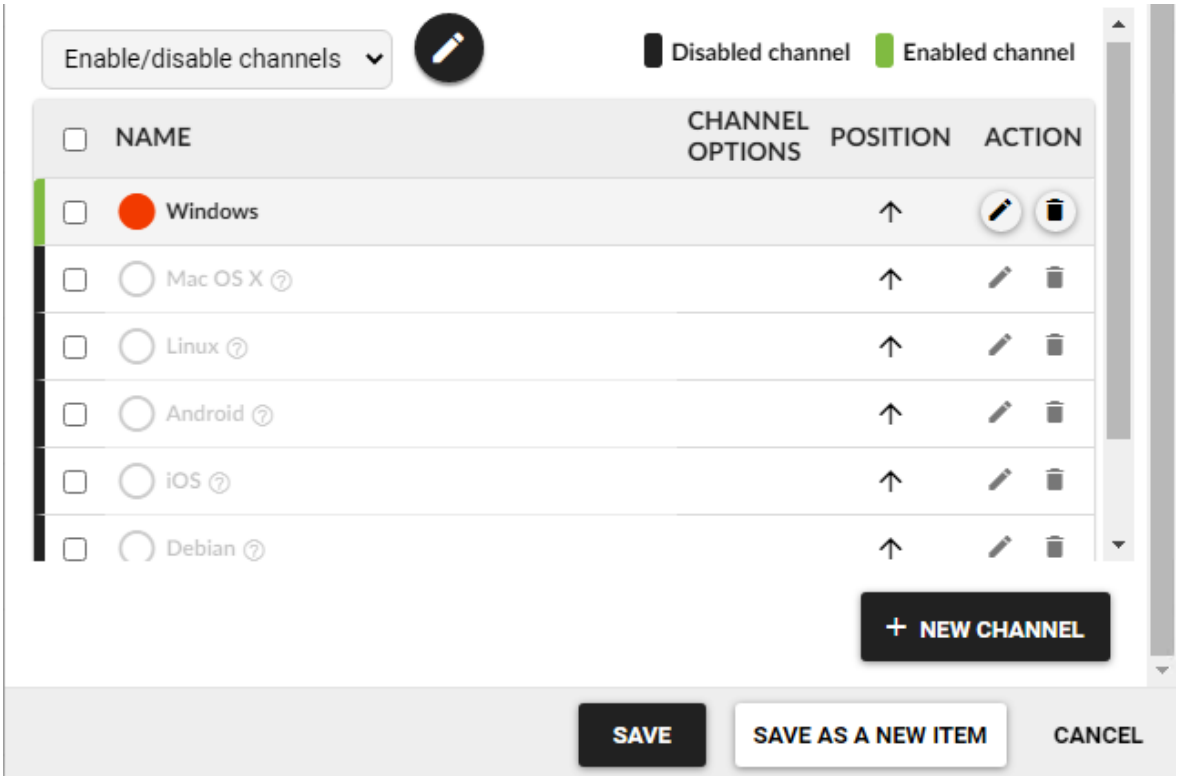
Tieto presety sú veľmi užitočné a poskytujú rýchlu konfiguráciu systému, pretože pomocou nich je možné automaticky vytvoriť konkrétny filtrovaný profil, report alebo dashboard.



Obr. 33 - možnosti nastavenia presetu

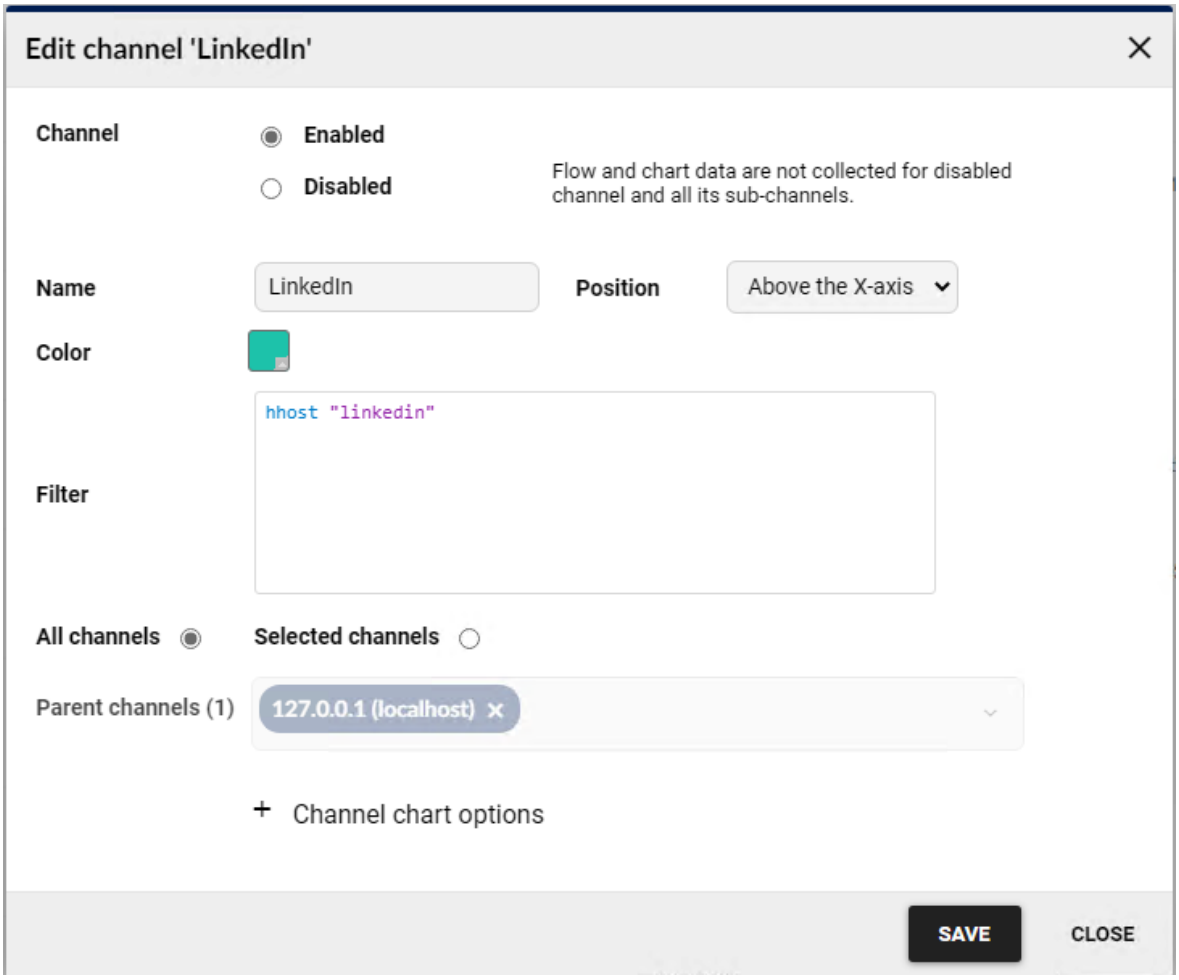
Ako už bolo spomenuté na začiatku, presety sa skladá hlavne z prednastaveného profilu. Po zvolení vybraných presetov je možné vidieť vytvorené profile v module FMC. Profily je možné ďalej editovať a upravovať ich podľa potreby. Napr. v prípade profilu na zobrazenie

operačných systémov v sieti je možné profil upraviť aby zobrazoval čisto len napr. stanice s operačným systémom Windows a následne tento profil je možné uložiť pod novým názvom.



Obr. 34 - upravenie profilu

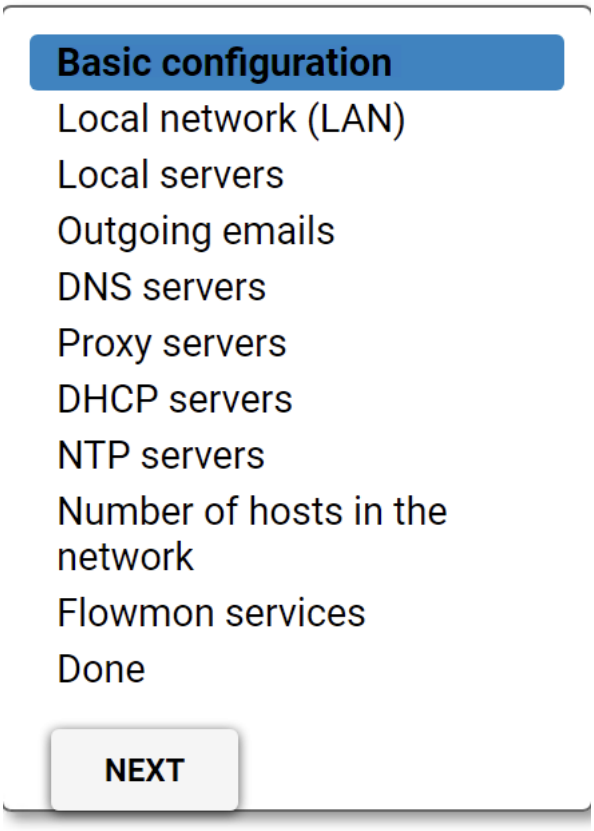
Filtrovanie pomocou profilov je založené na vopred definovanom syntaxe filtra, ktorý je súčasťou profilu, tým je uľahčené filtrovanie a práca s flows pretože odpadá potreba písania jednotlivých podmienok. Na nižšie priloženom obrázku je možné vidieť syntax filtru z profilu sociálne siete, kde je vidieť podmienku pre filtrovanie len sociálnej siete Linkedin. Rovnaký syntax filtru je možné použiť aj priamo pri filtrovaní v module FMC.



Obr. 35 - syntax filtru

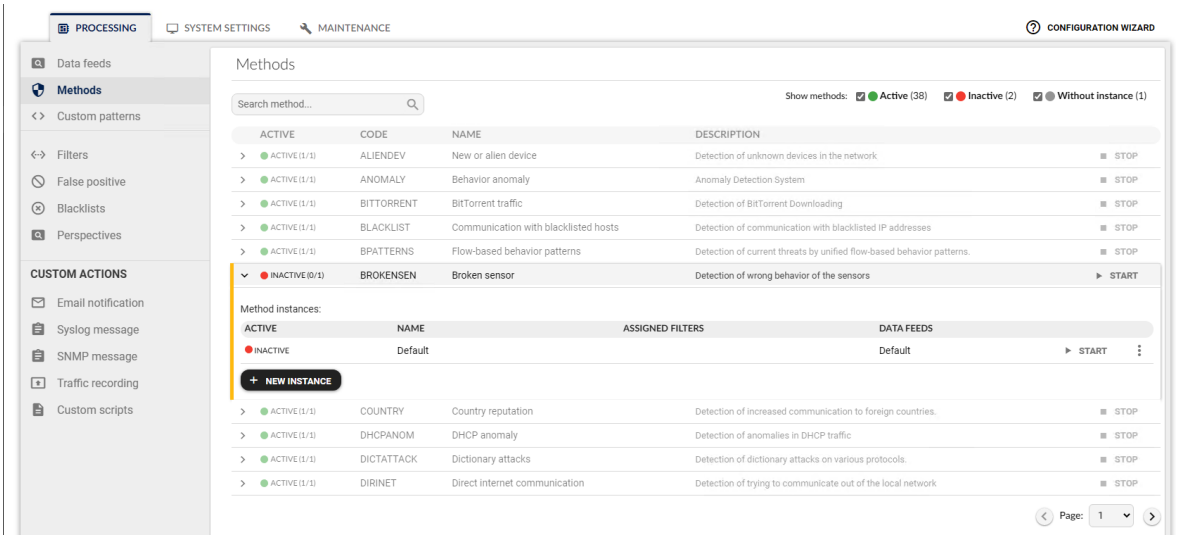
6.4 Konfigurácia ADS modulu

Pri prvom spustení bezpečnostného modulu ADS je užívateľovi ponúknuté automatické nastavenie modulu v niekoľkých korkoch. Nastavenie sprevádza používateľa nastavením údajov o monitorovanej sieti - jej veľkosť, počet používateľov alebo či sa jedná o firemnú sieť alebo ISP. Ďalej je definovaný IP rozsah pre lokálnu sieť aj s dostupnými verejnými IP adresami od ISP, sú definované IP adresy serverov v sieti (za účelom presnejšej detekcie anomálií a rozlišovania medzi klientami a servermi). Je definovaný emailový server odosielania správ (SMTP) za účelom vylúčenia iných nepovolených SMTP serverov a sú pridané IP adresy DNS serverov (poskytnutý od ISP). Kompletné kroky nastavení je možno vidieť na nižšie priloženom obrázku, samozrejme jednotlivé nastavenia je možné neskôr upraviť priamo v module.



