FAKULTA RIADENIA A INFORMATIKY

KATEDRA INFORMAČNÝCH SIETÍ

BEZPEČNOSŤ IS

Správa Projekt – 2015/2016

Vedúci práce:

Doc. Ing. Pavel Segeč, PhD.

Študenti:

Bc. Miroslav Dočár, Bc. Martin Drozdík, Bc. Roman Kasala

Obsah

[1 Obrázky 5](#_Toc454063415)

[2 Tabuľky 7](#_Toc454063416)

[3 Etapa riešenia 8](#_Toc454063417)

[3.1 Popis témy 8](#_Toc454063418)

[3.2 Špecifikácia problému 8](#_Toc454063419)

[4 Úvod 9](#_Toc454063420)

[4.1 Ciele riešenia v Projekte 9](#_Toc454063421)

[4.2 Metodika práce 9](#_Toc454063422)

[4.3 Softvérové možnosti odchytávania a zberu dát 9](#_Toc454063423)

[4.4 Topológia siete a zoznam zariadení 10](#_Toc454063424)

[5 CISCO ASA 5510/5520 11](#_Toc454063425)

[6 NETFLOW 13](#_Toc454063426)

[6.1 NetFlow úvod 13](#_Toc454063427)

[6.2 NetFlow Export Formát Datagramov 15](#_Toc454063428)

[6.3 Konfigurácia NetFlow na Cisco IOS 18](#_Toc454063429)

[6.4 Konfigurácia služby Netflow na ASA cez CLI alebo ASDM (Adaptive Security Device Manager) 19](#_Toc454063430)

[6.4.1 Konfigurácia služby Netflow na ASA cez CLI: 19](#_Toc454063431)

[6.4.2 Konfigurácia služby NetFlow pomocou ASDM: 19](#_Toc454063432)

[6.5 Konfigurácia NetFlow na Juniper 22](#_Toc454063433)

[6.5.1 Vysvetlenie jednotlivých príkazov: 22](#_Toc454063434)

[6.6 NetFlow kolektory 23](#_Toc454063435)

[6.6.1 NTOP 23](#_Toc454063436)

[6.6.2 NTOPng 24](#_Toc454063437)

[6.6.3 Pmacct 30](#_Toc454063438)

[6.6.4 Scrutinizer 31](#_Toc454063439)

[6.6.5 PRTG 35](#_Toc454063440)

[7 SNMP - Simple Network Management Protocol 38](#_Toc454063441)

[7.1 Vznik a verzie SNMP 38](#_Toc454063442)

[7.1.1 SNMPv1 39](#_Toc454063443)

[7.1.2 SNMPv2 39](#_Toc454063444)

[7.1.3 SNMPv3 39](#_Toc454063445)

[7.2 Architektúra systému správy SNMP 39](#_Toc454063446)

[7.2.1 SNMP manažér 40](#_Toc454063447)

[7.2.2 SNMP agent 40](#_Toc454063448)

[7.3 Autentizácia, bezpečnosť a komunikácia 41](#_Toc454063449)

[7.4 SNMP operácie a SNMP formát paketu správy 42](#_Toc454063450)

[7.4.1 SNMP verzia 1 42](#_Toc454063451)

[7.4.2 SNMP verzia 2 45](#_Toc454063452)

[7.4.3 SNMP Verzia 3 47](#_Toc454063453)

[7.5 Management Information Base - MIB 48](#_Toc454063454)

[7.6 Typy SNMP Objektov 49](#_Toc454063455)

[7.7 Čo dokáže SNMP ? 51](#_Toc454063456)

[7.8 Monitorovací systému – Módy / Režimy 52](#_Toc454063457)

[7.8.1 Monitor poll 52](#_Toc454063458)

[7.8.2 Agent push 52](#_Toc454063459)

[7.8.3 Hybrid mode 52](#_Toc454063460)

[7.9 SNMP Konfigurácia na ASA FW 5520 cez Management int. 53](#_Toc454063461)

[7.9.1 Nastavenie management (spravovacieho) portu na ASA FW 5520 53](#_Toc454063462)

[7.9.2 Nastavenie SNMP na ASA FW 5520 53](#_Toc454063463)

[7.9.3 Otestovanie funkčnosti 54](#_Toc454063464)

[7.10 Porovnanie 5 najlepších nástrojov 55](#_Toc454063465)

[7.11 Výber monitorovacieho nástroja - PRTG Network Monitor 56](#_Toc454063466)

[7.11.1 Základné funkcie monitorovacieho nástroja: 56](#_Toc454063467)

[7.11.2 Senzory a protokoly: 56](#_Toc454063468)

[7.11.3 Zobrazenie: 56](#_Toc454063469)

[7.11.4 Upozornenia a hlásenia: 57](#_Toc454063470)

[7.11.5 Hĺbkové správy: 57](#_Toc454063471)

[7.12 Sledovanie ASA 5520 pomocou PRTG Network Monitor prostredníctvom SNMP 58](#_Toc454063472)

[7.12.1 Konfigurácia na ASA 5520 58](#_Toc454063473)

[7.12.2 Nastavenie firewallu do transparentného módu a vytvorenie Bridge-Groupy 58](#_Toc454063474)

[7.12.3 Konfigurácia Interfacov G0/0 a G0/1 58](#_Toc454063475)

[7.12.4 Nastavenie SNMP, vytvorenie skupiny a užívateľa. 58](#_Toc454063476)

[7.13 Inštalácia PRTG Network Monitor 59](#_Toc454063477)

[7.13.1 Nastavenie PRTG 59](#_Toc454063478)

[7.14 Tabuľka KIS FRI zariadení podporujúce SNMP 62](#_Toc454063479)

[8 RMON - Remote Monitoring Network 63](#_Toc454063480)

[9 PACKET CAPTURE s EEM (Embedded Event Manager) 65](#_Toc454063481)

[9.1 Príklad konfigurácie na CISCO ASA cez CLI 65](#_Toc454063482)

[9.2 Príklad konfigurácie na CISCO ASA cez CLI cez ASDM 67](#_Toc454063483)

[9.3 Príklad konfigurácie na CISCO IOS 71](#_Toc454063484)

[10 PORT MIRRORING 73](#_Toc454063485)

[10.1.1 PORT MIRRORING – Local SPAN 73](#_Toc454063486)

[10.1.2 PORT MIRRORING – Remote SPAN 73](#_Toc454063487)

[10.1.3 Konfigurácia 74](#_Toc454063488)

[11 Problémy 75](#_Toc454063489)

[12 Záver 76](#_Toc454063490)

[13 Zdroje 77](#_Toc454063491)

# Obrázky

[Obrázok 5.1 - Skúšobná topológia na KIS FRI UNIZA 12](#_Toc454063355)

[Obrázok 6.1 Vytvorenie IP flow a uloženie v NetFlow Cache 13](#_Toc454063356)

[Obrázok 6.2 NetFlow verzia 1 - obsah datagramu 15](#_Toc454063357)

[Obrázok 6.3 NetFlow verzia 5 - obsah datagramu 16](#_Toc454063358)

[Obrázok 6.4 Detail verzie NetFlow 9 formátu pre export 17](#_Toc454063359)

[Obrázok 6.5 Prihlasovacie okno do ASDM 19](#_Toc454063360)

[Obrázok 6.6 1. krok pre nastavenie NetFlow na ASA5510 20](#_Toc454063361)

[Obrázok 6.7 2. krok pre nastavenie NetFlow na ASA5510 20](#_Toc454063362)

[Obrázok 6.8 3. krok pre nastavenie NetFlow na ASA5510 21](#_Toc454063363)

[Obrázok 6.9 4. krok pre nastavenie NetFlow na ASA5510 21](#_Toc454063364)

[Obrázok 6.10 Konfigurácia NTOP pre prijímanie NetFlow 24](#_Toc454063365)

[Obrázok 6.11 Nefunknčnosť kolektora bez sondy 25](#_Toc454063366)

[Obrázok 6.12 Ukážka funkcie NetFlow sondy a kolektoru 26](#_Toc454063367)

[Obrázok 6.13 Ukážka flows uložených cez netflow kolektor ntopng 27](#_Toc454063368)

[Obrázok 6.14 NTOPng - výber rozhrania 28](#_Toc454063369)

[Obrázok 6.15 NTOPng - zoznam pripojených hostov 28](#_Toc454063370)

[Obrázok 6.16 NTOPng - informácie o hostovi 29](#_Toc454063371)

[Obrázok 6.17 NTOPng - protokoly v sieti 29](#_Toc454063372)

[Obrázok 6.18 Zobrazenie licencie 31](#_Toc454063373)

[Obrázok 6.19 Zobrazenie upozornení 32](#_Toc454063374)

[Obrázok 6.20 Zobrazenie podrobností o exporteroch 32](#_Toc454063375)

[Obrázok 6.21 Chybné hlášky pri nastavení exportera 33](#_Toc454063376)

[Obrázok 6.22 Výpis vo wireshark-u 34](#_Toc454063377)

[Obrázok 6.23 – 1. krok pre nastavenie PRTG 35](#_Toc454063378)

[Obrázok 6.24 – 2. krok pre nastavenie PRTG 35](#_Toc454063379)

[Obrázok 6.25 – 3. krok pre nastavenie PRTG 35](#_Toc454063380)

[Obrázok 6.26 - 4. krok pre nastavenie PRTG 36](#_Toc454063381)

[Obrázok 6.27 – 5. krok pre nastavenie PRTG 36](#_Toc454063382)

[Obrázok 6.28 - 6. krok pre nastavenie PRTG 36](#_Toc454063383)

[Obrázok 6.29 - 7. krok pre nastavenie PRTG 37](#_Toc454063384)

[Obrázok 6.30 – PRTG Netflow v9 senzor 37](#_Toc454063385)

[Obrázok 7.1 – SNMP Manager – SNMP Agent 40](#_Toc454063386)

[Obrázok 7.2 - Komunikácia Správca - Agent 42](#_Toc454063387)

[Obrázok 7.3 - Formát SNMP správy 42](#_Toc454063388)

[Obrázok 7.4 - Formát SNMP PDU správy 43](#_Toc454063389)

[Obrázok 7.5 - Formát SNMP Trap správy 44](#_Toc454063390)

[Obrázok 7.6 - Stromová štruktúra MIB databázy 48](#_Toc454063391)

[Obrázok 7.7 51](#_Toc454063392)

[Obrázok 7.8 – Výpis snmpwalk 54](#_Toc454063393)

[Obrázok 7.9 - Testovacia topológia 58](#_Toc454063394)

[Obrázok 7.10 - 1. krok pre nastavenie PRTG 59](#_Toc454063395)

[Obrázok 7.11 - 2. krok pre nastavenie PRTG 59](#_Toc454063396)

[Obrázok 7.12 - 3. krok pre nastavenie PRTG 59](#_Toc454063397)

[Obrázok 7.13 - 4. krok pre nastavenie PRTG 60](#_Toc454063398)

[Obrázok 7.14 - 5.krok pre nastavenie PRTG - Credentials for SNMP 60](#_Toc454063399)

[Obrázok 7.15 - 6. krok pre nastavenie PRTG 60](#_Toc454063400)

[Obrázok 7.16 - 7. krok pre nastavenie PRTG 61](#_Toc454063401)

[Obrázok 7.17 - 8. krok pre nastavenie PRTG 61](#_Toc454063402)

[Obrázok 7.18 - 9. krok pre nastavenie PRTG 61](#_Toc454063403)

[Obrázok 7.19 – 10. . krok pre nastavenie PRTG 62](#_Toc454063404)

[Obrázok 7.20 – PRTG senzory 62](#_Toc454063405)

[Obrázok 9.1 - Začiatok konfigurácie v ASDM 67](#_Toc454063406)

[Obrázok 9.2 Nastavenie pre vstupný interface 67](#_Toc454063407)

[Obrázok 9.3 Nastavenie pre výstupný interface 68](#_Toc454063408)

[Obrázok 9.4 Nastavenie buffera 68](#_Toc454063409)

[Obrázok 9.5 Zapnutie zachytávania paketov 69](#_Toc454063410)

[Obrázok 9.6 Zobrazenie odchytených paketov 69](#_Toc454063411)

[Obrázok 9.7 Export zachytených dát 70](#_Toc454063412)

[Obrázok 10.1 Local SPAN 73](#_Toc454063413)

[Obrázok 10.2 Remote SPAN 73](#_Toc454063414)

# Tabuľky

[Tabuľka 7.1 - Formát SNMP správy 43](#_Toc454063338)

[Tabuľka 7.2 - Chybový stav správy 43](#_Toc454063339)

[Tabuľka 7.3 - Formát poľa PDU 43](#_Toc454063340)

[Tabuľka 7.4 - Príčiny generovania Trap správy 45](#_Toc454063341)

[Tabuľka 7.5 - Formát Trap správy 45](#_Toc454063342)

[Tabuľka 7.6 - Typ PDU SNMPv2 46](#_Toc454063343)

[Tabuľka 7.7 - Rozšírený chybový stav správy SNMPv2 46](#_Toc454063344)

[Tabuľka 7.8 - Formát PDU správy GetBulk 47](#_Toc454063345)

[Tabuľka 7.9 - Formát hlavičky správy SNMPv3 47](#_Toc454063346)

[Tabuľka 7.10 - Atribúty MIB objektov 48](#_Toc454063347)

[Tabuľka 7.11 - Agregátne dátové typy MIB objektov 49](#_Toc454063348)

[Tabuľka 7.12 - Neagregátne dátové typy MIB objektov 49](#_Toc454063349)

[Tabuľka 7.13 - Zhrnutie najdôležitejších funkcií a vlastností piatich najlepších nástrojov 55](#_Toc454063350)

[Tabuľka 7.14 – Údaje pre Credentials for SNMP 60](#_Toc454063351)

[Tabuľka 7.15 - KIS FRI zariadenia podporujúce SNMP 62](#_Toc454063352)

[Tabuľka 12.1 - Zhrnutie testovaných technológií 76](#_Toc454063353)

[Tabuľka 12.2 - Zhrnutie testovaných kolektorov pre NetFlow 76](#_Toc454063354)

# Etapa riešenia

## Popis témy

Úlohou je zbieranie dát zo siete a ich následná analýza. Po tejto analýze by sme mali byť schopný určiť, kedy sa jedná o sieťový útok a implementovať opatrenia na kritické miesta v sieti, pre rýchle stopnutie sieťového útoku.

## Špecifikácia problému

Projekt Bezpečnosť pozostáva zo štyroch vrstiev, pričom každá z vrstiev má špecifické ciele, ktorými sa zaoberala na predmete Projekt 1. Dlhodobým cieľom našej vrstvy, t.j. druhej vrstvy s názvom Technológie získavania dát, je získať dáta zo siete, v podobe, ktorú nám bližšie špecifikuje nasledujúca vrstva (Analýza príznakov), ktorá získané dáta analyzuje. V našej vrstve pritom potrebujeme riešiť nasledovné problémy:

* odkiaľ zbierať dáta (z hľadiska topológie a zariadenia)
* akú technológiu získavania dát použiť.

# Úvod

## Ciele riešenia v Projekte

Medzi ciele Projektu 1 patrilo:

* Oboznámenie sa so softvérovými možnosťami odchytávania a zberu dát.
* Oboznámenie sa s topológiou na KIS FRI UNIZA + podrobný zoznam zariadení.
* Oboznámenie sa s CISCO ASA 5510/5520 firewallmi a ich konfiguráciou v transparentnom režime.
* Využiť zariadenie FW ASA pre zber dát a monitoring.