Obr. 36 - sprievodca nastavení ADS modulu

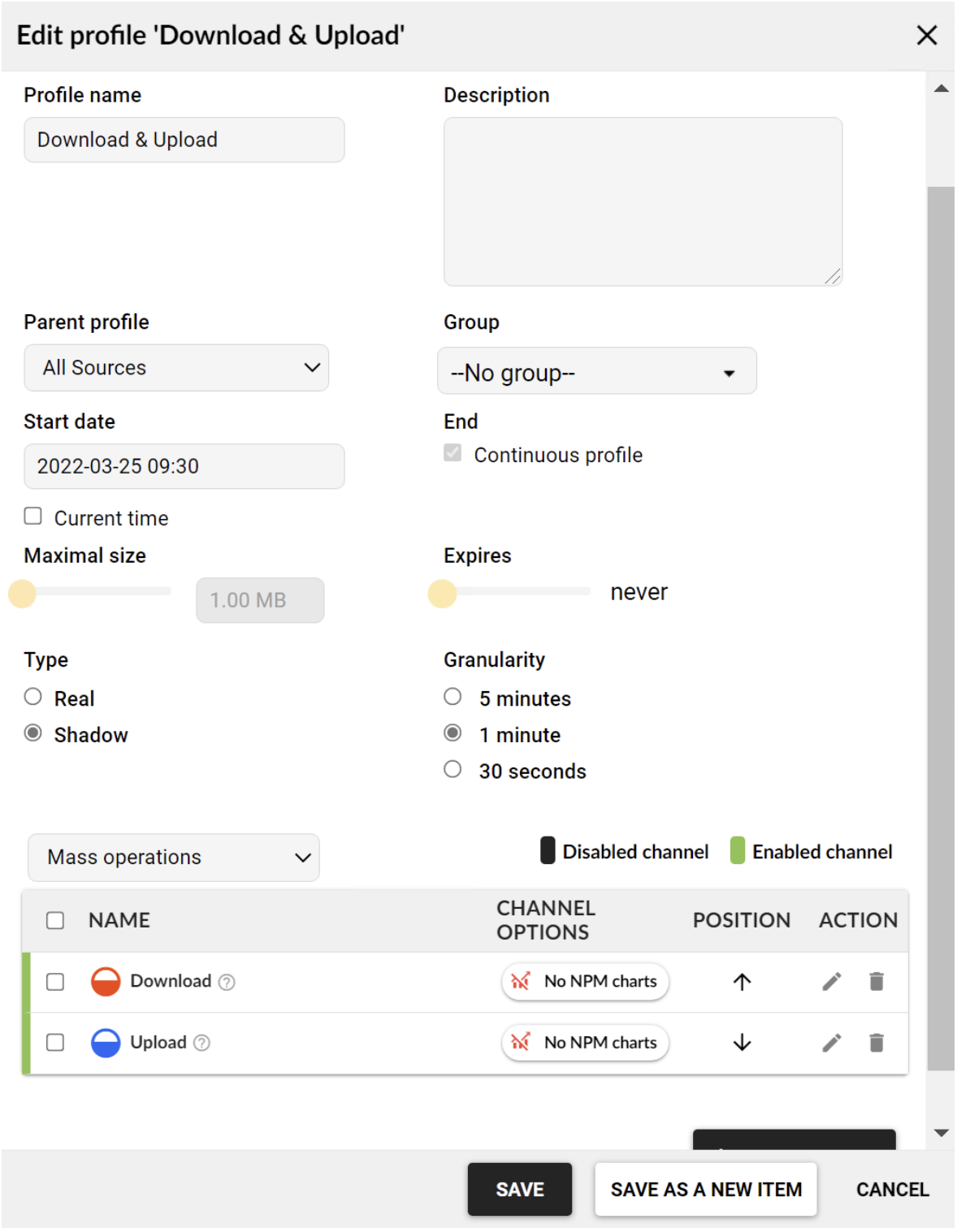
Ďalšie veľmi dôležité nastavenie v module ADS predstavujú metódy detekcie. V tejto časti je možné zapnúť, alebo vypnúť metódy detekcie, ktoré modul ADS ponúka. Je vhodné mať zapnuté naozaj len tie metódy, ktoré sú zaujímavé pre danú počítačovú sieť. Neodporúča sa mať zapnuté všetky detekčne metódy z dôvodu zvýšenia záťaže ADS modulu, ale hlavne zvýšeniu počtu detegovaných udalostí, čim môže byť znížená orientácia v module ADS. Flowmon užívateľská príručka má veľmi podrobne popísane jednotlivé metódy detekcie, kde je uvedený popis metódy, jej konfigurácia a taktiež aj interpretácia výsledkov - čo daná metóda prakticky znázorňuje. V prípade posudzovanej firemnej sieti je napr. vypnutá metóda Broken sensor (Obr. 40). Táto metóda je určená na monitorovanie aktívnych senzorov v prostrediach ako IoT alebo Supervisory control and data acquisition (SCADA), čiže v tomto prípade nie je táto metóda potrebná.



Obr. 37 - detekčné metódy v module ADS

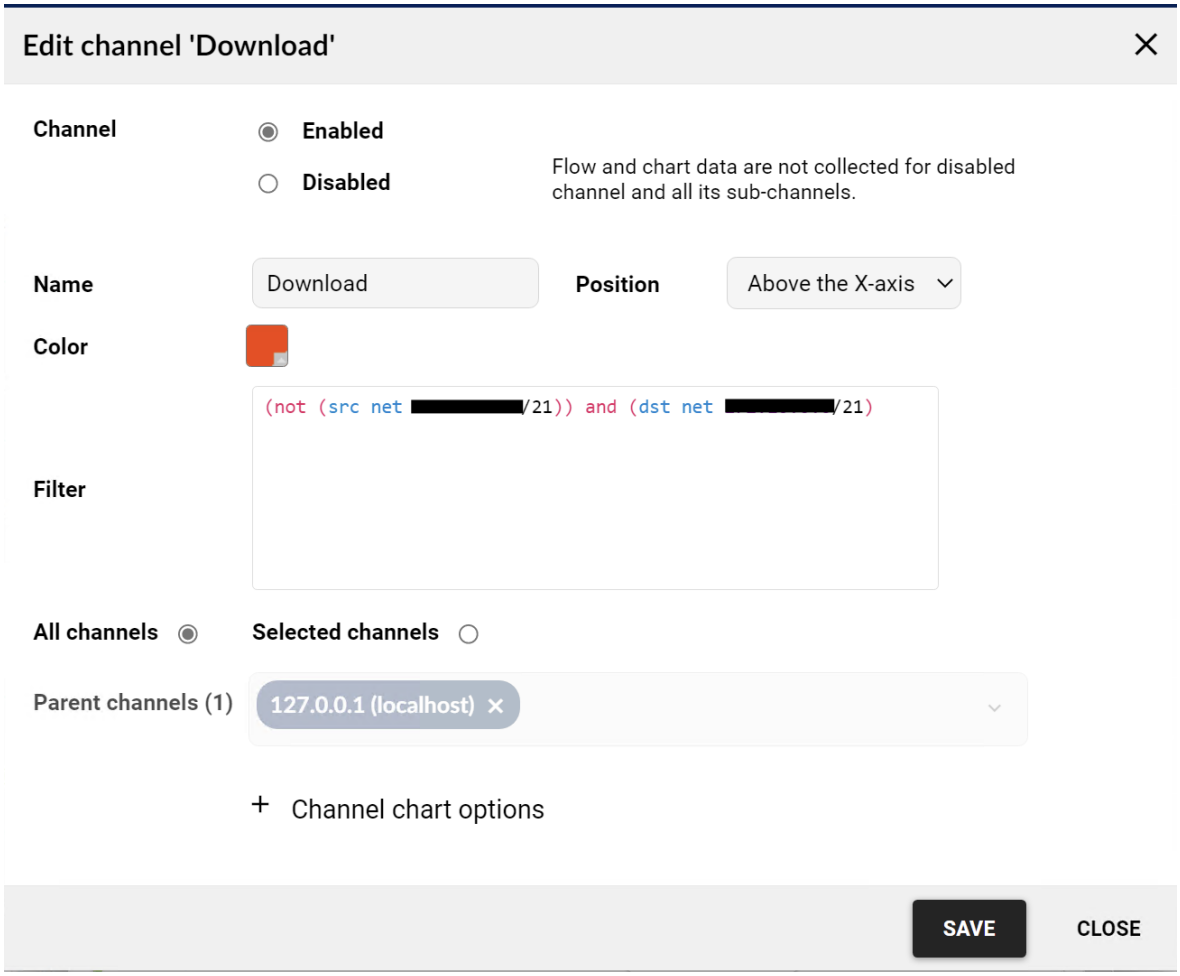
6.5 Vytvorenie vlastného profilu

V monitorovanej sieti správca chce byť schopný vidieť, aké veľké množstvo dát je prenášaných sieťou (download a upload). Za týmto účelom je vytvorený vlastný profil, ktorý zobrazuje len download a upload do alebo z Internetu. V module FMC v sekcii profiles je pridaný nový profil. Typ profilu je shadow, čo znamená, že sa nezhromažďujú žiadne údaje o flows, a preto sa šetrí miesto na disku. Tento typ profilu pristupuje k údajom svojho nadradeného profilu pri procese spracovania údajov. Na Obr. 37 je možné vidieť jednotlivé nastavenia profilu.



Obr. 38 - nastavenia profilu

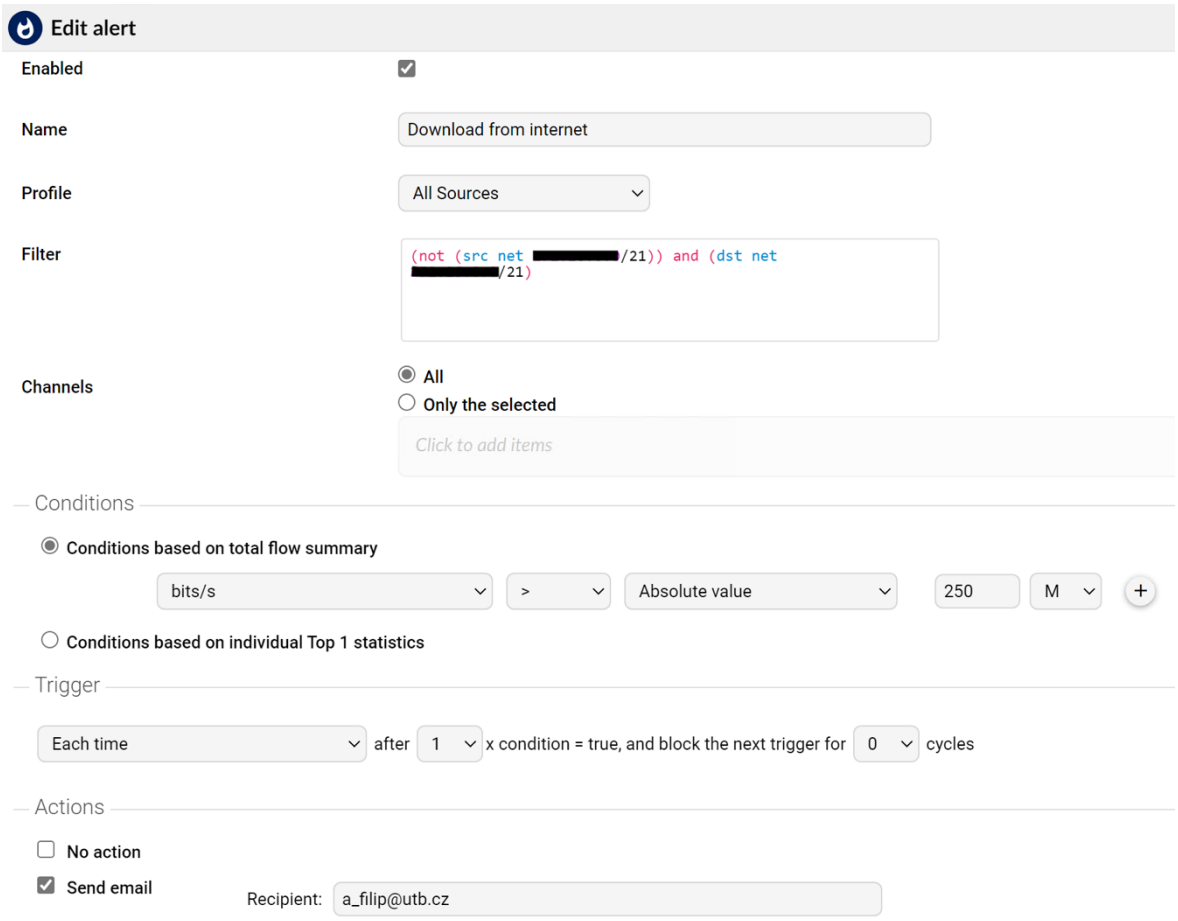
Na nižšie priloženom obrázku je vidieť nastavenia pre konkrétny kanál. Je tu zadefinovaná podmienka vo filtri, ktorá filtruje komunikáciu na základe zdrojovej a cieľovej siete. Obdobné nastavenia sú aj pre kanál upload, kde je zmenené poradie zdrojovej a cieľovej siete vo filtri.



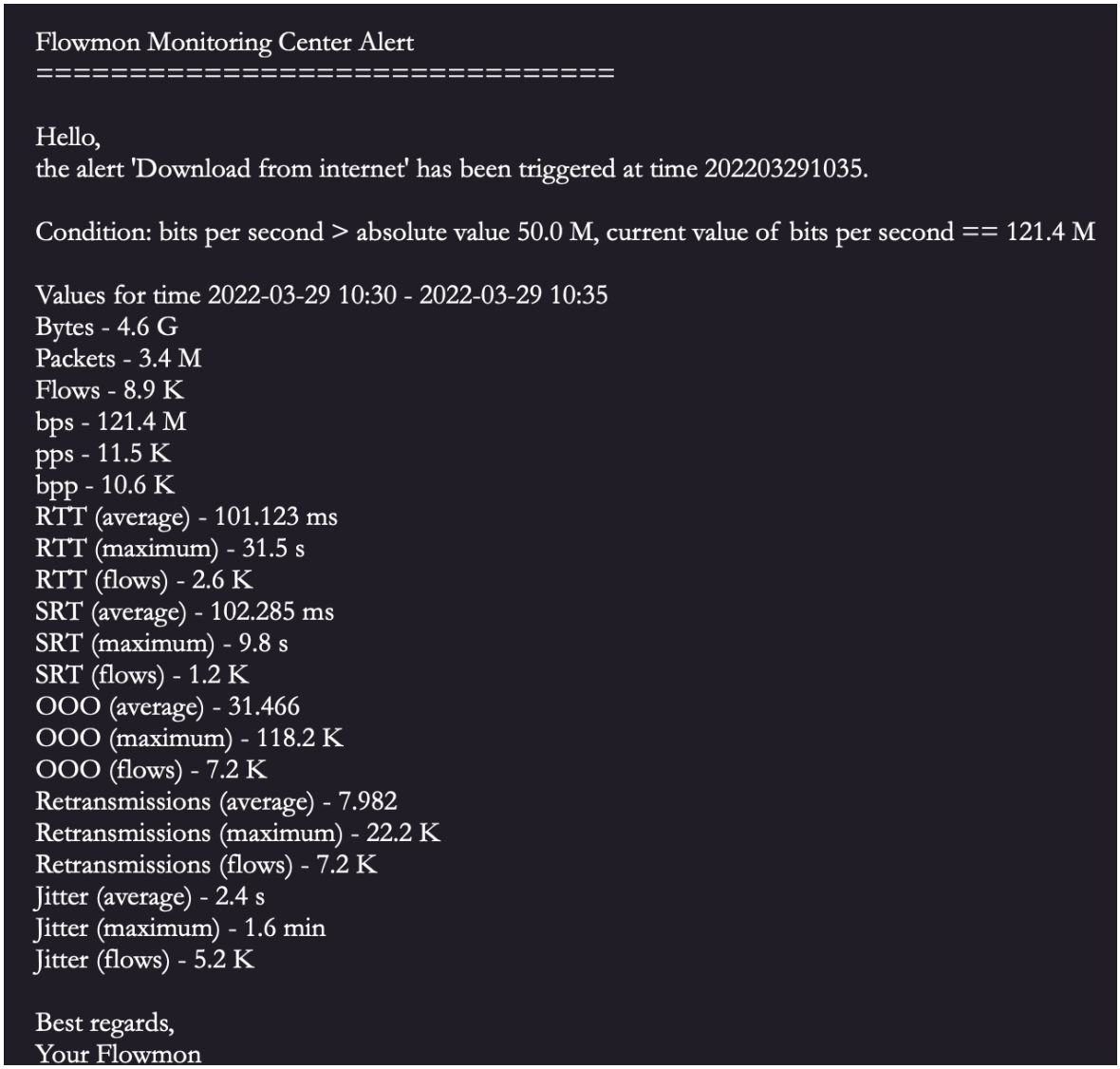
Obr. 39 - nastavenie kanálu - download

6.6 Alerting - triggers

Ďalšia z požiadaviek lokálneho správcu siete v danej firme je automatické upozorňovanie vždy, keď bude sieť vyťažená vysokým downloadom alebo uploadom, do alebo z Internetu. Takýto alert je možné nastaviť v základom module FMC a pomocou filtru definovať podmienku. Vo filtre je definovaná zdrojová a cieľová sieť tak, aby alert bol spustený len vtedy, keď ide o download alebo upload smerom z alebo do Internetu (nie v rámci lokálnej siete). Ako už bolo spomenuté, firma je pripojená prostredníctvom ISP do Internetu rýchlosťou 500/100 Mbps. Povedzme, že je žiadúce, aby alert bol odoslaný vždy, keď je celková kapacita pripojenia prekročená nad 50 %, čiže 250 Mbps pre download a 50 Mbps pre upload. Na nižšie priloženom obrázku je vidno nastavenia alertu pre download v sieti. Alert na upload má nastavenia obdobné, rozdiel je len v hodnote, ktorá je definovaná v bits/s a taktiež úprave filtra. Na Obr. 42 je možné vidieť prijatý email po prekročení danej hodnoty.



Obr. 40 - nastavenia alertu - download



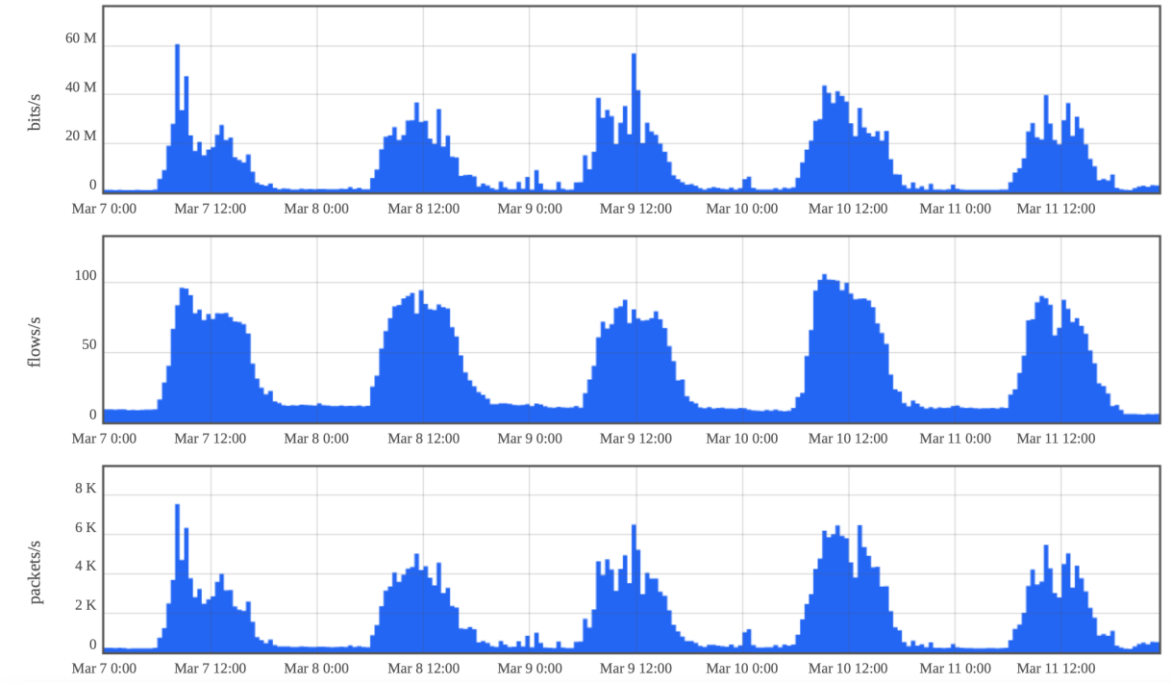
Obr. 41 - prijatý email po spustení alertu

7 ANALÝZA SIEŤOVEJ KOMUNIKÁCIE

Táto kapitola sa zaoberá analýzou sieťovej komunikácie v monitorovanej firemnej sieti. V prvej podkapitole je popísaná štruktúra komunikácie a sú vysvetlené základné vzťahy medzi jednotlivými ukazovateľmi. Následne sú uvedené štatistiky za dané obdobie z pohľadu najviac využívaných TCP a UDP služieb, štatistika užívateľov, ktorý odoslali alebo prijali najväčší objem dát, alebo sú uvedené najčastejšie navštevované webové stránky. V ďalšej podkapitole sú uvedené výsledky z modulu ADS na detekciu anomálii a sú hlbšie popísané a rozobraté 2 anomálie (jedna z oblasti prevádzkyschopnosti siete a jedna z pohľadu bezpečnosti siete). V závere tejto kapitoly sú uvedené možnosti vizualizácie dát pomocou dashboardu a je uvedený príklad používania definovaných profilov v module FMC.