Medzi ciele Projektu 2 patrilo:

* Testovať a zdokumentovať rôzne technológie pre zber dát na zariadeniach, ktoré sú dostupné (switche, routre, firewall ASA)

## Metodika práce

Úvodom projektu sme si naštudovali rôzne softvérové či hardvérové prostriedky na získavanie dát (vid. dokument Príloha 1 - Zber dát – nástroje). Následne sme získali a spracovali topológiu katedry Informačných sietí ako aj celej fakulty (viď dokument Príloha 2 – Topológia FRI-KIS) spolu so zoznamom zariadení (viď dokument Príloha 3 – Zariadenia FRI-KIS). Po zistení aké hardvérové prostriedky sa v sieti nachádzajú, sme boli schopný povedať kde sa aké technológie na zber dát dajú použiť. Ďalším bodom bolo testovanie a správne nakonfigurovanie Cisco Firewall-u ASA 5510. Úlohou bolo nakonfigurovať ho tak, aby bol schopný v transparentnom režime odchytávať prevádzku na katedre informačných sietí. Po nakonfigurovaní sme mohli testovať rôzne služby, programy, technológie pre zber dát.

## Softvérové možnosti odchytávania a zberu dát

Medzi prvé body Projektu 1 patrilo oboznámenie sa so softvérovými a hardvérovými prostriedkami na získavanie dát zo siete. Na základe topológie siete z prostredia FRI fakulty, ale aj z prostredia katedry KIS, sme zistili dostupné hardvérové prostriedky, medzi ktoré patrili napríklad smerovače, prepínače, firewall-y či Access Pointy. Na každom zariadení je možné spustiť iné technológie získavania dát, medzi ktoré patrí napríklad Port Mirorring, rôzne Cisco nástroje (NetFlow), rôzne nástroje na zber dát z wi-fi sietí, či IDS/IPS nástroje na detekciu útokov. Ako sme spomenuli predtým, informácie o jednotlivých nástrojoch sú zozbierané v dokumente Príloha 1 – Zber dát - nástroje. Tieto technológie si odskúšame v nasledujúcich kapitolách.

## Topológia siete a zoznam zariadení

Na základe informácii ktoré nám poskytli Ing. Jozef Mičic a Doc. Ing. Pavel Segeč, PhD. sa nám podarilo spracovať topológiu spolu so zoznamom zariadení. Na základe toho môžeme určiť, ktoré technológie sa dajú použiť na konkrétnom zariadení v sieti. Túto topológiu môžeme vidieť v súbore Príloha 2 – Topológia FRI-KIS.

# CISCO ASA 5510/5520

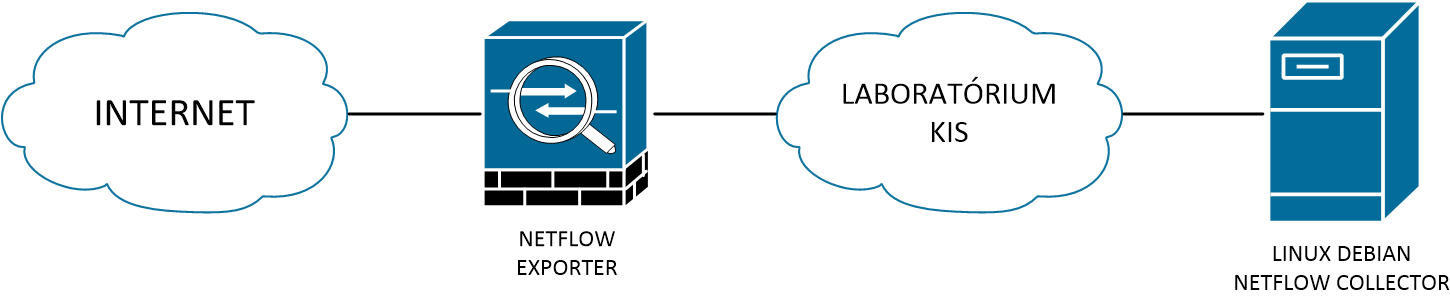
Základným bodom riešenia bola konfigurácia Cisco Firewall ASA 5510 na odchytávanie dát zo siete. Cieľom bolo aby firewall vystupoval v sieti ako transparentný. Pri konfigurácií Cisco ASA 5510 sme riešili niektoré problémy, ktoré sú popísané v kapitole Problémy.

Základná konfigurácia vyzerá nasledovne :

enable   
conf t   
firewall transparent   
interface e0/0   
nameif INSIDE   
security-level 100   
bridge-group 1   
no shutdown   
interface e0/1   
nameif OUTSIDE   
security-level 0   
bridge-group 1   
no shutdown   
interface BVI1   
ip address 158.193.139.17 255.255.255.0  
access-list INSIDE extended permit ip any any   
access-group INSIDE in interface INSIDE   
policy-map global\_policy   
class inspection\_default   
inspect icmp

Následná konfigurácia, konkrétne konfigurácia softvérových nástrojov na odchytávanie dát už prebiehala pomocou grafického rozhrania ASDM a vzdialeného prístupu. Na to sme však museli na ASA firewalle nakonfigurovať nasledujúce veci:

enable  
conf t  
crypto key generate rsa modulus 1024   
aaa authentication ssh console LOCAL   
username projekt1 password Projekt.1   
ssh version 2   
ssh 158.193.139.0 255.255.255.0 inside   
ssh 158.193.152.0 255.255.255.0 outside   
http server enable   
http 158.193.139.0 255.255.255.0 inside   
http 158.193.152.0 255.255.255.0 outside   
asdm image disk0:/asdm-741.bin



Obrázok . - Skúšobná topológia na KIS FRI UNIZA

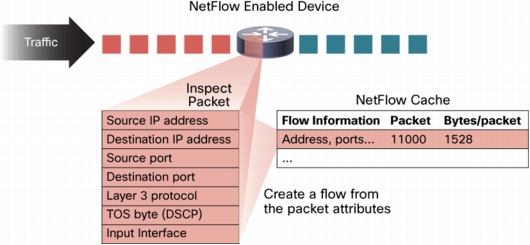
# NETFLOW

## NetFlow úvod

NetFlow bol vymyslený firmou Cisco pre zaznamenávanie sieťovej prevádzky na zariadeniach. IP Flow sa skladá z paketov, ktoré majú rovnaké atribúty. Typicky sa kontroluje 5 až 7 atribútov, ktoré sa musia zhodovať aby v konečnom dôsledku tvorili IP Flow:

* Zdrojová IP adresa
* Cieľová IP adresa
* Zdrojový port UPD alebo TCP
* Cieľový port UPD alebo TCP
* Typ protokolu na tretej vrstve
* Priorita prevádzky (Class of Service)
* Rozhranie smerovača alebo prepínača

Následne sa v tomto IP Flow spočíta počet paketov a bytov. Tieto informácie sú následne uložené v databáze NetFlow nazývanej NetFlow cache.



Obrázok . Vytvorenie IP flow a uloženie v NetFlow Cache

Ďalšie informácie, ktoré sa pridávajú k týmto IP Flow tokom sú: časový záznam pre zaznamenanie dĺžky „života“ toku (používa sa na výpočet paketov alebo bytov za daný čas), next-hop adresa vrátane BGP AS, masky cieľovej a zdrojovej adresy pre prepočítanie prefixov, TCP príznaky pre preskúmanie TCP handshake.

Sú dve možnosti ako sa dostať k NetFlow dátam: buď cez CLI (Command Line Interface) – príkazový riadok so show príkazmi alebo posielať tieto dáta na server zvaný NetFlow collector. Dáta sa posielajú periodicky. V princípe, NetFlow cache je stále zaplňovaná IP Flow tokmi a vnútorný softvér smerovača alebo prepínača hľadá v tejto cache IP Flow toky, ktoré sa už ukončili alebo expirovali a tieto IP Flow toky sa pošlú na collector. Ukončením Ip Flow toku sa myslí ukončenie komunikácie. Sú to napríklad tieto veci:

* Neaktívny IP Flow toky (15 sekúnd je default)
* Dlhé IP Flow toky (30 minút = 1800 sekúnd je default)
* Ukončenie relácie (paket obsahuje TCP FIN príznak)

Dáta sa posielajú zvyčajne pomocou UDP protokolu (používané porty sú 2055, 9555, 9025, ...). V dnešnej implementácii sa ale používa aj protokol SCTP (Stream Control Transmission Protocol). Ten sa používa hlavne kvôli tomu, že pri UDP je možnosť straty niektorých IP Flow tokov a tým pádom by to malo dopad na celkové štatistiky a analýzy.

Typicky pre správne fungovanie monitoringu pomocou NetFlow, musí sieť obsahovať tri komponenty:

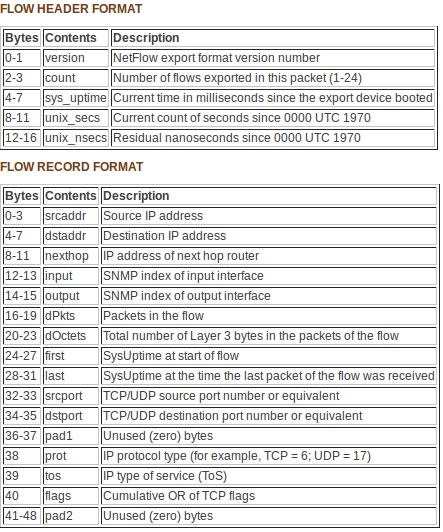
* Flow exporter – zariadenie, ktoré zbiera dáta, vytvára z nich IP Flow toky a exportuje ich na jeden alebo viac collectorov
* Flow collector – zariadenie, zodpovedné za prijatie IP Flow tokov, uchovávať a predspracovať ich
* NetFlow analyzers – aplikácie, ktoré analyzujú IP Flow toky z collectora

Stretávame sa s celkovo tromi názvami pre NetFlow a to CFlow, JFlow a SFlow. Názov vlastne určuje, z akého zariadenia sa IP Flow tok posiela. CFlow posielajú zariadenia Cisco, JFlow posielajú zariadenia Juiper a SFlow posielajú zariadenia od HP. Rozdiely medzi týmito technológiami môže byť vo vnútornej štruktúre datagramov. Ďalšie rozdiely sú napríklad v tom, že CFlow zachytáva všetky pakety, ale SFlow zachytáva len prevádzku smerom dnu. Prevádzka, ktorá smeruje von nezachytáva.

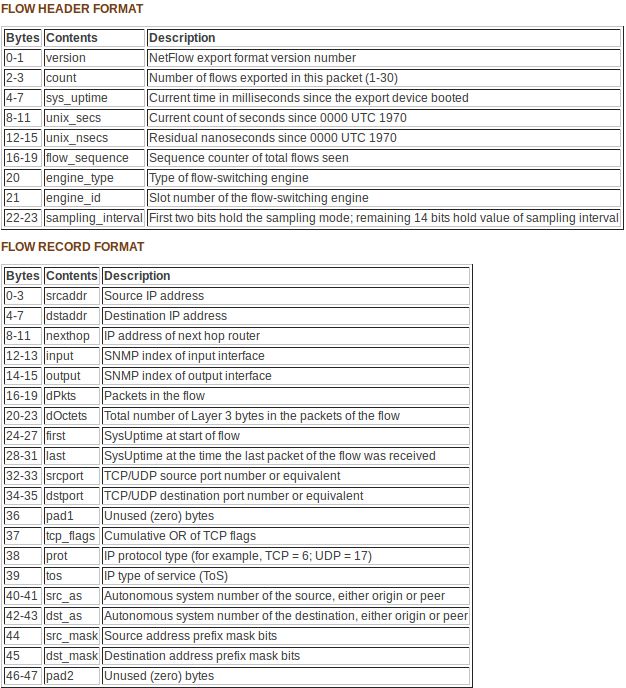
## NetFlow Export Formát Datagramov

Všetky verzie odosielajú datagramy, ktoré obsahujú hlavičku a sekvenciu zaznamenaných tokov (flow records). Hlavička obsahuje informácie ako verzia NetFlow-u, sekvenčné číslo, číslo záznamu a pod. Samotný zaznamenaný tok obsahuje informácie o tomto toku, IP adresy, porty, smerovacie informácie a pod. NetFlow vo verzii 9 prináša nový formát pre export. Tie sú zložené na tzv. šablónach. Tieto šablóny robia záznamy tokov rozšíriteľnými.

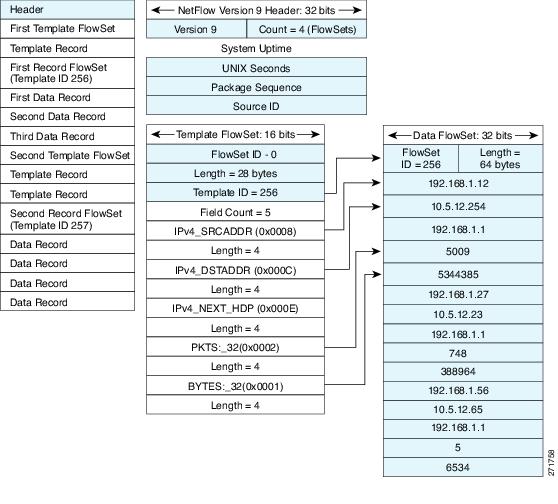
Verzia 1 bola exportovaná len vo formáte podporovanom Cisco IOS a dnes sa už nepoužíva. Do verzie 5 bola pridaná informácia o BGP autonómnych systémoch a sekvenčné čísla jednotlivých tokov. Verzia 7 pridala NetFlow podporu pre Cisco Catalyst série prepínače, ktoré pracujú v hybridnom alebo natívnom móde. Verzie 2,3,4 a 6 formáty pre export neboli uvedené na trh alebo nie sú podporované. Export vo verzii 8 sa používa, keď je povolená router-based NetFlow agregácia.



Obrázok . NetFlow verzia 1 - obsah datagramu



Obrázok . NetFlow verzia 5 - obsah datagramu



Obrázok . Detail verzie NetFlow 9 formátu pre export

## Konfigurácia NetFlow na Cisco IOS

Najprv treba povoliť Cisco Express Forwarding:

*router(config)# ip cef*

*router(config)# ip cef distributed*

Treba povoliť na rozhraniach NetFlow:

interface

ip flow ingress

staršie príkazy:

interface

ip route-cache flow

Napríklad:

interface FastEthernet0

ip flow ingress

interface Serial2/1

ip flow ingress

Je nevyhnutné povoliť NetFlow na všetkých rozhraniach, cez ktoré tieto toky pôjdu.

Povolenie exportu v globálnom režime:

Router(config)# ip flow-export version 5

Router(config)# ip flow-export destination <ip\_address> 2000

Router(config)# ip flow-export source FastEthernet0

IP adresa je adresa NetFlow Collectora, na ktorý sa budú posielať NetFlow toky a port, na ktorom počúva tento NetFlow Collector. V tomto prípade je to port 2000.