7.1 Štruktúra komunikácie

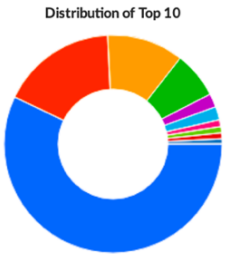
V tejto podkapitole je popísaná celková štruktúra sieťovej komunikácie v sledovanej sieti a zobrazené základne štatistiky. Štatistiky sú z časového intervalu 2022-03-07 00:00 — 2022-03-11 23:00, čo predstavuje pracovné dni pondelok až piatok. Ako je možné vidieť na nižšie priloženom obrázku, jednotlivé grafy sú približne rovnaké. V prípade, že by počet packetov výrazne prevyšoval prvý graf (celková sieťová komunikácia), tak to indikuje, že v sieti nejaké zariadenie generuje packety, ktoré nemajú žiaden alebo len veľmi malý payload. V prípade, že by graf flows bol nadmerne zvýšený v porovnaní s celkovou sieťovou komunikáciou, mohlo by to indikovať podozrenie na nejaký slovníkový útok v sieti (veľké množstvo nadviazaných spojení a veľmi malí objem dát).



Obr. 42 - štruktúra celkovej komunikácie

Najčastejšie používané sieťové služby cez TCP

Na nižšie priloženom obrázku sú uvedené TCP sieťové služby, ktoré predstavujú najväčší podiel dát prenesených v monitorovanej sieti. Služby používajúce známe porty sú označené príslušným názvom služby. Služby s dynamicky priradenými portami sú označené číselnou hodnotou.

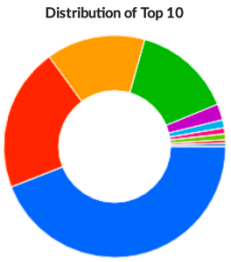


	PORT	PROTOCOL	INPUT BYTES
1	https	6	224.84 GB(60.4%)
2	http	6	67.37 GB(18.1%)
3	ms-sql-s	6	44.73 GB(12.0%)
4	imaps	6	27.07 GB(7.3%)
5	63041	6	8.01 GB(2.2%)
6	52133	6	7.63 GB(2.1%)
7	50361	6	4.12 GB(1.1%)
8	49671	6	3.57 GB(1.0%)
9	57640	6	3.50 GB(0.9%)
10	51618	6	2.97 GB(0.8%)
	Excluded		**0**
	Total		**372.11 GB**

Obr. 43 - najčastejšie používané sieťové služby cez TCP

Najčastejšie používané sieťové služby cez UDP

Nižšie je možné vidieť sieťové služby zistené v monitorovanej sieti využívajúce protokol UDP. Rovnako ako pri protokole TCP, k známym portom je pridelené meno služby a pri dynamických portoch je uvedená numerická hodnota. Niektoré neznáme porty je možné dohľadať na Internete, napr. port 19305 používajú aplikácie ako Google Talk, DUO alebo Hangouts.

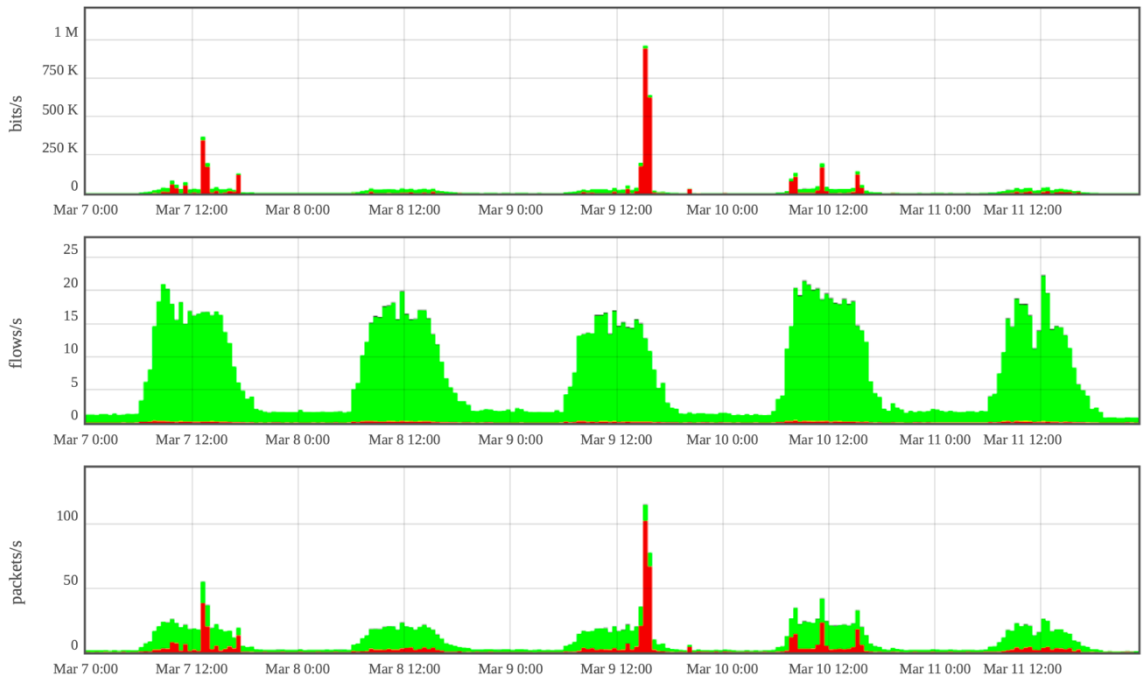


	PORT	PROTOCOL	INPUT BYTES
1	https	17	106.58 GB(49.8%)
2	19305	17	50.62 GB(23.7%)
3	57450	17	34.88 GB(16.3%)
4	8234	17	34.88 GB(16.3%)
5	plethora	17	5.68 GB(2.7%)
6	ipsec-nat-t	17	2.76 GB(1.3%)
7	19321	17	2.17 GB(1.0%)
8	52810	17	2.08 GB(1.0%)
9	52099	17	1.19 GB(0.6%)
10	57636	17	1.14 GB(0.5%)
	Excluded		**0**
	Total		**213.89 GB**

Obr. 44 - najčastejšie používané sieťové služby cez UDP

Prehľad služieb v sieti

Na nižšie priloženom obrázku je možné vidieť štruktúru služieb v sieti. Sieťová komunikácia je zobrazená v bitoch, packetoch a flows za sekundu. Grafy by mali mať periodickú charakteristiku, každá anomália alebo neočakávaná špička by mala byť podrobnejšie analyzovaná pomocou modulu FMC.

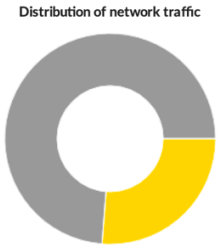


	SERVICE	MAXIMAL BITS/S	BITS PER SECOND	INPUT PACKETS	MAXIMAL PACKETS/S	PACKETS PER SECOND	INPUT FLOWS	MAXIMAL FLOWS/S	FLOWS/S	INPUT BYTES
1	smb	1.86 Mb/s	14.78 kb/s	1.09 M(25.2%)	201.55	2.54	44.15 k(1.4%)	0.53	0.10	754.65 MB(58.5%)
2	dns	34.79 kb/s	10.22 kb/s	3.18 M(73.5%)	28.40	7.43	3.14 M(97.8%)	28.28	7.34	521.76 MB(40.5%)
3	dhcp	1.09 kb/s	179.72 b/s	29.12 k(0.7%)	0.42	0.07	15.40 k(0.5%)	0.18	0.04	9.18 MB(0.7%)
4	snmp	667.89 b/s	80.62 b/s	29.25 k(0.7%)	0.68	0.07	12.78 k(0.4%)	0.19	0.03	4.12 MB(0.3%)
5	smtp	56.37 b/s	0.04b/s	38 (0.0%)	0.11	0.00	5 (0.0%)	0.01	0.00	2.32 kB(0.0%)
6	snmp_trap	0 b/s	0 b/s	0(0.0%)	0	0	0(0.0%)	0	0	0 B(0.0%)
7	telnet	0 b/s	0 b/s	0(0.0%)	0	0	0(0.0%)	0	0	0 B(0.0%)
	Total	**1.88 Mb/s**	**25.25 kb/s**	**4.33 M**	**213.74**	**10.11**	**3.21 M**	**28.68**	**7.50**	**1.26 GB**

Obr. 45 - služby v monitorovanej sieti

Používatelia s najvyšším objemom odoslaných dát v sieti

V tejto časti sú zhrnuté stanice s najväčším objemom odoslaných dát v monitorovanej sieti. Zobrazené stanice sú zodpovedné za najväčšie zaťaženie vnútornej infraštruktúry. V tomto zozname by sa mali byť najmä dôležité dátové servery. Ak sa tu nachádzajú aj používateľské stanice, je odporúčané vykonať kontrolu týchto staníc a hlbšie analyzovať sieťovú komunikáciu. Koláčový graf vľavo zobrazuje percentuálne rozloženie komunikácie medzi TOP 10 stanicami. Graf vpravo porovnáva prenesený objem TOP 10 staníc v kontraste s celkovým objemom dát v sieti.

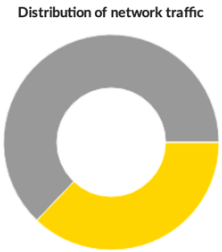


	SOURCE IP ADDRESS	BITS PER SECOND	INPUT BYTES
1	[redacted]1.5	673.84 kb/s	34.93 GB(6.0%)
2	68.232.34.200	788.76 kb/s	21.71 GB(3.7%)
3	[redacted]201.251	594.84 kb/s	15.08 GB(2.6%)
4	video-edge-87b076.prg03.justin.tv	6.04 Mb/s	14.79 GB(2.5%)
5	[redacted].static.masterinter.net	733.35 kb/s	13.63 GB(2.3%)
6	74.125.250.81	1.15 Mb/s	12.75 GB(2.2%)
7	193.85.19.195	274.60 kb/s	12.40 GB(2.1%)
8	[redacted].3.99	183.83 kb/s	9.88 GB(1.7%)
9	93.184.220.29	218.50 kb/s	9.59 GB(1.6%)
10	cache.google.com	584.24 kb/s	8.90 GB(1.5%)
	TOP 10	**3.08 Mb/s**	**153.67 GB**
	Excluded	**0**	**0**
	Rest	**8.67 Mb/s**	**432.49 GB**
	Total	**11.75 Mb/s**	**586.16 GB**

Obr. 46 - užívatelia s najvyšším objemom odoslaných dát

Používatelia s najvyšším objemom prijatých dát v sieti

V tejto časti sú zhrnuté stanice s najvyšším objemom sťahovania z Internetu.

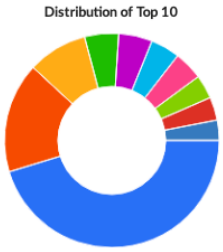


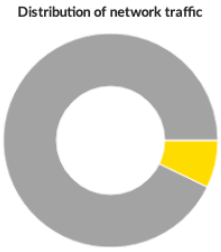
	DESTINATION IP ADDRESS	BITS PER SECOND	INPUT BYTES
1	[redacted].2.1	1.57 Mb/s	66.23 GB(11.3%)
2	[redacted].1.76	673.91 kb/s	34.93 GB(6.0%)
3	[redacted].3.49	1.03 Mb/s	22.03 GB(3.8%)
4	[redacted].3.193	366.96 kb/s	19.11 GB(3.3%)
5	[redacted].2.112	579.74 kb/s	15.33 GB(2.6%)
6	[redacted]2.148	733.33 kb/s	14.94 GB(2.5%)
7	[redacted]3.99	214.30 kb/s	11.52 GB(2.0%)
8	[redacted]2.50	227.68 kb/s	11.19 GB(1.9%)
9	74.125.250.81	1.01 Mb/s	11.18 GB(1.9%)
10	prg03s01-in-f14.1e100.net	237.36 kb/s	11.06 GB(1.9%)
	TOP 10	**4.36 Mb/s**	**217.53 GB**
	Excluded	**0**	**0**
	Rest	**7.39 Mb/s**	**368.63 GB**
	Total	**11.75 Mb/s**	**586.16 GB**

Obr. 47 - užívatelia s najvyšším objemom prijatých dát

Najnavštevovanejšie webové stránky

Na nižšie priloženom obrázku je možne vidieť najpoužívanejšie webové stránky v monitorovanej sieti. Zobrazené štatistiky sumarizujú množstvo údajov, ktoré boli z týchto staníc prenesené pomocou protokolu Hypertext Transfer Protocol (HTTP).





	HTTP HOSTNAME	INPUT BYTES	FLOWS
1	atson.events.data.microsoft.com	3.19 GB(0.5%)	530.55 k(3.2%)
2	bitbucket.org	2.53 GB(0.4%)	194.97 k(1.2%)
3	api.bitbucket.org	304.83 MB(0.1%)	105.57 k(0.6%)
4	po[redacted]cz	2.16 GB(0.4%)	59.96 k(0.4%)
5	help[redacted].cz	1.48 GB(0.3%)	59.39 k(0.4%)
6	v10.events.data.microsoft.com	243.51 MB(0.0%)	51.69 k(0.3%)
7	fcmconnection.googleapis.com	67.46 MB(0.0%)	51.19 k(0.3%)
8	wss-primary.slack.com	246.76 MB(0.0%)	42.07 k(0.3%)
9	www.googleapis.com	533.31 MB(0.1%)	40.99 k(0.3%)
10	mail.google.com	1.07 GB(0.2%)	35.70 k(0.2%)
	TOP 10	**11.79 GB**	**1.17 M**
	Excluded	**0**	**0**
	Rest	**574.37 GB**	**15.19 M**
	Total	**586.16 GB**	**16.36 M**

Obr. 48 - najnavštevovanejšie webové stránky

Najnavštevovanejšie webové servery

Na nižšie priloženom obrázku sú zobrazené najpoužívanejšie webové servery v monitorovanej sieti. Zobrazené štatistiky sumarizujú množstvo údajov, ktoré boli prenesené z týchto staníc na porte TCP 80 a TCP 443.

	SOURCE IP ADDRESS	INPUT BYTES
1	68.232.34.200	21.71 GB(8.1%)
2	video-edge-87b076.prg03.justin.tv	14.79 GB(5.5%)
3	93.184.220.29	9.59 GB(3.6%)
4	video-edge-87c7fe.prg03.justin.tv	7.39 GB(2.8%)
5	vip0x008.map2.ssl.hwcdn.net	5.23 GB(2.0%)
6	37.218.242.151	4.85 GB(1.8%)
7	[redacted]19.216	4.72 GB(1.8%)
8	a92-122-48-27.deploy.static.akamaitechnologies.com	4.29 GB(1.6%)
9	https-178-79-227-0.vie.llnw.net	3.83 GB(1.4%)
10	https-178-79-227-128.vie.llnw.net	3.43 GB(1.3%)
	TOP 10	**79.83 GB**
	Excluded	**0**
	Rest	**186.81 GB**
	Total	**266.65 GB**

Obr. 49 - najnavštevovanejšie webové servery

Top klienti webových serverov

Najaktívnejší klienti, ktorí komunikovali na TCP portoch 80 a 443 s webovými servermi.

	DESTINATION IP ADDRESS	INPUT BYTES
1	[redacted]2.1	49.22 GB(18.5%)
2	[redacted].3.49	9.39 GB(3.5%)
3	[redacted]4.149	8.97 GB(3.4%)
4	[redacted]2.50	8.73 GB(3.3%)
5	[redacted]3.175	7.55 GB(2.8%)
6	[redacted]3.99	7.36 GB(2.8%)
7	[redacted]4.125	7.15 GB(2.7%)
8	[redacted]4.231	5.85 GB(2.2%)
9	[redacted]1.25	5.38 GB(2.0%)
10	[redacted]2.33	4.99 GB(1.9%)
	TOP 10	114.59 GB
	Excluded	0
	Rest	152.05 GB
	Total	266.65 GB

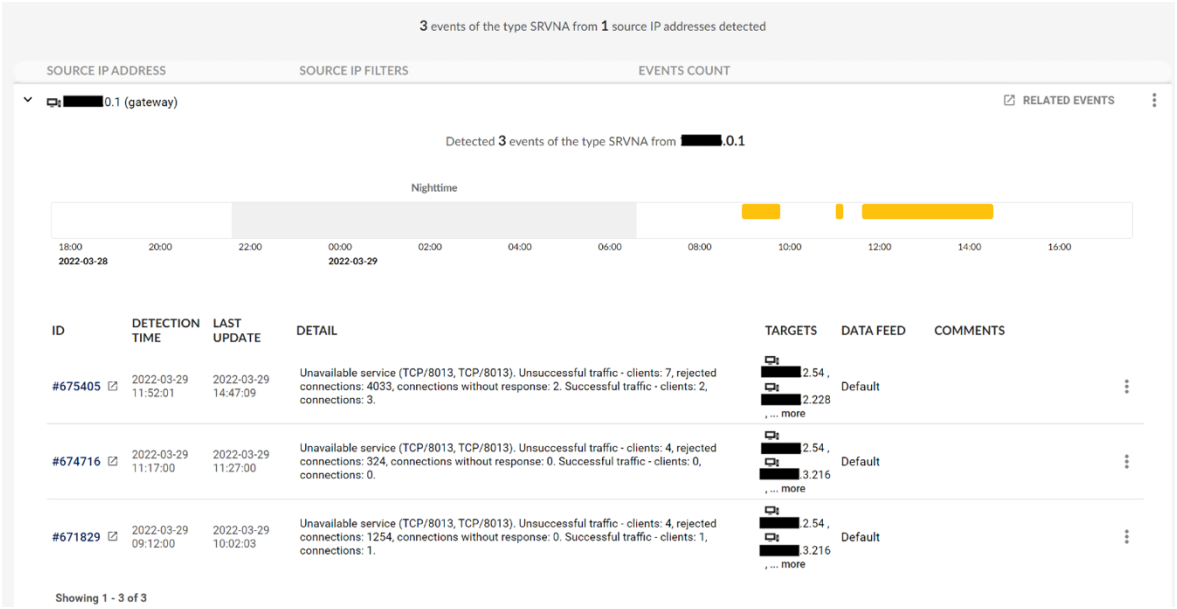
Obr. 50 - klienti webových serverov

7.2 Detekcia anomálii

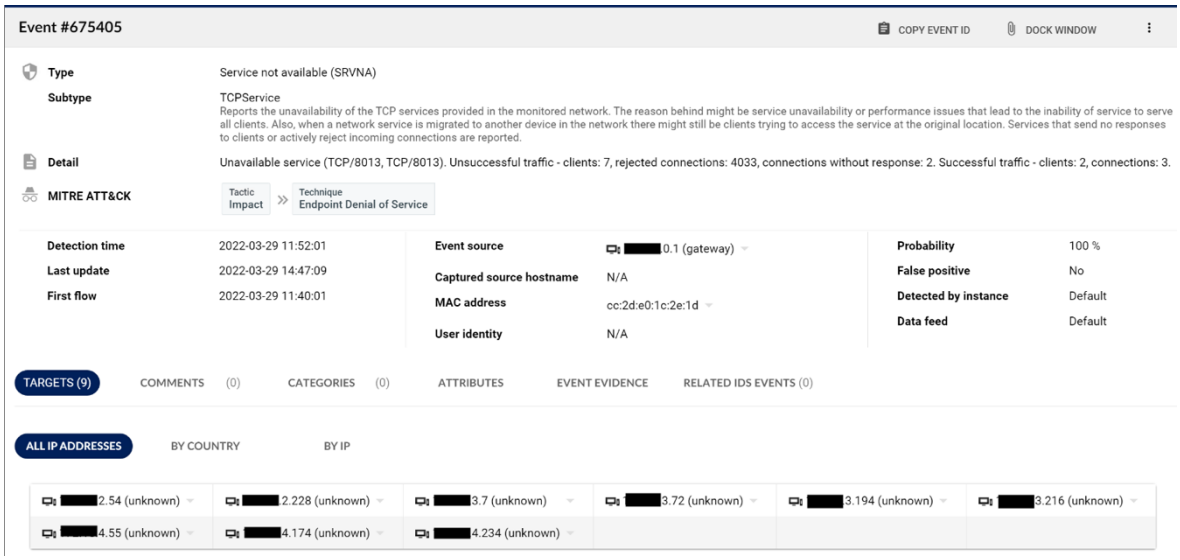
V module ADS je možné prechádzať medzi jednotlivými detegovanými anomáliami na základe povolených metód v nastaveniach ADS. Jednotlivé udalosti je možné zobraziť podľa priorít (kritická, vysoká, stredná, nízka, informačná), alebo priamo podľa konkrétnych detekčných metód. Ďalej je možné jednotlivé udalosti rozdeliť podľa perspektívy, a to na udalosti zaoberajúce sa bezpečnosťou alebo prevádzkyschopnosťou siete. Na nižšie priloženom obrázku je možné vidieť príklad detekčnej metódy SRVNA (service not available), ktorá je súčasťou perspektívy zaoberajúca sa prevádzkyschopnosti siete.