Príkaz *ip flow-export source* je použitý pre definovanie, ktorým portom budú odosielané NetFlow toky. Pokiaľ smerovač používa BGP protokol, môže byť AS zahrnuté v exporte:

router(config)# ip flow-export version 9 [peer-as | origin-as]

Nastavenie časovačov:

router(config)# ip flow-cache timeout active 5

router(config)# ip flow-cache timeout inactive 30

Show príkazy pre kontrolu nakonfigurovaného NetFlow:

router# show ip flow export

router# show ip cache flow

router# show ip cache verbose flow

## Konfigurácia služby Netflow na ASA cez CLI alebo ASDM (Adaptive Security Device Manager)

Sú dve možnosti ako správne nakonfigurovať Netflow na Firewalle ASA 5510/5520:

### Konfigurácia služby Netflow na ASA cez CLI:

flow-export destination INSIDE 158.193.139.16 2055

flow-export template timeout-rate 10

access-list INSIDE extended permit ip any any

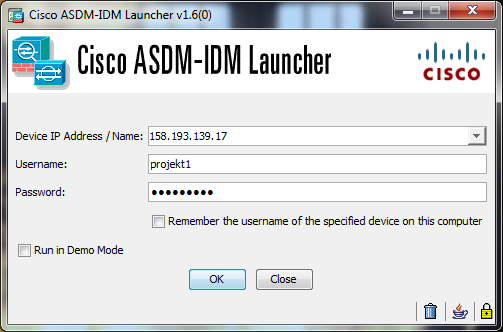
access-list OUTSIDE extended permit ip any any

policy-map global-policy

class global-class

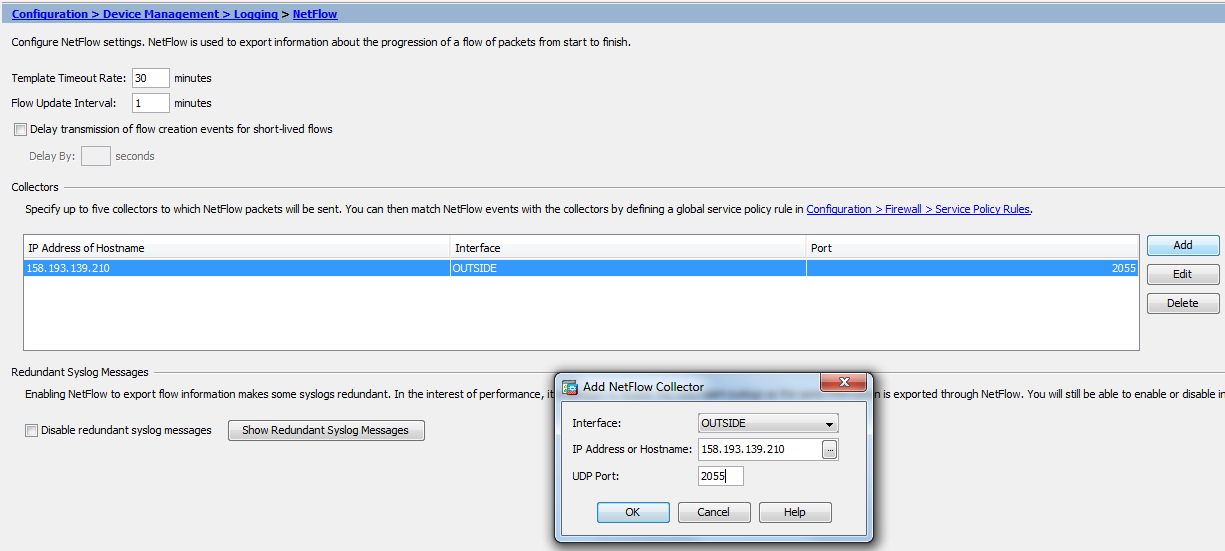
flow-export event-type all destination 158.193.139.16

### Konfigurácia služby NetFlow pomocou ASDM:



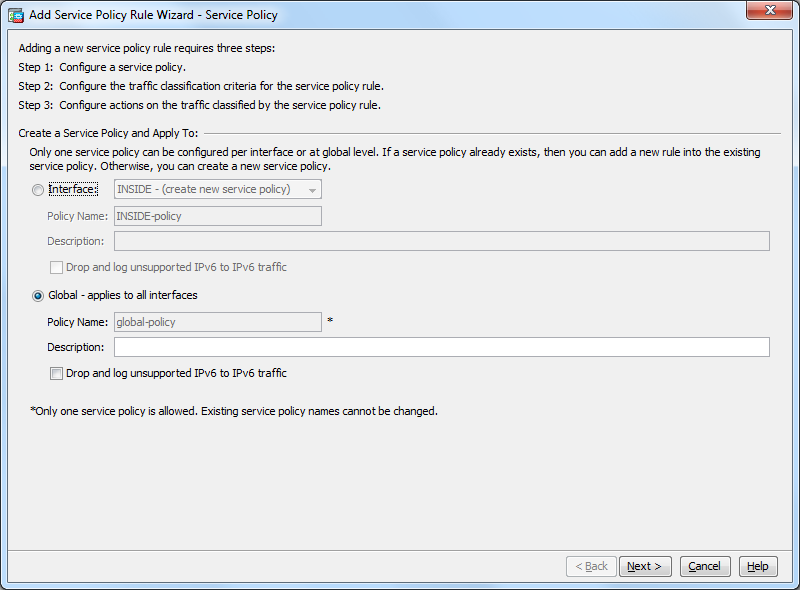
Obrázok . Prihlasovacie okno do ASDM

* *Configuration -> Device Management -> Logging -> NetFlow -> Add*

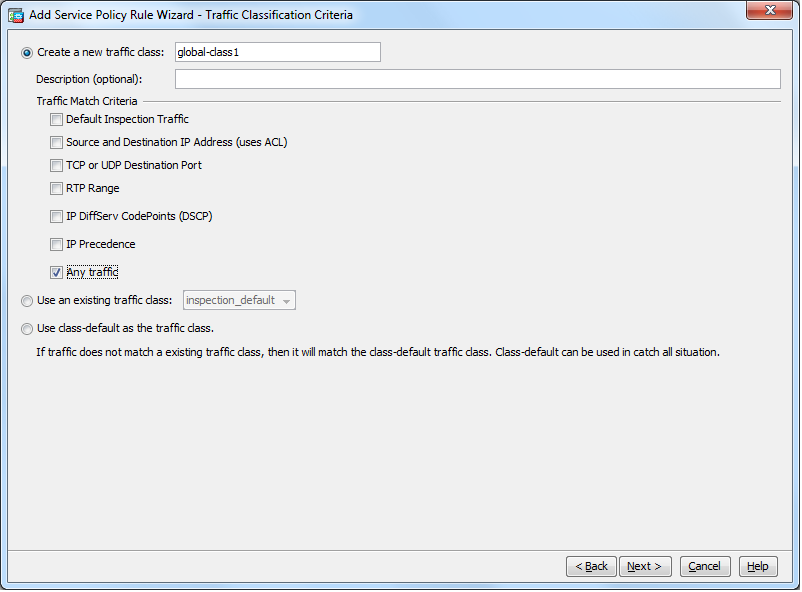


Obrázok . 1. krok pre nastavenie NetFlow na ASA5510

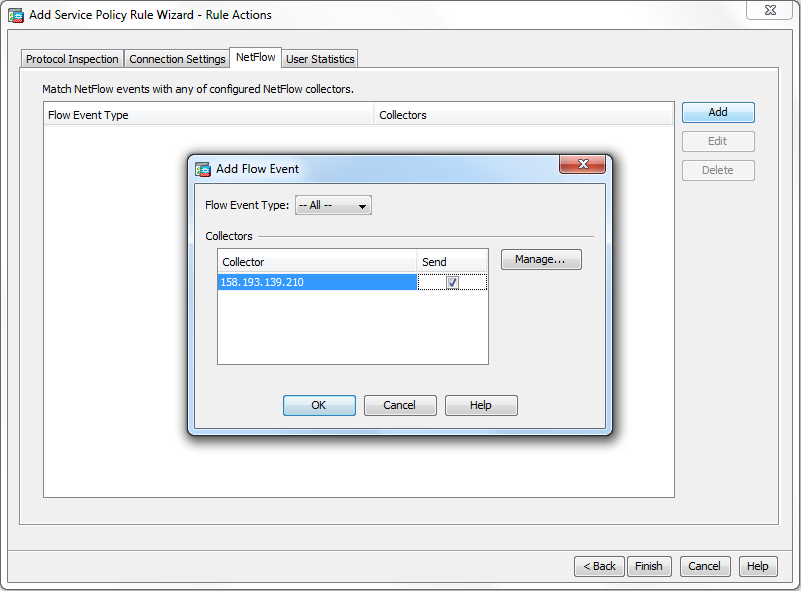
* *Configuration -> Firewall -> Service Policy Rules -> Add*



Obrázok . 2. krok pre nastavenie NetFlow na ASA5510



Obrázok . 3. krok pre nastavenie NetFlow na ASA5510



Obrázok . 4. krok pre nastavenie NetFlow na ASA5510

## Konfigurácia NetFlow na Juniper

forwarding-options

sampling {

input {

rate 1;

run-length 0;

max-packets-per-second 50000;

}

family inet {

output {

flow-active-timeout 60;

flow-server 192.168.33.38 {

port 9996;

}

flow-server 192.168.33.96 {

port 9996;

version 500;

}

}

}

}

}

### Vysvetlenie jednotlivých príkazov:

*Forwarding-options* – štart JFlow konfigurácie

*sampling* – štart konfigurácie JFlow možností

*input* – ak sa tento príkaz nezadá, sampling bude neaktívny

*rate* *1* – špecifikuje pomer paketov ktoré majú byť testované. Defaultne je nastavená 0 čo znamená, že žiadne pakety sa netestujú. Rate 1 hovorí o pomere 1:1 čo znamená, že sa bude logovať každý jeden paket

*run-length 0* – špecifikuje počet vhodných paketov na testovanie po prvom, ktorý spustí event. Defaultne je táto hodnota nastavená na 0 čo znamená, že sa po spustení event-u sa ďalej prevádzka netestuje

*max-packets-per-seconds 50000* - číslo hovorí o počte testovaní za sekundu, default = 1000

*family inet* – IPv4 (možné hodnoty sú: inet | inet6 | mpls)

*output* – konfigurácia exportu JFlow

*flow-active-timeout 60* – nastavenie ako často sa majú exportovať dáta v sekundách

*flow-server 192.168.33.96* – nastavenie IP adresy collectora

*port 9996* – UDP port servera

*version 500* – verzia formátu: 5, 8 alebo 500 (500 ASN)

## NetFlow kolektory

### NTOP

NTOP nám umožňuje prehľad IP toku pomocou webového rozhrania. V ňom vidíme veľkosť IP toku, ktorý prechádza cez firewall. Tento collector nám taktiež umožňuje v určitých intervaloch, ukladať informácie o toku do súboru s koncovkou .flow.

NTOP sme nainštalovali na server s operačným systémom Debian. Skúsili sme dva spôsoby inštalácie a to cez klasické balíčky, ktoré zahŕňa OS Debian a inštalácia zo stiahnutých zdrojových kódov.

NTOP pozná graficky aj funkcionalitou lepšiu verziu a to NTOPng. Tá sa vďaka výhodám stala pre nás prvoradá. Jej inštaláciu a konfiguráciu si ukážeme v kapitole 5.6.2**.**

Inštalačné kroky zo balíčkov:

sudo apt-get install libpcap-dev libgdbm-dev libevent-dev librrd-dev python-dev libgeoip-dev automake libtool subversion

sudo apt-get update

sudo apt-get install ntop

Spustenie služby NTOP:

service ntop start

Inštalačné kroky zo zdrojových kódov:

sudo apt-get install libpcap-dev libgdbm-dev libevent-dev librrd-dev python-dev libgeoip-dev automake libtool subversion

apt-get install ntop ntop-data ntop-dbg

/etc/inid.d/ntop/start | status

or

cd ~

wget http://sourceforge.net/projects/ntop/files/ntop/Stable/ntop-5.0.1.tar.gz

tar xvfz ntop-5.0.1.tar.gz && cd ntop-5.0.1

./autogen.sh

make

make install

Spustenie služby NTOP:

cd ntop-5.0.1

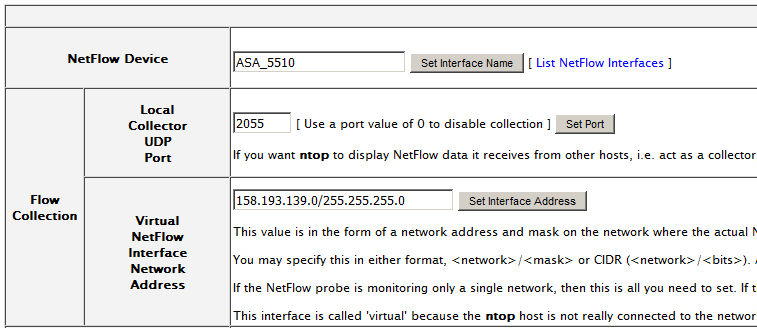
ntop

Konfigurácia NTOP aby prijímal NetFlow toky:

https://158.193.139.16:3000

Plugins -> NetFlow -> Active

Plugins -> NetFlow -> View/Configure -> Add NetFlow Device



Obrázok . Konfigurácia NTOP pre prijímanie NetFlow

### NTOPng

NtopNG je open-source sieťový analyzátor, ktorý poskytuje webové rozhranie pre sledovanie sieťovej prevádzky v reálnom čase. NtopNG môžeme nainštalovať na ľubovolnom monitorovacom servery, a použiť webový prehliadač pre sledovanie sieťovej prevádzky v reálnom čase. NtopNG je nadstavba klasického NTOP sieťového nástroja.

Vlastnosti Ntop:

* Real-time analýza sieťovej prevádzky.
* Zotriedenie dát sieťovej prevádzky podľa protokolov a rôznych iných kritérií.
* Zobrazenie distribúcie prevádzky vzhľadom na jednotlivé protokoly.
* Zobrazovanie štatistík o sieťovej prevádzke.
* Geo-lokácia IP adries.
* Hlboká inšpekcia paketov na základe zisťovania služieb (napr. Google, Facebook).
* Identifikácia hostiteľského OS.
* Historická analýza prevádzky (napr. hodinové, denné, týždenné, mesačné, ročné).
* Podpora pre sFlow, NetFlow (v5 / v9) a IPFIX cez nProbe.
* Matica sieťovej komunikácie (kto hovorí s kým?).
* Podpora IPv6.

Následná inštalácia balíčkov a ich konfigurácia prebiehala na systéme Debian (Linux version 3.16.0-4-amd64).

#### Inštalácia ntopng

su -

mcedit /etc/apt/sources.list.d/ntop.list

add following lines:

deb http://www.nmon.net/apt-stable/12.04/ x64/

deb http://www.nmon.net/apt-stable/12.04/ all/

wget -qO - http://www.nmon.net/apt-stable/ntop.key | apt-key add -

apt-get update

apt-get install libpcap-dev libglib2.0-dev libgeoip-dev redis-server libxml2-dev libnl1

apt-get install ntopng pfring nprobe ntopng-data n2disk nbox

#### Konfigurácia

cd /etc/ntopng/

touch ntopng.start

mcedit ntopng.conf

-G=/var/tmp/ntopng.pid

-i=eth0

-i=tcp://127.0.0.1:5556

Zmena hesla

echo -n "heslo" | md5sum

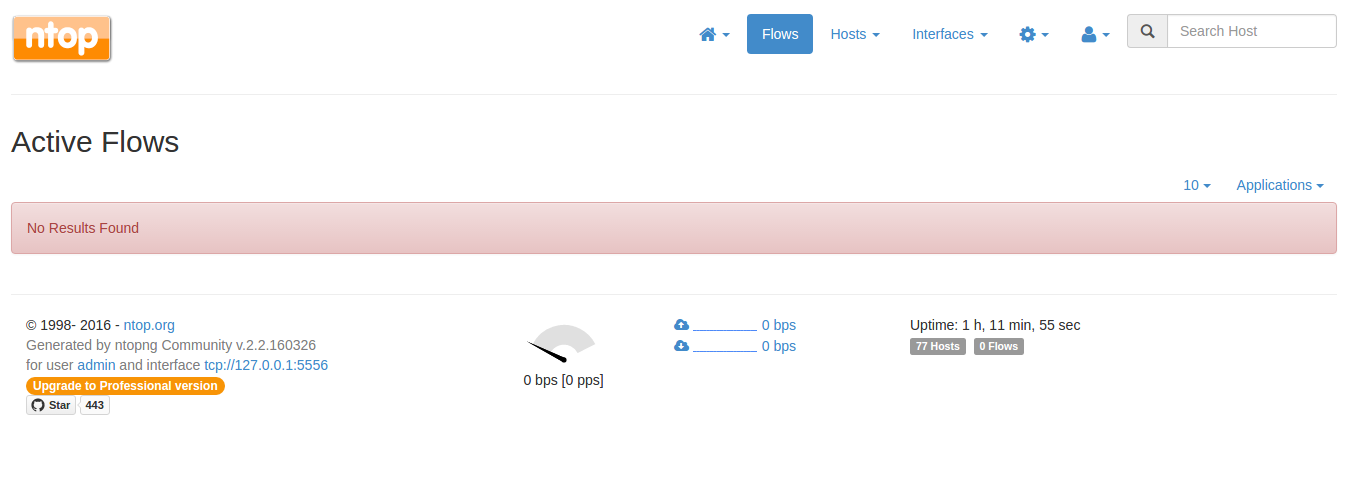
redis-cli SET user.admin.password ea847988ba59727dbf4e34ee75726dc3

#### Spustenie

service redis-server start

sudo service ntopng start

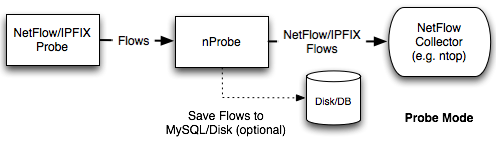
Po tomto nám ntopng ešte nebude fungovať, pretože potrebuje probe.