Obr. 51 - detekčná metóda SRVNA

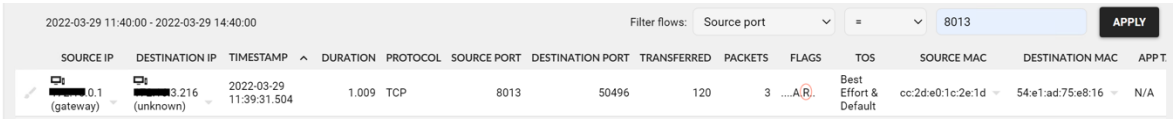
Po otvorení udalosti SRVNA je možné na nižšie priloženom Obr. 53 vidieť jednotlivé udalosti aj s prideleným poradovým ID. Všetky tieto 3 udalosti sa vzťahujú na spomenutú metódu a rovnakú zdrojovú IP adresu. Na Obr. 54 je možné vidieť konkrétne detaily udalosti s ID 675405. Ide o udalosť, ktorá hlasí nedostupnosť služieb na porte TCP 8013 smerom do Internetu. Je možné konštatovať, že určité stanice z lokálnej LAN siete sa snažia komunikovať na porte TCP 8013 smerom do Internetu a hraničný router túto komunikáciu zamieta. V časti Event Evidence (Obr. 55) je možno vidieť priamo do jednotlivých zachytených flows kde je vidno, že komunikácia zo strany routra končí vždy s TCP značkou (flag) R, čo predstavuje reset, inými slovami terminovanie TCP spojenia. Bolo zistené, že tento port využíva program FortiClient, a preto je vhodné overiť jednotlivé lokálne stanice a nastavenia tohoto programu a v prípade potreby vykonať potrebné zmeny v nastaveniach na hraničnom routri.



Obr. 52 - detekčná metóda SRVNA - všetky udalosti

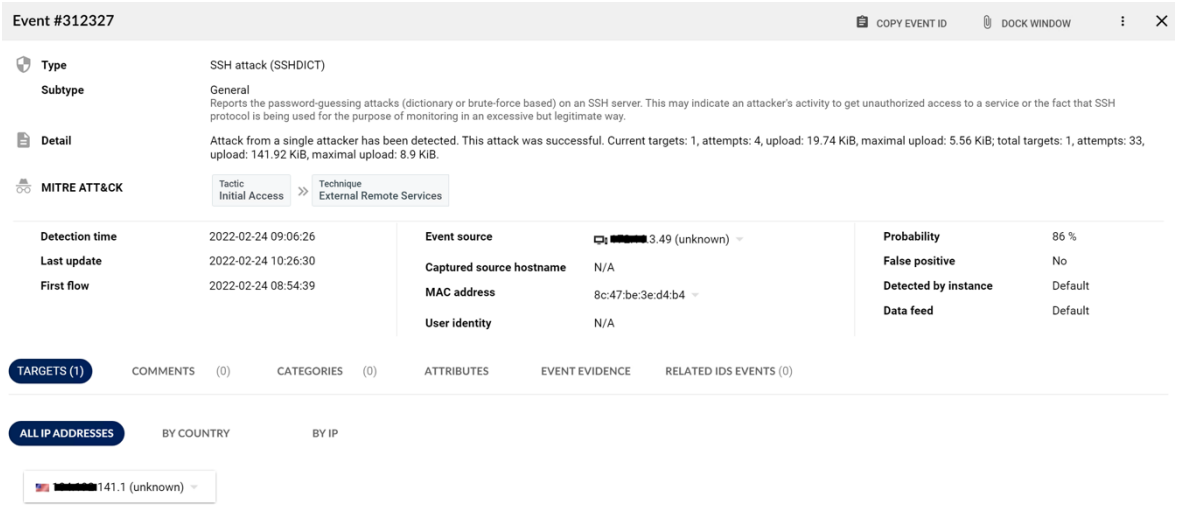


Obr. 53 - detekčná metóda SRVNA - detail konkrétnej udalosti



Obr. 54 - detekčná metóda SRVNA - event evidence

Čo sa týka metód, ktoré sa sústredia na bezpečnosť siete je vhodné spomenúť napr. SSHDICT (SSH attack), ktorý sa objavil v monitorovanej sieti, ale v konečnom dôsledku sa nejednalo o reálny útok. Obdobne ako pri prvom príklade je zvolený filter len na kritické udalosti. Ako je možné vidieť na obrázku nižšie, pravdepodobnosť (probability) nie je 100%, čo znamená, že nemusí v skutočnosti ísť o reálny útok.



Obr. 55 - detekčná metóda SSHDICT - prehľad udalosti

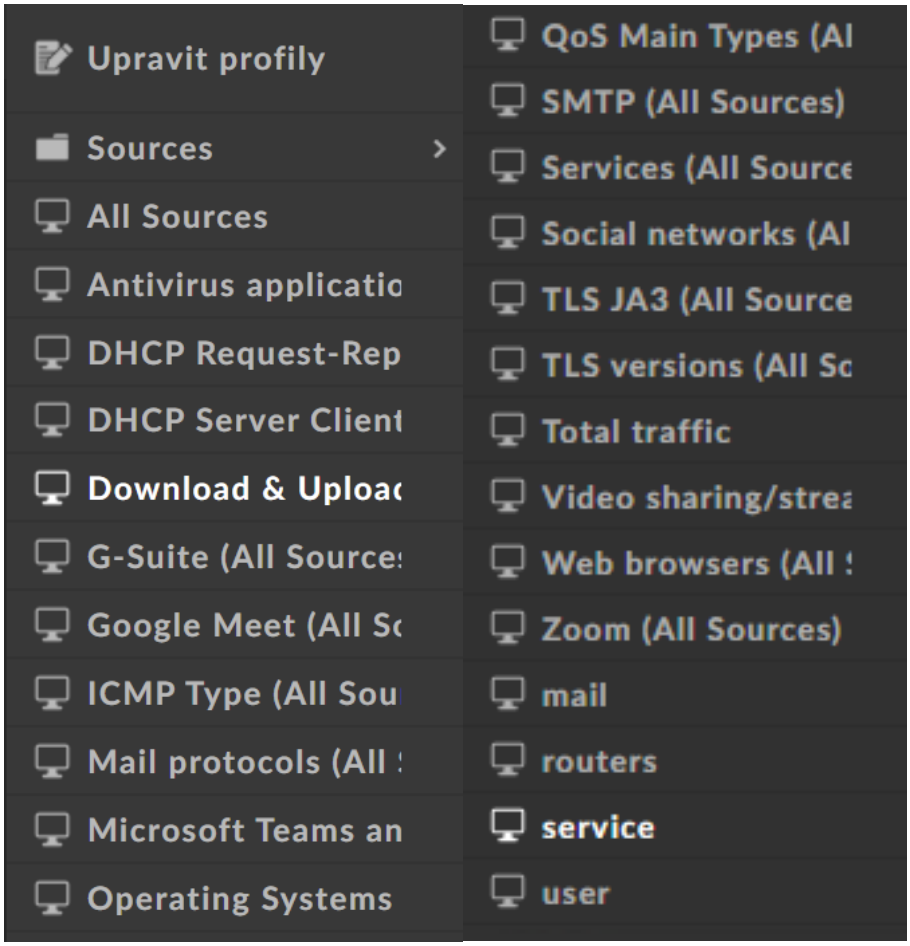
Za účelom hlbšieho pohľadu do komunikácie je potrebné investigovať jednotlivé flows v sekcii event evidence. Z event evidence je vidieť, že čas spojenia v sekundách je veľmi krátky a vo všetkých vyobrazených spojeniach je skoro rovnaký. Tento čas 1,5 sekundy nekorešponduje s používaním protokolu SSH reálnym používateľom (človekom), pretože čas je príliš krátky. Je možné predpokladať na základe času, že sa jedná o nejaký skript, ktorý sa v pravidelných intervaloch pripája na americký server pomocou SSH protokolu. Ako naznačujú vypísane flags v komunikácií, ide o úplne korektné SSH spojenie, pretože komunikácia neobsahuje flag R (reset) ale je vždy na začiatku A (acknowledgment) a ukončovací flag F (finish). Táto udalosť bola detegovaná danou metódou z dôvodu periodicity nadviazania spojení (približne každých 5 sekúnd), a taktiež veľmi krátkej doby jednotlivých spojení. Tieto dva faktory sú typickým znakom pre slovníkové útoky. Je vhodné vykonať kontrolu danej lokálnej stanice a preveriť, či naozaj využíva takýto skript. V prípade, že táto komunikácia je legitímna, je možné túto udalosť označiť ako false positive, čiže ADS modul už nebude detegovať túto anomáliu na danej zdrojovej a cieľovej IP adrese.

SOURCE IP	DESTINATION IP	TIMESTAMP	DURATION	PROTOCOL	SOURCE PORT	DESTINATION PORT	TRANSFERRED	PACKETS	FLAGS	TOS	SOURCE MAC	DESTINATION MAC
[redacted].3.49 (unknown)	[redacted]141.1 (unknown)	2022-02-24 08:54:39.031	1.474	TCP	61749	22	4549	24	....AP.SF	Best Effort & Default	8c:47:be:3e:d4:b4	cc:2d:e0:1c:2e:1d
[redacted]141.1 (unknown)	[redacted].3.49 (unknown)	2022-02-24 08:54:39.036	1.469	TCP	22	61749	4296	33	....AP.SF	Best Effort & Default	cc:2d:e0:1c:2e:1d	8c:47:be:3e:d4:b4
[redacted].3.49 (unknown)	[redacted]141.1 (unknown)	2022-02-24 08:54:40.644	1.525	TCP	61752	22	4917	33	....AP.SF	Best Effort & Default	8c:47:be:3e:d4:b4	cc:2d:e0:1c:2e:1d
[redacted]141.1 (unknown)	[redacted].3.49 (unknown)	2022-02-24 08:54:40.650	1.519	TCP	22	61752	6576	50	....AP.SF	Best Effort & Default	cc:2d:e0:1c:2e:1d	8c:47:be:3e:d4:b4
[redacted].3.49 (unknown)	[redacted].141.1 (unknown)	2022-02-24 08:54:44.331	1.507	TCP	61755	22	4853	32	....AP.SF	Best Effort & Default	8c:47:be:3e:d4:b4	cc:2d:e0:1c:2e:1d
[redacted].141.1 (unknown)	[redacted]3.49 (unknown)	2022-02-24 08:54:44.336	1.501	TCP	22	61755	8548	48	....AP.SF	Best Effort & Default	cc:2d:e0:1c:2e:1d	8c:47:be:3e:d4:b4
[redacted]3.49 (unknown)	[redacted].141.1 (unknown)	2022-02-24 08:54:45.973	1.646	TCP	61758	22	5533	49	....AP.SF	Best Effort & Default	8c:47:be:3e:d4:b4	cc:2d:e0:1c:2e:1d
[redacted].141.1 (unknown)	[redacted].3.49 (unknown)	2022-02-24 08:54:45.979	1.640	TCP	22	61758	16348	82	....AP.SF	Best Effort & Default	cc:2d:e0:1c:2e:1d	8c:47:be:3e:d4:b4