Obrázok . Nefunknčnosť kolektora bez sondy

Klasický Ntop obsahuje NetFlow v5/v9/IPFIX probe a collector, ktorý môže byť použitý na rozoberanie Netflow tokov. Pre jeho neoriginálny dizajn je preferovanejšia verzia NtopNG, ktorá však ku svojej funkčnost Netflow collectora potrebuje probe.

**nProbe** je nástroj ktorý slúži na odovzdanie informácií o prevádzke od NetFlow exportera ku NetFlow collectoru.



Obrázok . Ukážka funkcie NetFlow sondy a kolektoru

**Príkaz:**

nprobe --zmq "tcp://127.0.0.1:5556" -i eth0 -n none --collector-port 2055

nProbe pre svoju plnú funkčnosť vyžaduje licenciu, bez nej sa nProbe prepne do demo verzie kde podporuje len 25000 flows.

07/Apr/2016 08:23:47 [nprobe.c:3114] ERROR: Invalid nProbe license (/etc/nprobe.license) [Missing license file]

07/Apr/2016 08:23:47 [nprobe.c:3121] ERROR: \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

07/Apr/2016 08:23:47 [nprobe.c:3122] ERROR: \*\* \*\*

07/Apr/2016 08:23:47 [nprobe.c:3123] ERROR: \*\* Switching to DEMO MODE (missing valid license) \*\*

07/Apr/2016 08:23:47 [nprobe.c:3124] ERROR: \*\* \*\*

07/Apr/2016 08:23:47 [nprobe.c:3125] ERROR: \*\* Create your nProbe license at \*\*

07/Apr/2016 08:23:47 [nprobe.c:3126] ERROR: \*\* http://www.nmon.net/mklicense/ \*\*

07/Apr/2016 08:23:47 [nprobe.c:3127] ERROR: \*\* \*\*

07/Apr/2016 08:23:47 [nprobe.c:3128] ERROR: \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

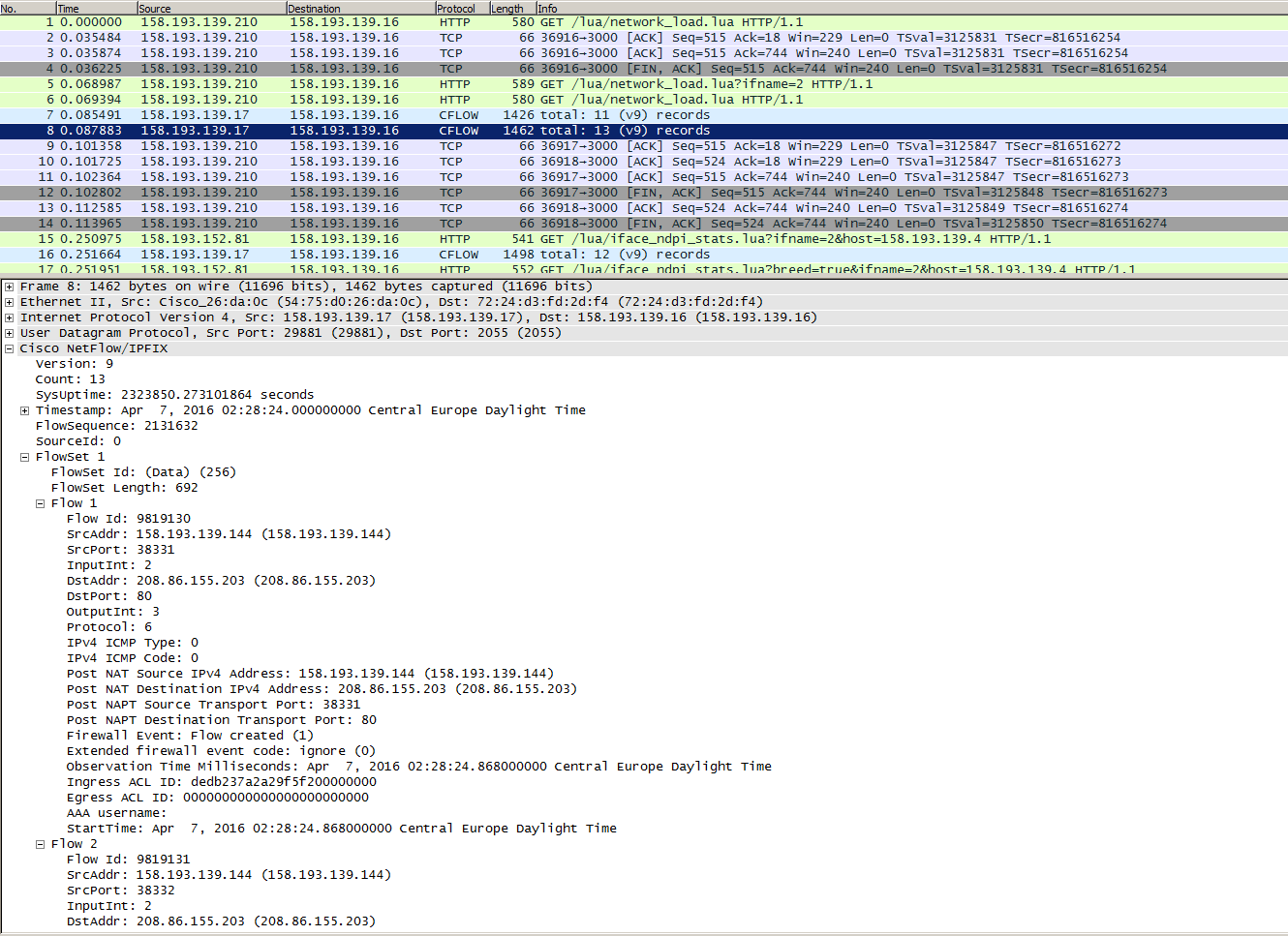
07/Apr/2016 08:23:47 [nprobe.c:6508] ERROR: \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

07/Apr/2016 08:23:47 [nprobe.c:6509] ERROR: \* NOTE: This is a DEMO version limited to 25000 flows export. \*

07/Apr/2016 08:23:47 [nprobe.c:6510] ERROR: \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Po konfigurácií nProbe už vidíme výsledky.

Následne som si toky ukladal na disk v podobe súborov s koncovkou .pcap. To som nastavil v nasledovných nastaveniach ([odkaz](http://158.193.139.16:3000/lua/if_stats.lua?if_name=eth0&page=packetdump)) kde bolo treba povoliť ukladanie na disk, ktoré sa následne ukladali do zložky *var/tmp/ntopng/2/pcap/.* Odchytené informácie som si otvoril v programe Wireshark.



Obrázok . Ukážka flows uložených cez netflow kolektor ntopng

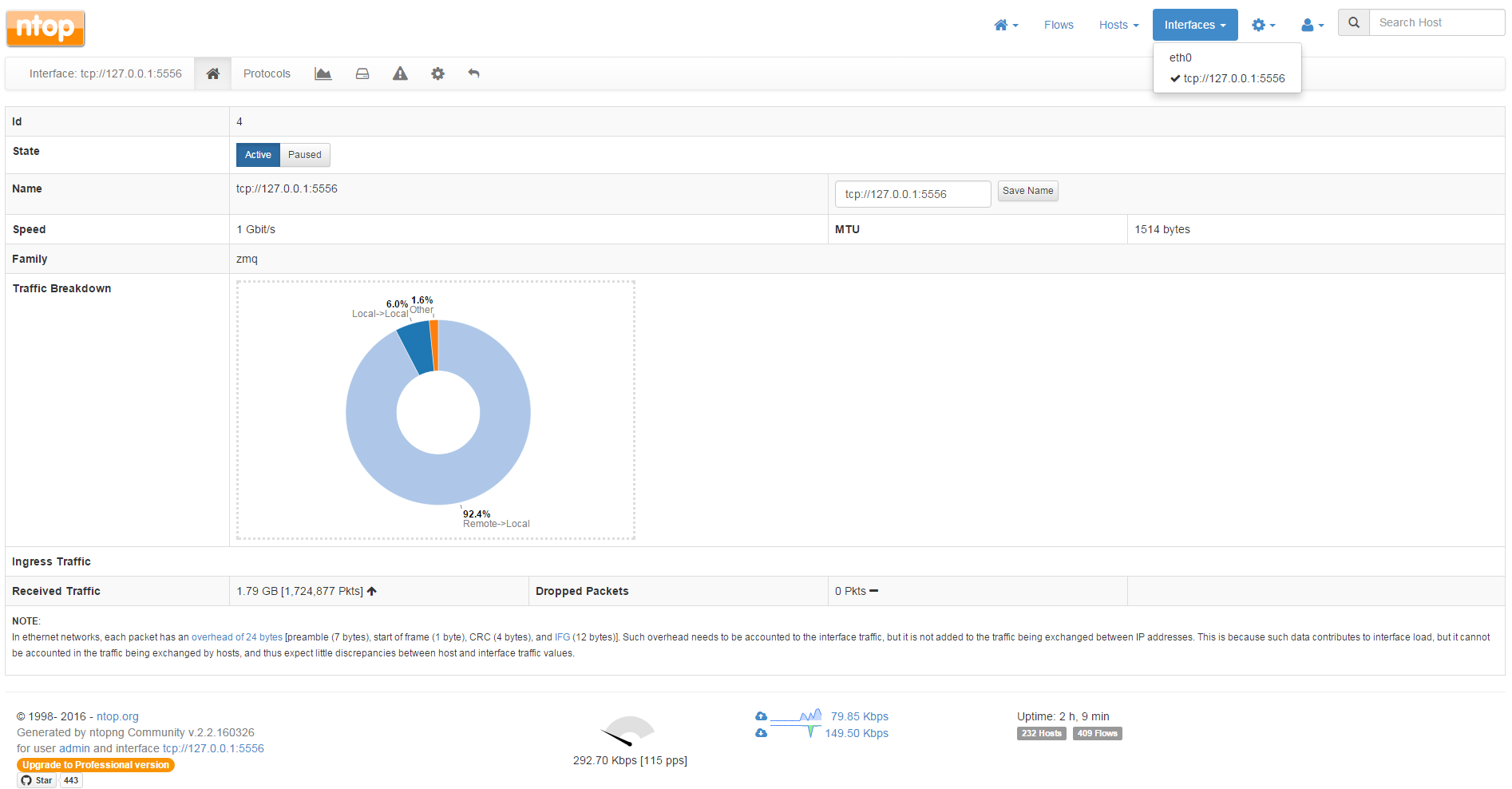
Stalo sa nám, že sa disk na servery rýchlo zaplnil flowmi a logmi a nebol schopný prevádzky, kvôli nedostatku priestoru. To zistíme a vyriešime nasledovnými príkazmi:

df -H //iba pre zistenie stavu kapacity disku

du -h --max-depth=1 | sort –hr //zistí ktorá zložka koľko zaberá, spustiť v koreňovom  
 //následné vymazanie logov

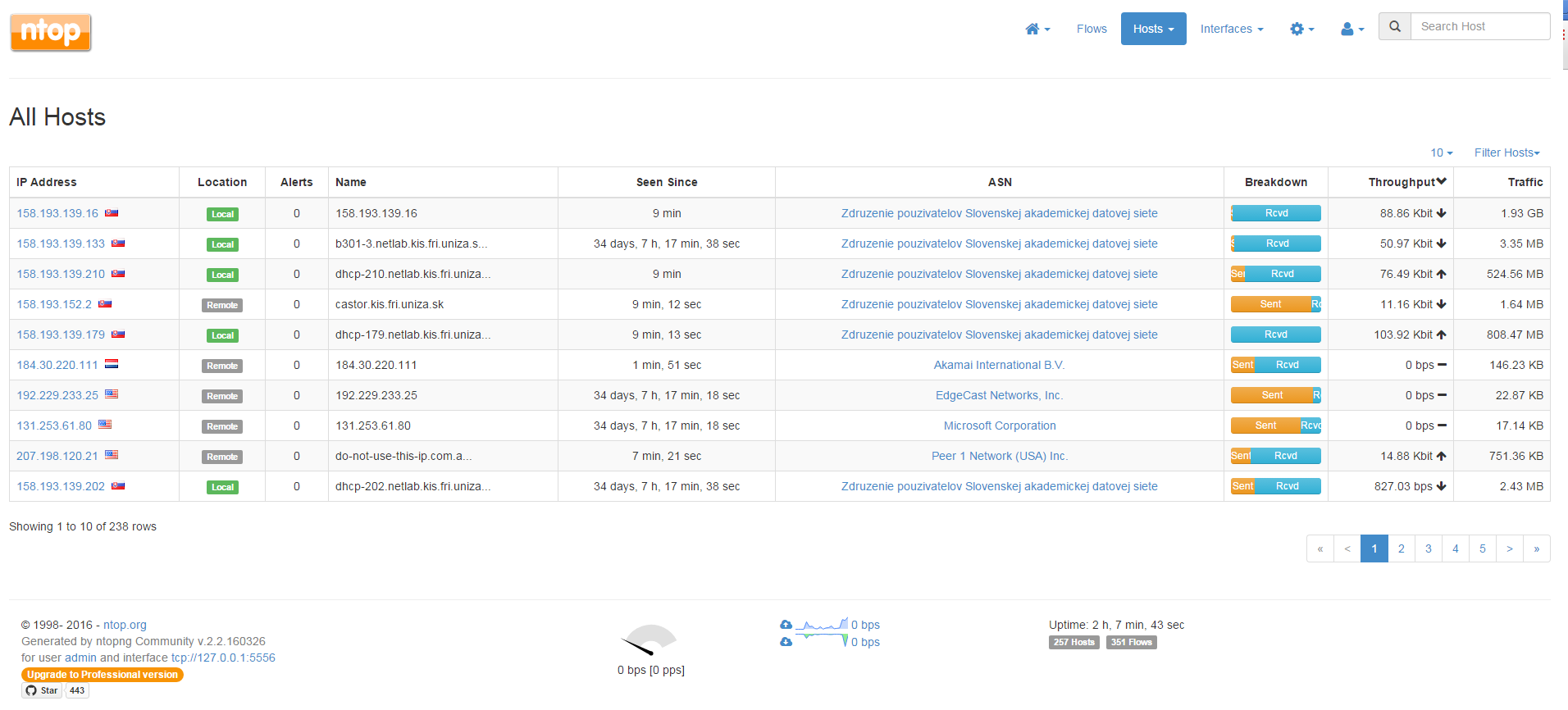
#### Návod na NTOPng (<http://158.193.139.16:3000/>)

Po prihlásení (Meno: admin, Heslo: Projekt59) na úvodnej stránke môžeme vidieť TOP FLOW TAKERS, teda siete s najväčšou dátovou komunikáciou. Samorejme ako prvé si musíme vybrať správne rozhranie v pravo hore, z ktorého nám budú chodiť informácie:



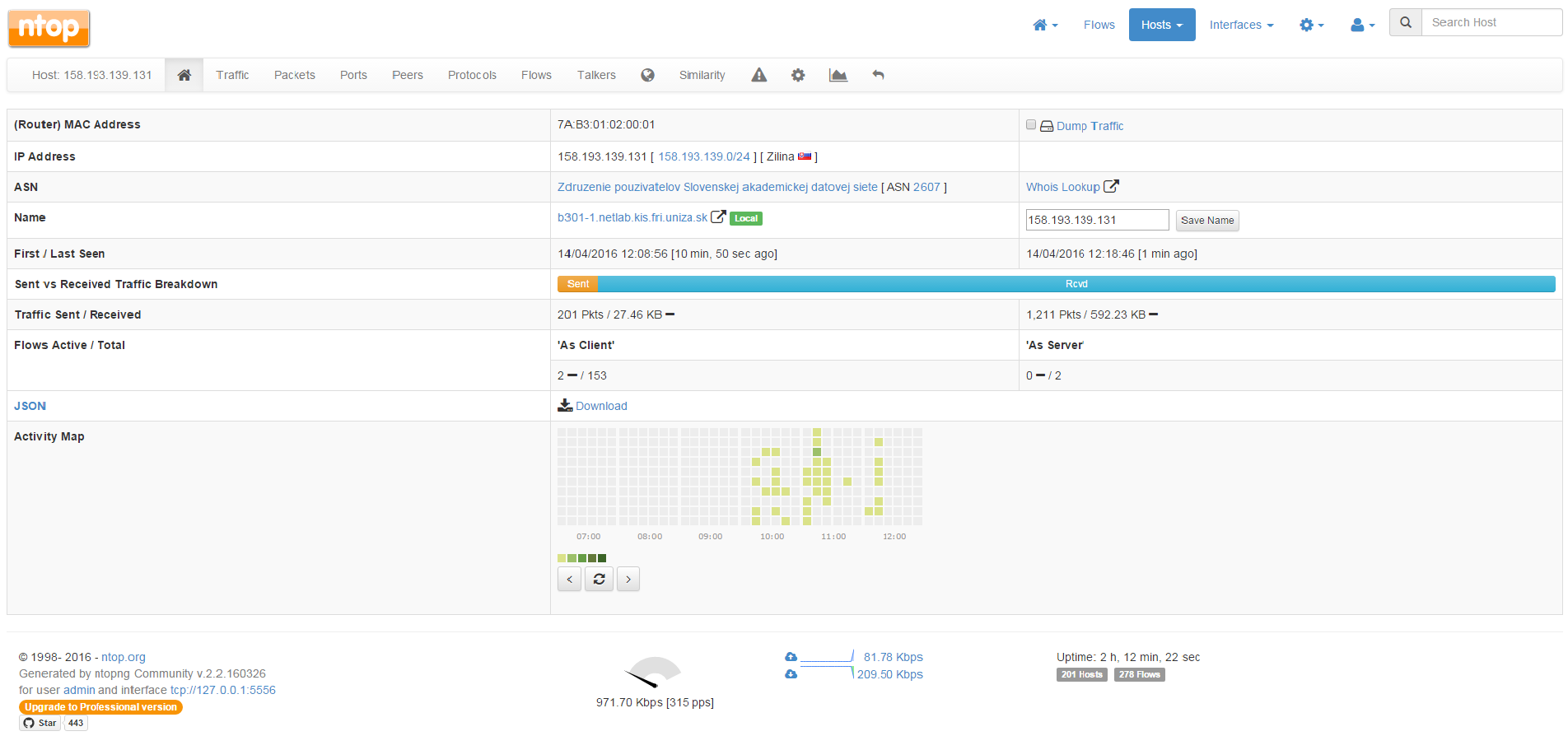
Obrázok . NTOPng - výber rozhrania

Zaujímať by nás mohla hlavne záložka Hosts na hornej lište a následne odkaz Hosts, kde vidíme zoznam pripojených hostov:



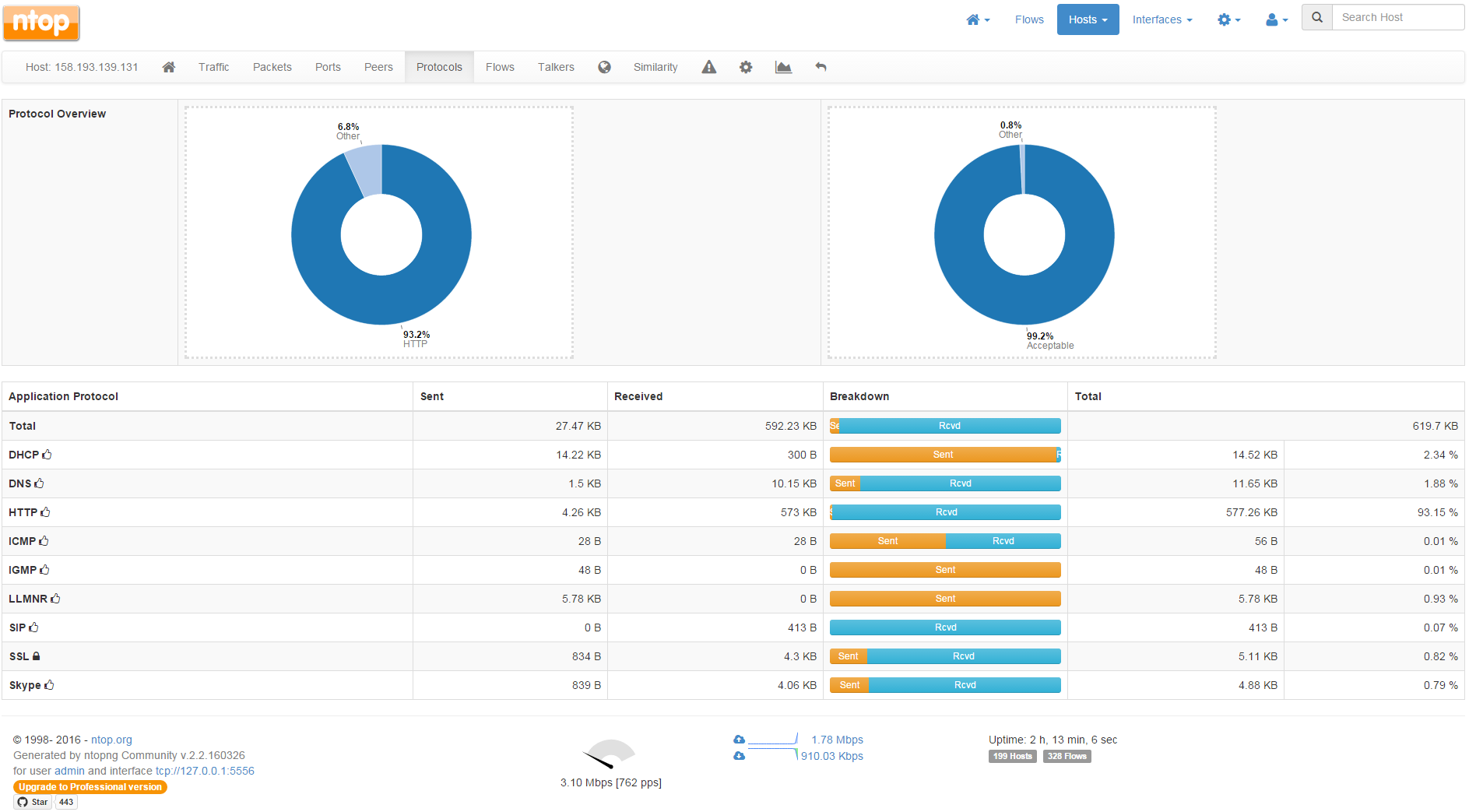
Obrázok . NTOPng - zoznam pripojených hostov

Následne si môžeme kliknúť na konkrétneho hosta a zobraziť detailnejšie informácie o ňom.



Obrázok . NTOPng - informácie o hostovi

Rovnako dôležitá je aj záložka Protocols, kde si môžeme zobraziť informácie o protokoloch prebiehajúcich sieťov:



Obrázok . NTOPng - protokoly v sieti

### Pmacct

Ako náhrada nProbe nástroja môže slúžiť nástroj **pmacct,** ktorý nainštalujeme nasledovne:

#### Inštalácia pmacct

wget http://www.pmacct.net/pmacct-1.5.3.tar.gz

tar xzvf pmacct-1.5.3.tar.gz

cd pmacct-1.5.3/

./configure

make

sudo make install

Pri konfigurácií sa vyskytli problémy s niektorými chýbajúcimi balíčkami. Tie bolo treba stiahnuť a doinštalovať:

wget <http://ftp.cz.debian.org/debian/pool/main/a/automake-1.14/automake_1.14.1-4_all.deb>

dpkg -i automake\_1.14.1-4\_all.deb

#### Konfigurácia pmacct

V zdrojovej složke pmacct-1.5.3/ sú v zložke examples prístupné príkladné konfigurácie. Tu som si zvoli základnú konfiguráciu a skopíroval ju do zdrojovej zložky nasledovne

cp pmacct-1.5.3/examples/pmacctd-imt.conf.example pmacct-1.5.3/pmacctd.conf

Ďalším krokom je natiahnutie konfiguračného súboru:

pmacctd -f pmacctd.conf

#### Spustenie pmacct

Spustiť pmacct v takej forme, aby nahradil sondu nProbe, sa nám nepodarilo. Nepodarilo sa nám docieliť, aby posielal informácie na kolektor NtopNG, tak ako to robí sonda nProbe.

Podarilo sa nám však rovnaké informácie získať v command line. Informácie o zdrojových a cieľových IP adresách, o počte paketov prijatých a odoslaných medzi nimi.

Tieto informácie môžeme zobraziť v dvoch stavoch, real-time zobrazenie nám informácie vypisuje priamo na obrazovku, prepínačom -r nastavíme refresh-time.

pmacctd -c src\_host,dst\_host -P print -r 10 -i eth0

Druhým štýlom je len spustenie daemona, a následné samostatné zobrazenie.

pmacctd -D -i eth0

pmacct -s

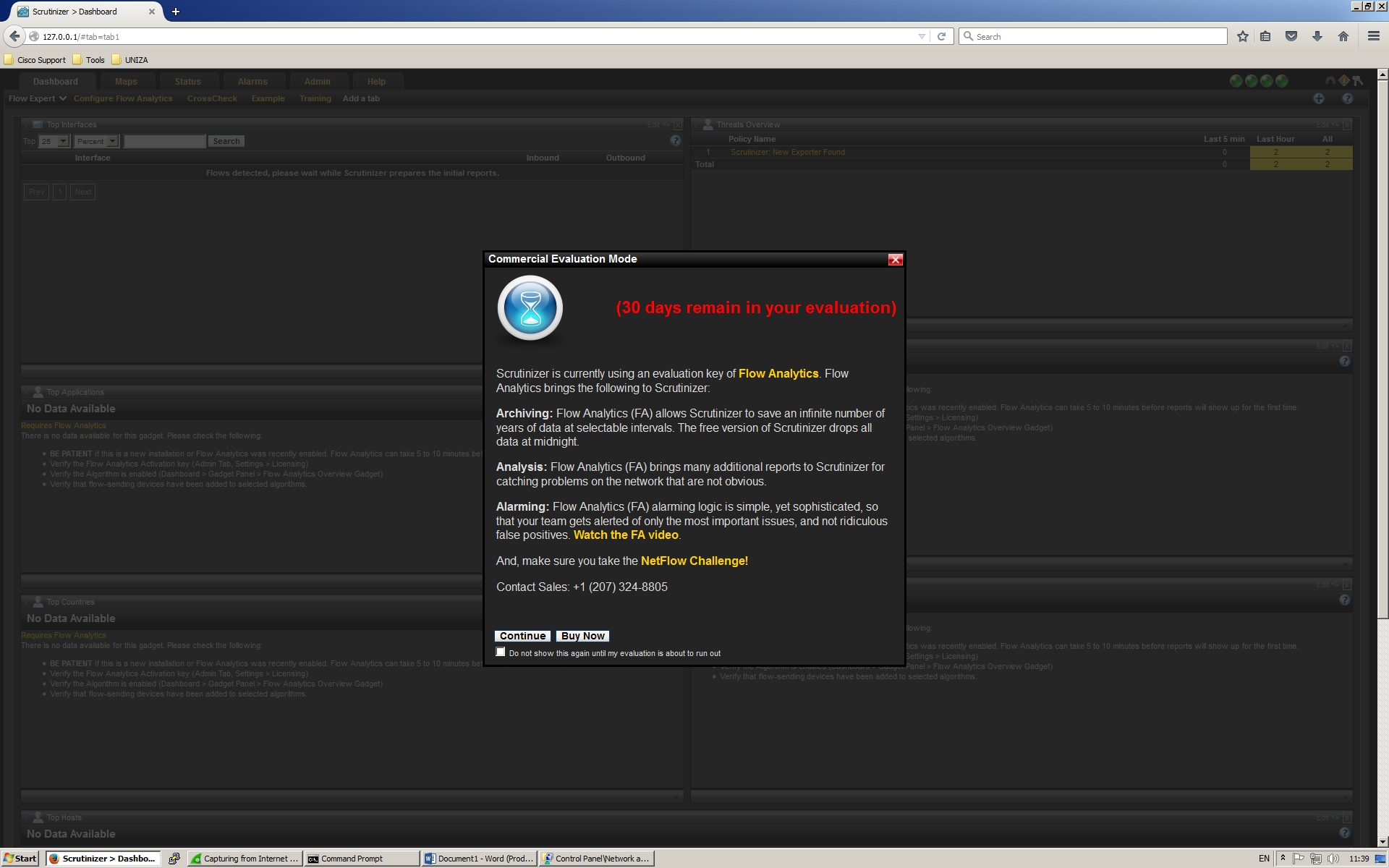
### Scrutinizer

**Inštalácia**

Inštalácia prebieha jednoducho. Stiahne sa inštalačný súbor exe, spustí sa a užívateľ si nastaví počas inštalácie jednotlivé veci podľa vlastnej potreby. Je treba spomenúť, že ak je na počítači/serveri nainštalovaný skype, je požadované pre správne fungovanie Scrutinizer-a, nastaviť inú hodnotu pre TCP port ako je prednastavená na 80. Scrutinizer počúva na portoch pre NetFlow 2055, 2056, 4432, 4739, 9995, 9996, 6343.

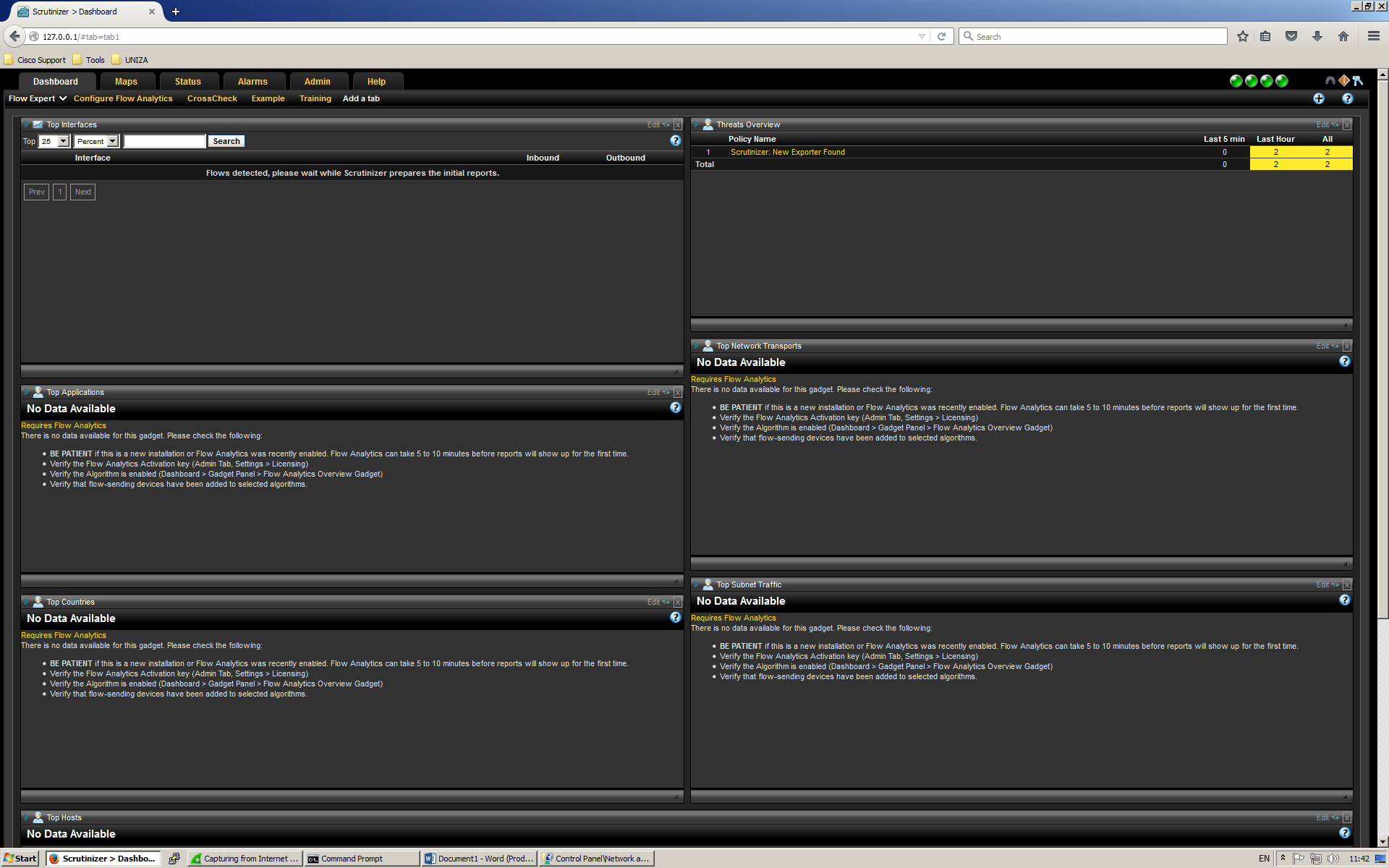
**Spustenie**

Pri spustení nás Scrutinizer upozorní, že licencia vyprší o 30 dní.



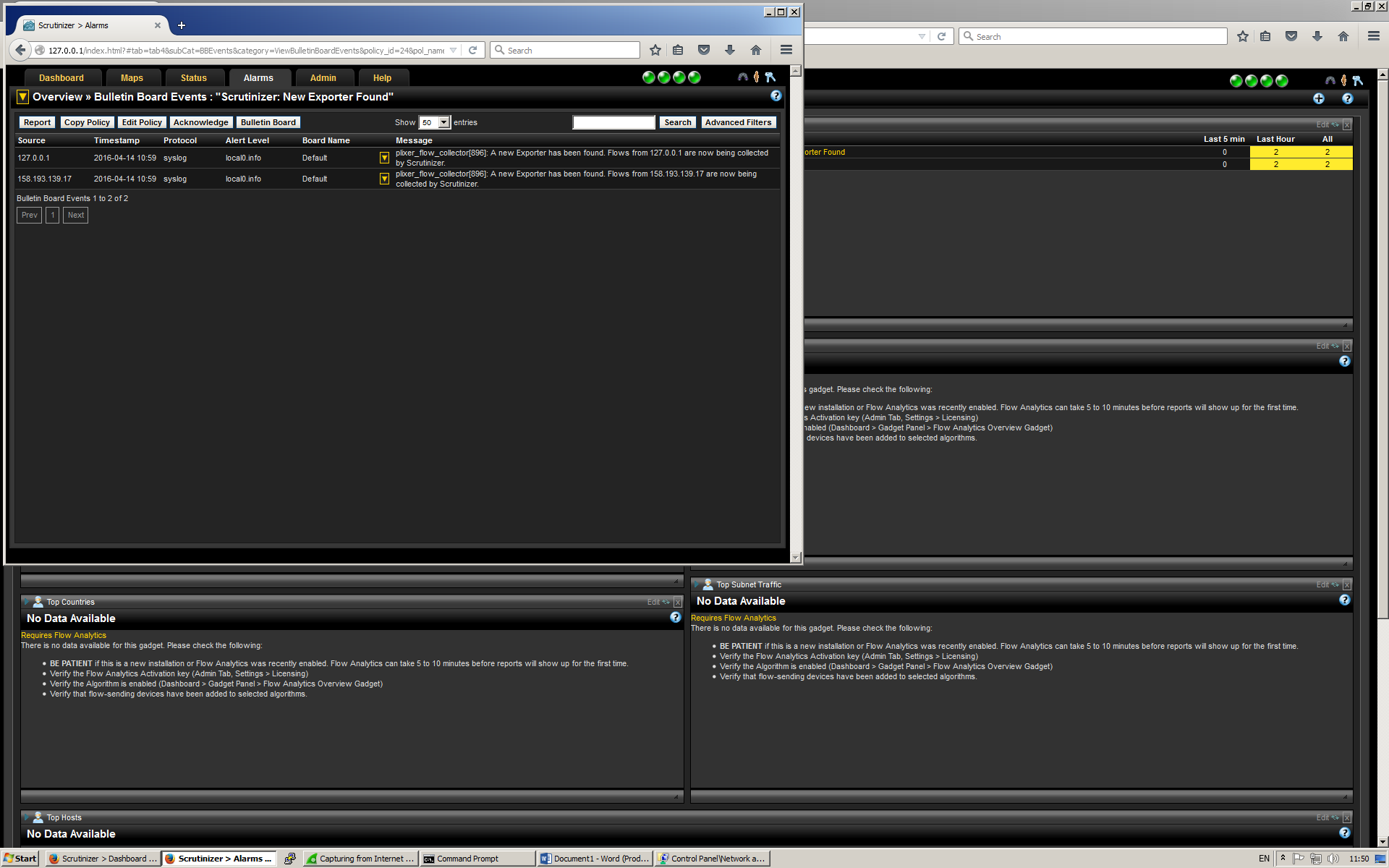
Obrázok . Zobrazenie licencie

Následne ak je dobre nastavené zariadenie posielajúce NetFlow (ASA 5510), malo by sa toto zariadenie zobraziť vo vrchnom okne zvanom “Threats Overview”. V našom prípade našlo ASA 5510 firewall a samého seba (127.0.0.1).



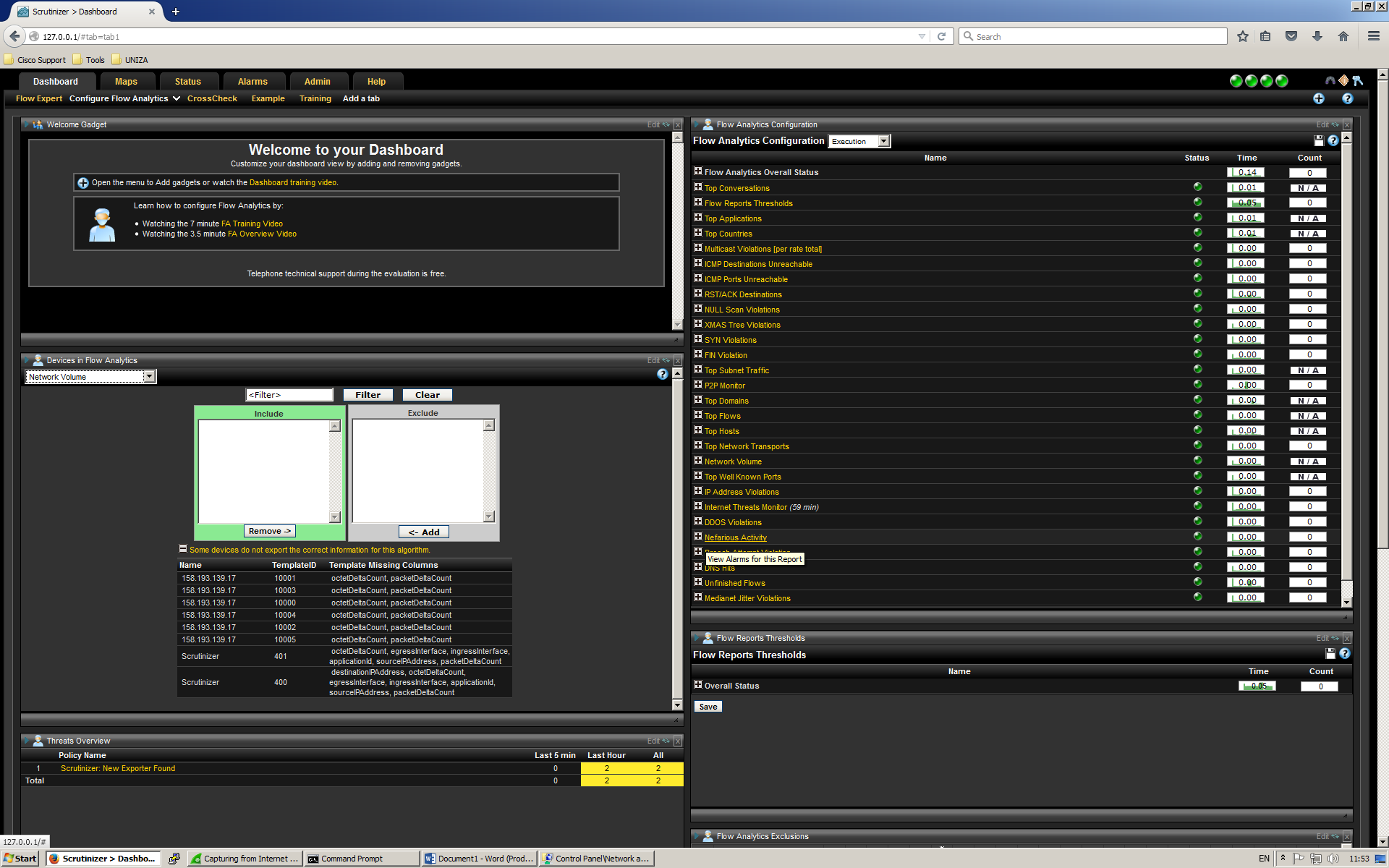
Obrázok . Zobrazenie upozornení

Po kliknutí na “Scrutinizer: New Exporter Found” vidíme popis jednotlivých nájdených zariadení.



Obrázok . Zobrazenie podrobností o exporteroch

Následne v záložke “Configure Flow Analytics” treba nastaviť algoritmy pre dané zariadenia. V našom prípade ale nastal problém s tým, že nevieme zariadenie ASA 5510 pridať do jednotlivých algoritmov, z ktorých by vznikali následne štatistiky. Dôvod je ten, že posielané NetFlow dáta z ASA 5510 nevie Scrutinizer spracovať, kvôli chýbajúcim dátam (Template Columns).



Obrázok . Chybné hlášky pri nastavení exportera

Pri testovaní Scrutinizera s ASA 5520 sme vedeli do niektorých algoritmov pridať zariadenie a následne sme videli aj štatistiky tomu zodpovedajúce.

To že na zariadenie, kde je Scrutinizer nainštalovaný sa posielajú NetFlow dáta z ASA 5510, dokumentuje aj výpis z Wiresharku, kde je vidieť, že NetFlow dáta naozaj prichádzajú. Na obrázku je aj vidieť, že ASA 5510 posiela NetFlow verzie 9. Ale svedčí o tom aj fakt, že ho samotný Scrutinizer vidí. Problém je len v spracovaní samotných dát.



Obrázok . Výpis vo wireshark-u

### PRTG

**Inštalácia PRTG Network Monitor**

Na webe <https://shop.paessler.com/shop/free_license/?showkey=1&download=1> stiahneme software ktorý je zadarmo. Po dobu 30 dní umožňuje neobmedzený počet senzorov. Po uplynutí 30tich dní len 100 senzor čo je stále veľmi dostačujúce. Počas inštalácie program bude pýtať licenčný kľuč ktorý je na webstránke priloženej vyššie.

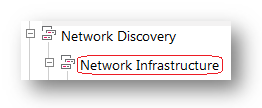
**Nastavenie PRTG**

Po prihlásení sa do PRTG pod administrátorským kontom klikneme v hornej lište zobrazovanej stránky na sekciu ***Devices.***



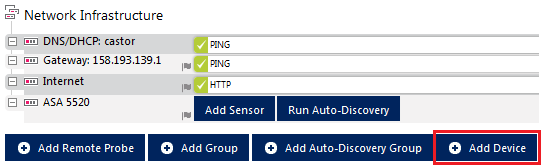
Obrázok . – 1. krok pre nastavenie PRTG

Následne pod ***Network Discovery*** klikneme na ***Network Infrastructure.***



Obrázok . – 2. krok pre nastavenie PRTG

Po načítaní stránky klikneme na tlačidlo **Add Device**.



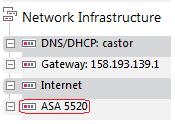
Obrázok . – 3. krok pre nastavenie PRTG

Zobrazí sa nám stránka kde môžeme zmeniť do akej skupiny sa zariadenie pridá. Klikneme ***Continue***. Následne sa zobrazia informácie zariadenia ktoré treba doplniť. Názov (ľubovoľný) a IP adresa portu zariadenia 158.193.139.81.



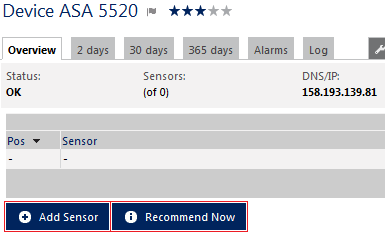
Obrázok . - 4. krok pre nastavenie PRTG

Klikneme ***Continue*** a následne na nami vytvorené zariadenie s názvom ASA 5520.



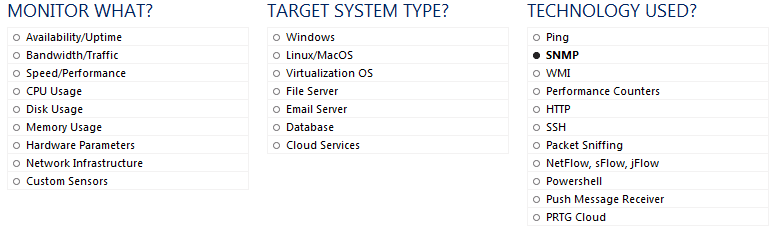
Obrázok . – 5. krok pre nastavenie PRTG

Po načítaní stránky klikneme na **Add Sensor**.



Obrázok . - 6. krok pre nastavenie PRTG

Tu následne vyhľadať senzor podľa toho čo chcem monitorovať, aký systém alebo akú technológiu použiť. V tomto prípade možnosť **Netflow, sFlow, jFlow.**



Obrázok . - 7. krok pre nastavenie PRTG

Ďalších krokom je výber z ponúknutých senzorov. My sme vybrali **Netflow v9.** Kde môžeme vidieť kopu rôznych údajov a grafov.