Obr. 56 - detekčná metóda SSHDICT - event evidence

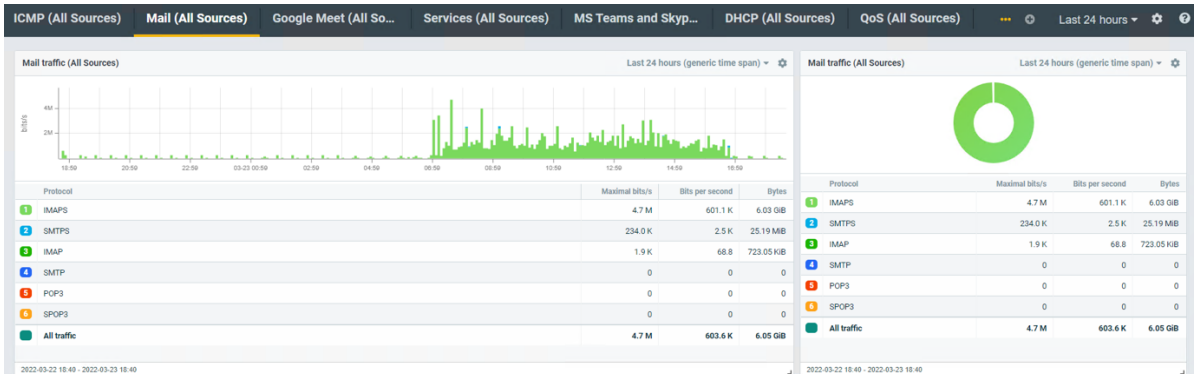
7.3 Reportovanie

Nástroj Flowmon ponúka široké možnosti v oblasti vizualizácie a reportovania zozbieraných dát a metrík. Ako už bolo uvedené v predošlej kapitole, pri konfigurácií boli využité presety, ktoré automaticky vytvoria profily v module FMC. Na nižšie priloženom obrázku je možne vidieť vytvorené profily.

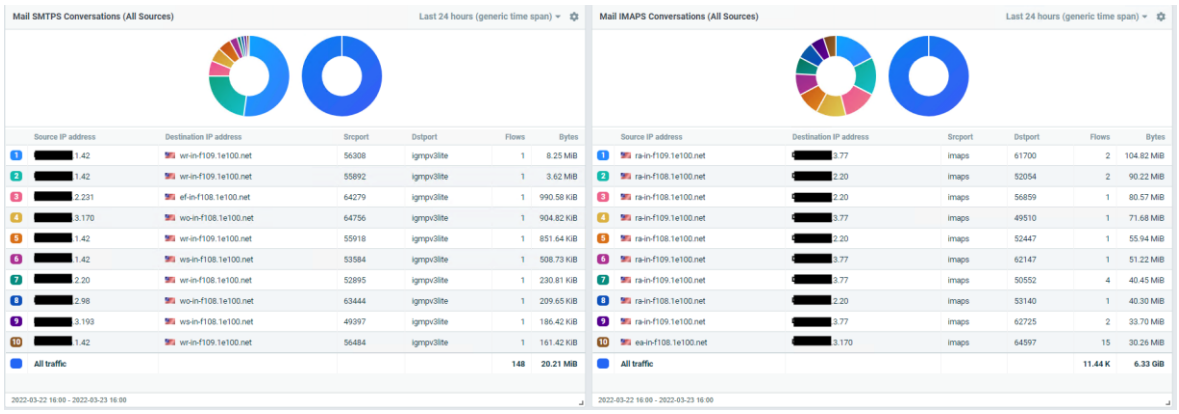


Obr. 57 - profily v module FMC

Tieto profily automaticky vytvárajú aj sekcie v časti dashboard, kde sú prednastavené nástenky s widgetami. Jednotlivé dashboardy je možné upravovať podľa potreby, alebo vytvoriť vlastné. Príklad dashboardu, ktorý poskytuje informácie o poštových protokolov v monitorovanej sieti je možné vidieť na Obr. 59 a Obr. 60.

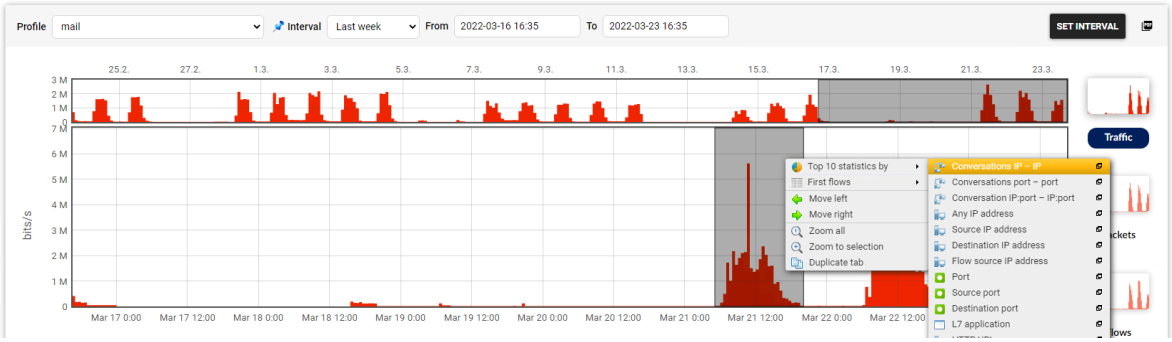


Obr. 58 - dashboard - emailová komunikácia



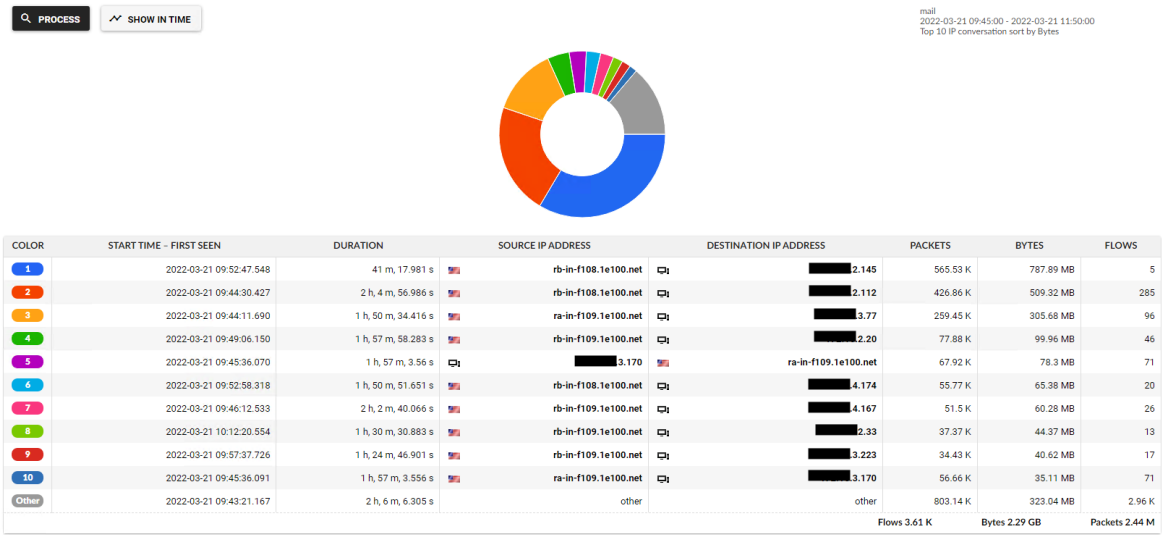
Obr. 59 - dashboard - emailová komunikácia II.

V module FMC je možné využiť rovnaký profil za účelom hlbšej investigácie komunikácie. Na nižšie priloženom obrázku je možné vidieť nárast objemu komunikácie prostredníctvom Internet Message Access Protocol Secure (IMAPS) protokolu. Ak je potrebné identifikovať užívateľa, ktorý stojí za touto komunikáciou, je možné na vybranom časovom úseku zobraziť štatistiku na základe konverzie IP k IP (Obr. 61).



Obr. 60 - filtrovanie komunikácie v module FMC

Následne je vytvorená štatistika, ktorá obsahuje informácie o zdrojovej a cieľovej IP, počet packetov, bytov a jednotlivých flows. Nižšie priložený obrázok ukazuje, že najväčší objem dát prostredníctvom protokolu IMAPS (TCP a UDP port 993) bolo stiahnutých užívateľmi s IP adresami x.x.2.145 a x.x.2.112. Po následnom hľadaní dostupných informácii o adrese, ktorá je uvedená ako zdrojová IP, bolo zistené že patrí spoločnosti Google [31].



COLOR	START TIME - FIRST SEEN	DURATION	SOURCE IP ADDRESS	DESTINATION IP ADDRESS	PACKETS	BYTES	FLOWS
1	2022-03-21 09:52:47.548	41 m, 17.981 s	rb-in-f108.1e100.net	[redacted]2.145	565.53 K	787.89 MB	5
2	2022-03-21 09:44:30.427	2 h, 4 m, 56.986 s	rb-in-f108.1e100.net	[redacted]2.112	426.86 K	509.32 MB	285
3	2022-03-21 09:44:11.690	1 h, 50 m, 34.416 s	ra-in-f109.1e100.net	[redacted]3.77	259.45 K	305.68 MB	96
4	2022-03-21 09:49:06.150	1 h, 57 m, 58.283 s	rb-in-f109.1e100.net	[redacted]2.20	77.88 K	99.96 MB	46
5	2022-03-21 09:45:36.070	1 h, 57 m, 3.56 s	[redacted]3.170	ra-in-f109.1e100.net	67.92 K	78.3 MB	71
6	2022-03-21 09:52:58.318	1 h, 50 m, 51.651 s	rb-in-f108.1e100.net	[redacted]4.174	55.77 K	65.38 MB	20
7	2022-03-21 09:46:12.533	2 h, 2 m, 40.066 s	rb-in-f109.1e100.net	[redacted]4.167	51.5 K	60.28 MB	26
8	2022-03-21 10:12:20.554	1 h, 30 m, 30.883 s	rb-in-f109.1e100.net	[redacted]2.33	37.37 K	44.37 MB	13
9	2022-03-21 09:57:37.726	1 h, 24 m, 46.901 s	rb-in-f109.1e100.net	[redacted]3.223	34.43 K	40.62 MB	17
10	2022-03-21 09:45:36.091	1 h, 57 m, 3.556 s	ra-in-f109.1e100.net	[redacted]3.170	56.66 K	35.11 MB	71
Other	2022-03-21 09:43:21.167	2 h, 6 m, 6.305 s	other	other	803.14 K	323.04 MB	2.96 K
					Flows 3.61 K	Bytes 2.29 GB	Packets 2.44 M

Obr. 61 - výsledná štatistika poštovej komunikácie

ZÁVER

Hlavným cieľom tejto diplomovej práce bolo v teoretickej časti popísať možnosti v oblasti monitoringu počítačových sietí. V úvode teoretickej časti sa čitateľ zoznámil s kategorizáciou potencionálnych útočníkov. V tejto časti sú uvedené taktiež aj príklady jednotlivých typov útokov, ktoré sú typické pre danú kategóriu útočníkov. Sú popísane a hlbšie vysvetlené faktory pri posudzovaní aktív v kybernetickej bezpečnosti ako napr. threat, vulnerability, risk a mitigation. V nasledujúcej kapitole som sa venoval problematike monitorovania počítačových sietí a otázke, či je vždy je monitoring potrebný pre každú počítačovú sieť. Boli popísané princípy monitorovania s agentom alebo bez agenta a porovnané ich hlavne výhody a nevýhody. V teoretickej časti sú taktiež podrobne popísané aj protokoly, ktoré sa využívajú k monitorovaniu, a to konkrétne protokol SNMP a NetFlow. Dôraz som kládol hlavne na protokol NetFlow a jeho dostupné verzie, pretože je využitý následne v praktickej časti tejto práci. V závere teoretickej časti som porovnával tri vybrané riešenia na hĺbkový monitoring siete, ktoré využívajú strojové učenie, behaviorálne analýzy, reputačné databázy a iné pri detekcii anomálií v sietí. Všetky tri nástroje majú počiatok v Českej republike. Iné zahraničné spoločnosti neboli ochotné so mnou komunikovať a poskytnúť PoC, preto boli zvolené práve tieto tri nástroje, kde komunikácia a poskytnutie technických informácii nebolo žiaden problém.