Obrázok . – PRTG Netflow v9 senzor

# SNMP - Simple Network Management Protocol

SNMP je protokol aplikačnej vrstvy, ktorý slúži na vzdialenú správu a monitorovanie zariadení v počítačovej sieti. Je súčasťou sady protokolov TCP/IP. Jedná sa o sériu štandardov (popísaných v RFC od IETF), ktorá sa prvýkrát objavila už v roku 1988 a vďaka širokej podpore zo strany výrobcov sieťových zariadení je tento protokol veľmi rozšírený a všeobecne považovaný za štandard v oblasti monitorovania a správy sietí.. Podpora SNMP je nielen u serverov a aktívnych sieťových prvkov (ako sú switche a routre), ale takmer u každého zariadenia, ktoré komunikuje po sieti (tlačiarne, UPS, WiFi AP, FW, rôzne sieťové čidlá atď.).

Pomocou SNMP môžeme čítať alebo nastavovať hodnoty na zariadení, alebo dostať upozornenie na nejakú definovanú udalosť. Hodnoty môžeme načítať jednorazovo v prípade potreby alebo v pravidelnom intervale. Ďalšie spracovanie už záleží na nás (alebo na použitej aplikácii), či iba zobrazíme danú hodnotu alebo budeme vykresľovať graf (napríklad priebeh teploty či vyťaženie procesora v čase).

## Vznik a verzie SNMP

Protokol SNMP vznikol na konci 80-tych rokov na pracovnom výbore IAB (Internet Architecture Board) za účelom správy smerovačov internetu. Vyvinul sa ako jeden variant protokolu SGMP (Simple Gateway Monitoring Protocol), ktorý bol navrhnutý koncom roku 1987 práve pre výmenu informácií medzi smerovačmi a bránami v internete (v tom čase ešte len v akademickej sieti). Druhým variantom, ktorý vznikol z protokolu SGMP na pôde organizácie ISO, bol protokol CMIP (Common Management Information Protocol), ktorý podobne ako celá sada protokolov ISO, nenašiel väčšiu podporu u výrobcov ani používateľov a nedočkal sa tak významnejšieho rozšírenia. Na druhej strane SNMP protokol (rovnako ako sada protokolov TCP/IP) preukázal veľkú životaschopnosť. Vďaka relatívnej jednoduchosti implementácie sa stal tento protokol veľmi populárnym, pretože presne spĺňal požiadavky na vzrastajúce potreby sieťovej správy. Od roku 1989, kedy bol formalizovaný, sa stal štandardom pre správu sietí založených na protokole TCP/IP, slúžiaci ako jednotiaci prostriedok pre správu konfigurácie, kapacity, bezpečnostného zaistenia sietí a všetkých zariadení siete. Protokol SNMP prešiel od svojho vývoja viacerými inováciami a v súčasnej dobe existuje v troch verziách.

### SNMPv1

Počiatočná verzia SNMP protokolu bola definovaná v roku 1988. Hlavným nedostatkom tejto verzie je slabé zabezpečenie komunikácie. Systém autorizácie prístupu je veľmi primitívny, keďže sa využíva metóda overovania užívateľov pomocou komunít (heslá) a prenášané dáta aj s heslami nie sú šifrované. V dnešnej dobe sa už táto verzia používa už len v starších a lacnejších zariadeniach.

### SNMPv2

Hlavným cieľom druhej vezie bolo poskytnúť silnejšie zabezpečenie protokolu prostredníctvom overovania užívateľov lokálnymi identifikátormi, nazývanými skupiny (parties). Táto verzia priniesla aj vylepšenia výkonu, umožnila komunikáciu medzi manažérmi a rozšírenie SNMP počítadiel z 32 bit na 64 bit (pre podporu rýchlejších sieťových rozhraní). SNMPv2 sa z dôvodu komplexnosti skupinového systému zabezpečenia príliš neuplatnil a preto sa vyvinuli viaceré "dcérske" verzie SNMPv2p, SNMPv2c, SNMPv2u... Najúspešnejším a najširšie podporovaných sa stal protokol SNMPv2c, ktorý si ponechal vylepšenia z SNMPv2, ale v oblasti zabezpečenia používa tú istú metódu ako verzia SNMPv1.

### SNMPv3

Najnovší protokol z rodiny SNMP bol navrhnutý v roku 1998. Sú ponechané najlepšie vlastnosti z predchádzajúcej verzie 2 a prináša do komunikácie bezpečnostné prvky vo forme kryptovania dátových paketov a autentifikácie viacerých užívateľov.

## Architektúra systému správy SNMP

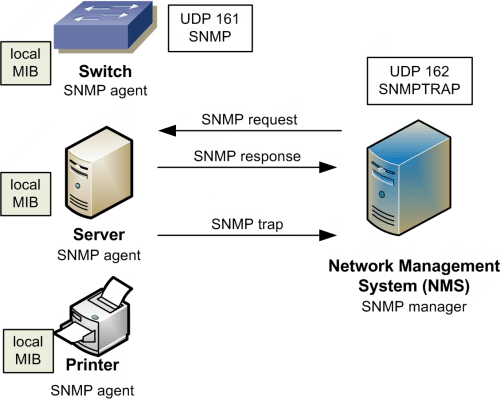
SNMP komunikácia je založená na modeli **Manager – Agent** (Obrázok 6.1) a umožňuje prenos medzi správcom siete – manažérom a agentmi na jednotlivých sieťových zariadeniach (hub, switch, router, počítač,...). K tomu vyžaduje, aby každé zariadenie siete poskytovalo isté základné informácie o sebe samom a zároveň uľahčovalo pridávanie ďalších informácii, špecifických pre dané zariadenie. Tieto základné a prídavné informácie sa spolu nazývajú **MIB (Management Information Base).** Systém správy siete postavený nad protokolom SNMP definuje dva druhy zariadení.

### SNMP manažér

Je program, ktorý beží na sieťovej monitorovacej stanici. U väčších systémov ide väčšinou o vyhradenú výkonnú pracovnú stanicu, na ktorej beží sieťový riadiaci systém **(NMS – Network Management System)**. SNMP manažér získava informácie o sieti dotazovaním sa na jednotlivých SNMP agentov pomocou SNMP operácii. Cieľom je získať všetky potrebné informácie o danom zariadení, ktoré agent reprezentuje. SNMP manažér poskytuje väčšinou grafické rozhranie, ktoré umožňuje prezentáciu získaných dát, sledovanie sieťových alarmov a archiváciu dát (napr. k analýze časového vývoja).

### SNMP agent

Je malý program, ktorý beží na sledovanom zariadení. Toto zariadenie reprezentuje a odpovedá na dotazy SNMP manažéra. Agent preto neustále monitoruje a zbiera informácie o všetkých dostupných funkciách a stavoch daného zariadenia. K získaniu informácii o zariadení musí manažér vyslať požiadavku na dané zariadenie a prejsť informácie poskytované agentom. Musí prejsť celou stromovou štruktúrou MIB až k objektu, ktorý obsahuje potrebné dáta, aby mohol získané informácie interpretovať.



Obrázok . – SNMP Manager – SNMP Agent

Informácie môžu byť vysielané agentom aj bez vyžiadania manažéra. Ak agent zaznamená isté podmienky napr. hardwarovú poruchu, prekročenie určitej hodnoty, atď. Vtedy agent vyšle informáciu, nazývanú trap, sám bez vyžiadania (to zabezpečujú **thresholdy**). Toto je dôležité pre zaistenie okamžitej informovanosti o vážnejších problémoch, ktoré by boli pri bežnej **polling aktivite** manažéra (procedúra vyžiadania informácii nastavená v určitých intervaloch) prehliadnuté. Pre väčšinu informácii nie je dôležité kontinuálne monitorovanie (zbytočne zaťažuje sieť), a tak kombinácia polling aktivity manažéra a trap aktivity agenta zaisťuje potrebnú efektivitu.

## Autentizácia, bezpečnosť a komunikácia

Informácie odosielané v SNMP paketoch sú štandardne uložené v čistom texte. Aby dáta zo zariadení mohol čítať alebo nastavovať len oprávnený používateľ, tak sa používa určitá forma autentizácie. Pre SNMPv1 a SNMPv2c sa používa *community string*, teda textový reťazec, a ten sa prenáša v každom pakete ako čistý text. Presnejšie sa používajú tieto dve heslá *read community string*, ktorý povoľuje prístup len na čítanie a *write community string*, ktorý povoľuje aj zápis. SNMPv3 prináša niekoľko vylepšení v oblasti bezpečnosti a to je autentizácia pomocou mena a hesla (User-based Security Model), ochranu proti zmene či odhaleniu (kontrolné súčty MD5 a SHA a šifrovanie komunikácie pomocou DES) a riadenie prístupu k jednotlivým objektom (View Access Control model).

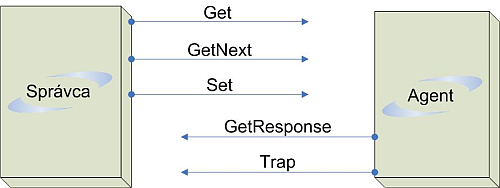
Protokol SNMP môže bežať nielen nad IP, ale aj ďalšími protokolmi, ako OSI CLNS, AppleTalk DDP či Novel IPX. V praxi sa ale stretneme takmer výlučne s IP sieťami.

SNMP využíva pre komunikáciu protokol UDP, ktorý je rýchly, ale neobsahuje mechanizmus pre overenie doručenia (ktorý je potrebný v TCP). SNMP od verzie 2 obsahuje vlastný mechanizmus na kontrolu doručenia. Každá SNMP správa sa zapuzdrí do jedného UDP paketu. Keď SNMP Manager posiela dotaz SNMP Agentovi (klientovi), tak zdrojový port je dynamicky volený a cieľový je defaultne port 161 (na ňom počúva SNMP Agent). SNMP Agent odpovedá z portu 161 na dynamický port správcu. Trapy odosiela SNMP Agent z dynamického portu na adresu SNMP Managera port 162.

## SNMP operácie a SNMP formát paketu správy

### SNMP verzia 1

SNMPv1 bola prvá implementácia SNMP protokolu v praxi a používa päť operácií:



Obrázok . - Komunikácia Správca - Agent

* **GetRequest** – žiadosť o informáciu, ktorú posiela manažér agentovi aby získal informácie o stave alebo hodnote istého objektu. Ide o príkaz „Read“. V rámci jedného príkazu je možné žiadať informácie o viacerých objektoch. To redukuje nutnú komunikáciu medzi zariadeniami.
* **GetNextRequest** – žiadosť o ďalšiu informáciu na nižšej vrstve MIB štruktúry.
* **GetResponse** – tento príkaz je vysielaný agentom ako odpoveď na príkaz GetRequest, ktorým vracia vyžiadanú informáciu.
* **SetRequest** – príkaz nastavuje hodnotu premennej u MIB agenta. Ide o príkaz „Write“. Toto nie je umožnené na každom zariadení (závisí od výrobcu). V prípade, že táto možnosť nie je prístupná, tak nie je možné zariadenie spravovať, ale len monitorovať.
* **Trap** – tento príkaz je vysielaný agentom manažérovi ako oznámenie o nejakej významnej udalosti. Na rozdiel od predchádzajúcich príkazov, nie je v tomto prípade očakávaná odpoveď.

http://www.kiwiki.info/images/8/83/Jk_dp_7.png

Obrázok . - Formát SNMP správy

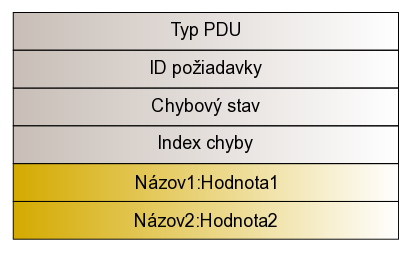
Základný formát paketu SNMP správy (Obrázok 6.3) je jednoduchý a presne daný. Hlavička obsahuje určenie použitej **verzie** **SNMP** protokolu a **community string** (groupy) do ktorej patria obe komunikujúce entity. Slúži na overenie totožnosti medzi agentom a správcom. Agent vždy patrí iba do jednej komunity, naopak správca môže byť členom viacerých komunít. Správca môže takto monitorovať viacero zariadení patriacich do rôznych komunít. Veľkosť hlavičky paketu, poľa pre verziu a komunitu, má pevnú šírku.

V poli **PDU (Protocol Data Unit)** je uvedená samotná protokolová operácia. Má premenlivú veľkosť závislú od množstva prenášaných dát (Tabuľka 6.1).

|  |  |  |
| --- | --- | --- |
| **Názov** | **Veľkosť (bitov)** | **Význam** |
| Verzia | 32 | Verzia protokolu |
| Komunita | 32 | Názov komunity |
| PDU | Premenlivá | Dátové pole |

Tabuľka 7.1 - Formát SNMP správy

* **Typ PDU** – v tomto poli je uvedená protokolová operácia, Get, GetNext a pod. Všetky operácie používajú rovnaký formát správ, výnimkou sú nevyžiadané Trap správy, ktoré používajú iný formát správy.
* **ID požiadavky -** je číslo na základe, ktorého sa páruje požiadavka správcu s odpoveďou agenta.
* **Chybový stav** - hovorí správcovi v akom stave je jeho požiadavka. Má šesť hodnôt
* **Index chyby** - ukazuje na objekt, ktorý generoval chybu. Ak v poli pre chybový stav je nula, index chyby je nulový. V žiadosti je index chyby vždy nulový.



Obrázok . - Formát SNMP PDU správy

|  |  |  |
| --- | --- | --- |
| **Hodnota** | **Kód** | **Popis** |
| 0 | noError | Nevyskytla sa žiadna chyba |
| 1 | tooBig | Pole PDU je príliš veľké k transportu |
| 2 | noSuchName | Meno požadovaného objektu sa nenašlo |
| 3 | badValue | Hodnota v požiadavke nezodpovedá štruktúre príjemcu |
| 4 | readOnly | Hodnota je iba na čítanie |
| 5 | genErr | Neznáma chyba |

Tabuľka 7.2 - Chybový stav správy

|  |  |
| --- | --- |
| **Názov** | **Veľkosť (bit)** |
| PDU Typ | 32 |
| ID požiadavky | 32 |
| Status chyby | 32 |
| Index chyby | 32 |
| Dáta | Premenlivá |

Tabuľka 7.3 - Formát poľa PDU

**Trap** ako jedinú operáciu negeneruje správca, ale agent, ktorý touto správou informuje správcu o výskyte dôležitý udalostí. Jednou zo situácií, kedy môže agent generovať Trap správu je, keď správca sa pokúša komunikovať s agentom patriacim do inej komunity ako správca. Vtedy agent túto situáciu hodnotí ako neautorizovaný prístup a informuje o tom svojho správcu.

Formát Trap je odlišný od formátu ostatných protokolových operácií.

* **Typ PDU -** v tomto poli je uvedená iba jedna hodnota Trap správa.
* **Skupina -** je identifikátorom objektu pre skupiny, ktorý generoval nevyžiadanú (Trap) správu.
* **Adresa -** agenta je 32 bitové číslo IP adresy agenta, ktorý generoval nevyžiadanú správu.
* **Generický typ správy -** udáva typ preddefinovanej nevyžiadanej správy. Dôvod prečo bola správa generovaná. Má sedem preddefinovaných stavov (Tabuľka 6.4).
* **Špecifický typ správy -** udáva špecifický typ nevyžiadanej správy. Upresňuje dôvod generovania správy.
* **Časová pečiatka -** je čas kedy bola správa generovaná.

[](http://www.kiwiki.info/index.php/S%C3%BAbor:Jk_dp_9.png)

Obrázok . - Formát SNMP Trap správy

|  |  |
| --- | --- |
| **Hodnota** | **Popis** |
| 0 | Studený štart |
| 1 | Teplý štart |
| 2 | Výpadok linky |
| 3 | Nahodenie linky |
| 4 | Neprešlo overenie totožnosti |
| 5 | Strata suseda EGP |
| 6 | Vyhradené |

Tabuľka 7.4 - Príčiny generovania Trap správy

Prehľad veľkosti v bitoch, ktoré sú vyhradené pre jednotlivé polia nevyžiadanej správy sú uvedené v Tabuľke 6.5.

|  |  |
| --- | --- |
| **Názov** | **Veľkosť (bit)** |
| Typ PDU | 32 |
| Skupina | Premenlivá |
| Adresa agenta | 32 |
| Generický typ správy | 32 |
| Špecifický typ správy | 32 |
| Časová známka | 32 |
| Dáta | Premenlivá |

Tabuľka 7.5 - Formát Trap správy

### SNMP verzia 2

Druhá verzia prichádza z určitými vylepšeniami oproti prvej verzie protokolu určenými na posilnenie SNMPv1 v mnohých oblastiach, vrátane definícií MIB objektov a bezpečnosti. V druhej verzii pribudli dve nové protokolové operácie **GetBulk** a **Inform** .

* **GetBulk** slúži na čítanie veľkého počtu dát, napríklad niekoľko riadkov v tabuľke.
* Operácia **Inform** umožňuje výmenu správ medzi viacerými správcami.

Počas vývoja druhej verzie protokolu sa do praxi dostali štyri jeho variácie pod označením: SNMPv2p, SNMPv2c, SNMPv2u s SNMPv2\*. Každý variant druhej verzie protokolu používa iný formát hlavičky správy. Formát dátového poľa PDU je pre všetky varianty rovnaký.

Základný formát dátového poľa PDU je rovnaký ako pri predchádzajúcej verzii (Obr. 6.4). V poli Typ PDU v druhej verzii protokolu sú hodnoty uvedené v Tabuľke 6.6.

|  |  |
| --- | --- |
| **Hodnota** | **Typ PDU správy** |
| 0 | Get |
| 1 | GetNext |
| 2 | Response |
| 3 | Set |
| 4 | Trap SNMPv1 |
| 5 | GetBulk |
| 6 | Inform |
| 7 | Trap SNMPv2 |
| 8 | Report |

Tabuľka 7.6 - Typ PDU SNMPv2

V poli Chybový stav (Obrázok 6.4) druhej verzii SNMP protokolu je preddefinovaných viac stavov ako v prvej verzii implementácii protokolu. Prvých šesť stavov (Tabuľka 6.2 - hodnoty 0-5) je totožných v oboch verziách SNMP protokolu. Rozšírenie chybových stavov druhej verzie je uvedené v Tabuľke 6.7.

|  |  |  |
| --- | --- | --- |
| **Hodnota** | **Kód** | **Popis** |
| 6 | noAccess | Odmietnutý prístup k objektu |
| 7 | wrongType | Typ objektu je nesprávny |
| 8 | wrongLength | Špecifikovaná dĺžka pre objekt je nesprávna |
| 9 | wrongEncoding | Nesprávne šifrovanie |
| 10 | wrongValue | Zadaná hodnota je neprípustná |
| 11 | noCreation | Premenná neexistuje, nie je možné ju vytvoriť |
| 12 | inconsistentValue | Špecifikovaná hodnota je blokovaná, alebo nie je možné priradiť hodnotu v danom okamihu |
| 13 | resourceValue | Pokus o nastavenie hodnoty, ktorej zdroje nie sú k dispozícii |
| 14 | commitFaild | Pokus o nastavenie hodnoty zlyhal |
| 15 | undoFaild | Pokus o nastavenie hodnoty zo skupiny premenných zlyhal a pokus vrátiť späť hodnoty ostatných premenných nebol úspešný |
| 16 | authorizationError | Problém s autorizáciou |
| 17 | notWritable | Premennú nie je možné vytvoriť ani zapísať |
| 18 | incosistentName | Premenná neexistuje |

Tabuľka 7.7 - Rozšírený chybový stav správy SNMPv2

Protokolová operácia **GetBulk** používa špeciálny formát dátového poľa (PDU). Hlavička správy je nasledovná:

|  |  |  |
| --- | --- | --- |
| **Názov** | **Veľkosť (bit)** | **Popis** |
| Typ PDU | 32 | Názov operácie - GetBulk |
| ID požiadavky | 32 | Párovanie požiadavky s odpoveďou |
| Bez opakovania | 32 | Počet objektov bez opakovaného čítania v požiadavke |
| Max opakovanie | 32 | Počet iterácií pri čítaní objektov z tabuľky |

Tabuľka 7.8 - Formát PDU správy GetBulk

### SNMP Verzia 3

Posledná verzia protokolu, ktorá bola aplikovaná do praxe mala za úlohu vyriešiť problémy, ktoré vznikli s nasadením rôznych variácií SNMP protokolu verzie 2. Tretia verzia používa rovnaké protokolové operácie ako SNMPv2 aj rovnaký formát dátového poľa PDU.

Hlavné vylepšenie SNMPv3 je v bezpečnosti protokolu. Obsahuje niekoľko úrovní zabezpečenia, ktoré umožňujú šifrovanie dát, alebo prístup k dátam na základe užívateľských prístupov. Napríklad konkrétny používateľ má prístup iba k niektorým údajom. Použitie nových bezpečnostných prvkov v SNMPv3 umožňuje bezpečnú správu a manažovanie sieťových zariadení cez verejnú sieť Internet.

|  |  |  |
| --- | --- | --- |
| **Názov** | **Veľkosť (bit)** | **Popis** |
| Verzia | 32 | Verzia SNMP protokolu |
| ID správy | 32 | Párovanie požiadavky s odpoveďou |
| Max veľkosť správy | 32 | Maximálna veľkosť správy, ktorú odosielateľ môže prijať |
| Indikátor správy | 8 | Riadi spracovanie správy |
| Bezpečnostný model | 32 | Indikuje použitý bezpečnostný model |
| Bezpečnostné parametre | Premenlivá | Skupina polí, ktoré indikujú použité bezpečnostné parametre |
| Pole PDU | Premenlivá | Dáta spolu s parametrami, ktoré bližšie určujú prenášané údaje |

Tabuľka 7.9 - Formát hlavičky správy SNMPv3

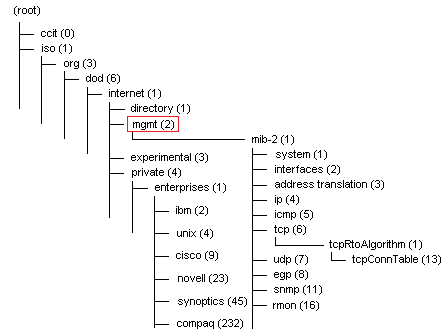
## Management Information Base - MIB

Agenti ukladajú dáta vo forme objektov do **MIB databázy**. Databáza je tvorená stromovou štruktúrou a skladá sa z objektov a ich atribútov, ktoré objekt popisujú. **SMI (Structure and Identification of Management Information)** definuje pravidlá pre pomenovávanie typov dát. Podľa SMI je každý uzol v databáze popísaný atribútmi.

|  |  |
| --- | --- |
| **Atribút** | **Popis** |
| Object | Meno objektu |
| Syntax | Typ objektu |
| Description | Popis objektu |
| Access | Prístupové práva k objektu |
| Status | Status |

Tabuľka 7.10 - Atribúty MIB objektov

V súčasnosti sa používajú dve verzie databázy MIB-2 a MIB-1 a sú navzájom kompatibilné. Stromová štruktúra MIB databázy je znázornená na Obrázku 6.6.



Obrázok . - Stromová štruktúra MIB databázy

Každá položka v MIB databáze sa dá jednoznačne popísať pomocou **identifikátoru objektu (OID).** Identifikátor objektu je celá cesta z koreňa databázy (ROOT) po položku. OID je tvorený číslom uzla, jednotlivé úrovne sú oddelené bodkou. Zvýraznená položka má OID .1.3.6.1.2. alebo pomocou popisov z návestí ako .iso.org.dod.internet.mgmt.

SMI definuje dátové typy pre siete typu TCP/IP. S použitím týchto typov bola definovaná prvá verzia MIB databázy. SMI definuje agregátne dátové typy a neagregátne dátové typy.

|  |  |
| --- | --- |
| **Názov** | **Popis** |
| Integer | Celé číslo |
| Octet String | Textový reťazec |
| Object Identifier | Identifikátor objektu |
| NULL | Prázdny objekt |

Tabuľka 7.11 - Agregátne dátové typy MIB objektov

|  |  |
| --- | --- |
| **Názov** | **Popis** |
| Network Address | Sieťová adresa |
| IpAddress | IP adresa |
| Counter | Nezáporné celé číslo |
| Gauge | Nezáporné celé číslo, ktoré môže stúpať alebo klesať |
| TimeTicks | Nezáporné celé číslo pre počítanie času |
| Opaque | Používa sa pre textové dáta |

Tabuľka 7.12 - Neagregátne dátové typy MIB objektov

## Typy SNMP Objektov

* **Integer** - jednoduché celé číslo. Hoci špecifikácia nedefinuje žiaden limit, väčšina implementácií obmedzuje tento typ veľkosti na 32 bitov.
* **Counter** - nezáporný integer, ktorý sa plynulo zväčšuje, až dosiahne max. hodnoty (232 - 1), potom začína znovu od nuly. Ako meno napovedá, používa sa najmä na počítanie zaujímavých udalostí v systéme.
* **Gauge** - nezáporný integer, jeho hodnota môže vzrastať i klesať, nikdy ale nemôže prekročiť max. hodnotu. Hodnota Gauge je maximálna, kedykoľvek modelovaná informácia je väčšia alebo rovnaká než toto maximum. V prípade následného poklesu sa zníži aj hodnota Gauge. Absolútna možná hodnota je opäť (232 - 1).
* **TimeTicks** - nezáporný integer reprezentujúci v stotinách sekundy čas od istej doby (možná hodnota (232 - 1). Môže byť použitý k vyjadreniu doby chodu nejakého zariadenia od jeho zapnutia.
* **IpAddress** - 32 bitová IP adresa.
* **OCTET STRING** - sekvencia bytov. Používa sa k vyjadreniu buď reťazca znakov, napr. meno systému, alebo ľubovoľných binárnych dát, napr. MAC (Media Access Control) adresy zariadenia.
* **OBJECT IDENTIFIER** - reprezentuje meno uzlu. SNMP dovoľuje ešte tri iné typy skalárnych hodnôt (NULL, Opaque a Network Address), ktoré sa však nepoužívajú.

Výpis č. 1 Použitie SNMP operácie z príkazového riadka

$ snmpget -v 1 -c public 192.168.5.3 sysUpTime.0

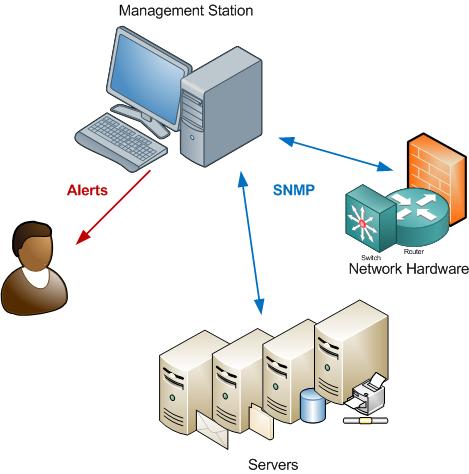
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: **(**295214760**)** 34 days, 4:02:27.60

Vo výpise č. 1 je príklad čítania z MIB databázy prostredníctvom SNMP protokolu. Na zistenie hodnoty z MIB databázy, v tomto prípade je to čas prevádzky (sysUpTime), je použitý príkaz snmpget z príkazového riadku operačného systému. Prvá voľba (-v) hovorí o použitej verzii SNMP protokolu (verzia 1). Táto voľba nie je povinná, systém vie automaticky zistiť verziu protokolu agenta. Druhá voľba (-c), za ktorou nasleduje textový reťazec je povinná, slovo public je názov komunity SNMP agenta. Za komunitou nasleduje IP adresa zariadenia, z ktorého chceme čítať údaje. Miesto IP adresy sa môže použiť doménové meno zariadenia, ak existuje. Za identifikáciou zariadenie nasleduje názov položky, ktorej hodnotu chcem zistiť. Namiesto príkazu snmpget môžeme použiť príkaz snmpwalk, ktorý vypíše obsah celej MIB databázy (všetky položky). Nová hodnota sa nastavuje príkazom snmpset.

## Čo dokáže SNMP ?

SNMP je veľmi jednoduchý, ale účinný. Má schopnosť pomáhať riadiť vašu sieť:

* Poskytuje čítacie / zapisovacie schopnosti - napríklad sa dá použiť pre resetovanie hesla na diaľku, alebo pre re-konfiguráciu IP adries.
* Zhromažďuje informácie o tom, koľko šírky pásma sa používa.
* Zbierať chybové hlásenie do logu, ktoré sú užitočné pre riešenie problémov a identifikáciu trendov.
* E-mailom upozornenie, keď má váš server málo miesta na disku.
* Monitoruje CPU a použitú pamäť zariadenia, upozorňuje pri prekročení prahovej hodnoty (*thresholds*).
* Pri zlyhaní zariadenia informuje Pagerom alebo SMS správou.
* Môže vykonávať *active polling*, tj. monitorovacia stanica sa pýta zariadení na stav každých pár minút.
* Pasívne SNMP - zariadenie môže poslať upozornenie na monitorovaciu stanicu pri objavení chybových stavov.



Obrázok .

## Monitorovací systému – Módy / Režimy

Režim zberu dát z monitorovaného systému je kritický. Režimy pre tento zberu sú nasledovné: *monitor poll, agent push, a hybrid scheme*.

### Monitor poll

V tomto režime sa jeden alebo viac procesov v monitorovacom systéme, v skutočnosti (***poll***) požaduje / dotazuje na prvky systému v niektorých vláknach. Počas cyklu sú zariadenia dotazované cez SNMP volania, hostia sa dajú sprístupniť cez Telnet / SSH na spúšťanie skriptov alebo výpis súborov alebo spúšťanie iných OS špecifických príkazov. Aplikácie môžu vyžadovať údaje o stave (*state data)*, alebo ich stavy výstupných súborov (*state-output-files*) môžu byť vypísané.

Výhodou tohto spôsobu je to, že je tu malý vplyv na zariadení / hostovi počas požadovania údajov. CPU hosťa je načítané iba v priebehu dotazovania. Zvyšok času monitorovacie funkcie nehrajú žiadnu úlohu pri zaťažení CPU.

Hlavnou nevýhodou tohto spôsobu je, že ak dotazovanie trvá príliš dlho, zamýšľaný dotazovací interval (*poll-period*) sa predĺži.

### Agent push

V režime Agent push, sledovaný host jednoducho tlačí (*pushing*) dáta sám od seba k aplikácií monitorovacieho systému. To môže byť vykonané pravidelne, alebo asynchrónne na požiadanie z monitorovacieho systému.

Výhodou tohto spôsobu je, že zaťaženie monitorovacieho systému môže byť znížené na jednoduchý príjem a ukladanie dát. Nemusí sa starať o časové limity pre SSH volanie, analýzu OS-špecifických výsledkov volaní, atď.

Nevýhodou tohto spôsobu je, že logika pre dotazovanie cyklu / možností nie je centralizované na monitorovací systém, ale je distribuovaný do každého vzdialeného uzla. Čím sa zmení monitorovacia logika, a musí byť vytlačený do každého uzla.

Tak tiež pri monitorovaní založenom na agentovi, host nemôže informovať, že je úplne "down" alebo je vypnutý, alebo ak sprostredkovateľ systému (napríklad smerovač) zabraňuje prístupu k systému.

### Hybrid mode

Stredná cesta medzi "Monitor-poll" a "Agent-Push" je hybridný prístup, kedy konfigurácia systému určuje, kde dochádza k monitorovaniu, a to buď na strane monitorovacieho systému