V praktickej časti je popísaná firemná sieť a vytýčené základne požiadavky na zvolený monitorovací nástroj. Bol zvolený nástroj na monitorovanie a bezpečnosť siete od firmy Flowmon, ktorý poskytuje prehľadné užívateľské GUI rozhranie a je možné rozšírenie funkcionality pomocou rôznych modulov. Nástroj Flowmon bol implementovaný do firemnej siete formou virtuálneho zariadenia v prostredí Windows Hyper-V a nastavením SPAN portu na core switch. V ďalších podkapitolách je uvedená základná konfigurácia systému spoločne s metódami detekcie v module ADS. V práci sú taktiež popísané nastavenia z alertingu - triggers, ktoré boli požadované firemným správcom. V závere praktickej časti sú prezentované výsledky z monitoringu a modulu ADS. Sú podrobnejšie popísane a rozobraté dve zistené anomálie, kedy jednu s nich je možné označiť ako false positive. Taktiež v tejto časti sa čitateľ zoznámi s možnosťami vizualizácie dát formou profilov, dashboardu alebo reportov.

Praktická časť tejto práce bola vytvorená na podnet firmy, ktorá žiadala zostať v anonymite, aby pomohla vedeniu vo výbere vhodného nástroja na monitorovanie sieťovej komunikácie a detegovanie bezpečnostných anomálii. Navrhnuté riešenie urýchľuje identifikáciu sieťových slabých miest a predchádza nedostupnosti siete. Výsledky demonštrujú nie len funkcionality nástroja Flowmon, ale sú užitočným zdrojom informácií rovnako pre menšie spoločnosti alebo pre subjekty, pre ktoré je oblasť monitoringu prevádzkovaných sietí a informačných systémov vyžadovaná legislatívou (Zákon o kybernetickej bezpečnosti 69/2018 Z. z.).

ZOZNAM POUŽITEJ LITERATÚRY

[1] WOLAND, Aaron, 2018. *Integrated security technologies and solutions: Cisco security solutions for advanced threat protection with next generation firewall, intrusion prevention, AMP, and content security*. I. Indianapolis: Cisco Press. ISBN 9781587147067.

[2] WOLAND, Aaron, 2019. Integrated Security Technologies and Solutions - Volume II : Cisco Security Solutions for Network Access Control, Segmentation, Context Sharing, Secure Connectivity and Virtualization. II. Indianapolis: Cisco Press. ISBN 9781587147074.

[3] GUPTA, Brij a Srivathsan SRINIVASAGOPALAN, 2020. *Handbook of research on intrusion detection systems*. PA: IGI Global,: IGI Global. ISBN 9781799822431.

[4] *Agent vs. Agentless Monitoring* [online], 2018. [cit. 2022-04-15]. Dostupné z: https://www.panopta.com/resources/agent-vs-agentless-monitoring/

[5] *SNMP protokol: snmpget* [online]. In: . [cit. 2022-04-15]. Dostupné z: https://netbeez.net/wp-content/uploads/2020/08/snmpget.png

[6] *Network monitoring* [online]. [cit. 2022-04-15]. Dostupné z: https://netbeez.net/network-monitoring

[7] *A Simple Network Management Protocol (SNMP): rfc1098* [online]. [cit. 2022-04-15]. Dostupné z: https://www.rfc-editor.org/rfc/rfc1098

[8] *Encryption traffic* [online]. [cit. 2022-04-15]. Dostupné z: https://meterpreter.org/https-encryption-traffic/

[9] KUROSE, James F. a Keith W. ROSS, 2013. . *Computer Networking: A Top-Down Approach (6th Edition)*. Boston. ISBN 978-0273768968.

[10] *Wireshark* [online]. [cit. 2022-04-15]. Dostupné z: www.wireshark.org

[11] *Cyber Defence Lab: Nfdump* [online]. In: . [cit. 2022-04-15]. Dostupné z: https://cylab.be/storage/blog/42/files/4ID-giAvSzHJ971XqgTn63U6wHsWHLH85bKna81F7.png

[12] *Nfdump* [online]. [cit. 2022-04-16]. Dostupné z: https://github.com/phaag/nfdump

[13] SANTOS, Omar, 2016. Network security with NetFlow and IPFIX: big data analytics for information security. Indianapolis: Cisco Press. ISBN 1-58714-438-7.

[14] PUŽMANOVÁ, Rita, 2009. *TCP/IP v kostce*. Kopp. ISBN 9788072323883.

[15] *Active Vs. Passive Monitoring: Which is Best for Your Network?* [online]. [cit. 2022-04-16]. Dostupné z: https://www.whatsupgold.com/blog/active-vs.-passive-monitoring-which-is-best-for-your-network

[16] HEIN, Daniel. *Active Monitoring and Passive Monitoring: What's the Difference?* [online]. [cit. 2022-04-16]. Dostupné z: https://solutionsreview.com/network-monitoring/active-monitoring-and-passive-monitoring-whats-the-difference/

[17] *SNMP message exchange* [online]. In: . [cit. 2022-04-16]. Dostupné z: https://blog.paessler.com/hs-fs/hubfs/2020/visuals/Body/SNMP-message-exchange.jpg?width=823&name=SNMP-message-exchange.jpg

[18] *IT explained - SNMP* [online]. [cit. 2022-04-16]. Dostupné z: https://www.paessler.com/it-explained/snmp

[19] *SNMP* [online], 2019. [cit. 2022-04-16]. Dostupné z: https://www.fi.muni.cz/~kas/pv090/referaty/2019-podzim/snmp.html

[20] *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)* [online]. [cit. 2022-04-16]. Dostupné z: https://datatracker.ietf.org/doc/html/rfc3412

[21] *SNMP* [online]. [cit. 2022-04-16]. Dostupné z: http://techtarget.com/search-networking/definition/SNMP

[22] BECK, Frédéric. *NetFlow, RMON and Cisco-NAM deployment* [online]. In: . [cit. 2022-04-16]. Dostupné z: https://www.researchgate.net/publication/29646829_NetFlow_RMON_and_Cisco-NAM_deployment

[23] *Cisco Systems NetFlow Services Export Version 9: rfc3954* [online], 2004. [cit. 2022-04-16]. Dostupné z: https://www.ietf.org/rfc/rfc3954.txt

[24] *TAP vs SPAN* [online]. In: . [cit. 2022-04-16]. Dostupné z: https://www.garland-technology.com/tap-vs-span

[25] ŽÁDNÍ, Martin. *Network Monitoring Based on IP Data Flows: Produced by CESNET led working group on Network monitoring (CBPD131)* [online]. In: . [cit. 2022-04-16]. Dostupné z: https://silo.tips/download/network-monitoring-based-on-ip-data-flows

[26] *Greycortex* [online]. [cit. 2022-04-16]. Dostupné z: https://www.greycortex.com/

[27] *ASNM* [online]. [cit. 2022-04-18]. Dostupné z: https://www.fit.vutbr.cz/~ihomoliak/asnm/

[28] *Caligare* [online]. [cit. 2022-04-18]. Dostupné z: https://www.caligare.com/

[29] *Progress announces acquisition kemp* [online]. [cit. 2022-04-18]. Dostupné z: //https://kemptechnologies.com/emea/news/progress-announces-acquisition-kemp/

[30] *Flowmon* [online]. [cit. 2022-04-18]. Dostupné z: https://www.flowmon.com

[31] *What is 1e100.net* [online]. [cit. 2022-04-18]. Dostupné z: https://support.google.com/faqs/answer/174717?hl=en

ZOZNAM POUŽÍTYCH SYMBOLOV A SKRATIEK

ADS	Anomaly Dedection System
AMP	Application Performance Monitoring
API	Application Programming Interface
ARP	Address Resolution Protocol
AS	Autonomous System
ASNM	Advanced Security Network Metrics
Bd	Baud
BSD	Berkeley Software Distribution
BYOD	Bring Your Own Device
CESNET	Czech Education and Scientific Network
CFI	Caligare Flow Inspector
CPU	Central Processing Unit
CVE	Common Vulnerabilities and Exposures
DDoS	Distributed Daniel-of-Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial-of-Service
DPI	Deep Packet Inspection
ESP	Encapsulating Security Payload
FMC	Flowmon Monitoring Center
AWS	Amazon Web Services
FPI	Flowmon Packet Investigator
GB	Gigabyte
GPL	General Public License
GRE	Generic Routing Encapsulation

GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HW	Hardware
ICMP	Internet Control Message Protocol
ICT	Information and Comunications Technologies
IDS	Intrusion Detection System
IETF	The Internet Engineering Task Force
IMAPS	Internet Message Access Protocol Secure
IoT	Internet of Things
IP	Internet Protocol
IPFIX	Internet Protocol Flow Information Export
ISO	International Organization for Standardization
ISO	Open Systems Interconnection
VLAN	Virtual Local Area Network
ISP	Internet Service Provider
IT	Information Technology
KPI	generovanie Key Performance Indicators
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LEEF	Long Extended Event Format
MAC	Media Access Control
MIB	Management Information Base
MPLS	Multiprotocol Label Switching
NBA	Network Behavior Analysis
NTP	Netowrk Time Protocol
OID	Object Identifier

OTV	Overlay Transport Virtualization
PDF	Portable Document Format
PoC	Proof of Concept
QoE	Quality of Experience
QoS	Quality of Service
RAM	Random Access Memory
RFC	Request for Comments
SCADA	Supervisory control and data acquisition
SIEM	Security Information and Event Management
CEF	Common Event Format
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SPAN	Switch Port Analyzer
SQL	Structured Query Language
SQL	Structured Query Language
SRVNA	Service not available
SSD	Solid-State Drive
SSL	Secure Sockets Layer
TAP	Test Access Point
TB	Terabyte
TCP	Transmission Control Protocol
TRILL	Transparent Interconnection of Lots of Links
TSL	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VA	Virtual Appliance

VNC	Virtual Network Computing
VOIP	Voice over Internet Protocol
WINS	Microsoft Windows Internet Name
WMI	Windows Management Instrumentation

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK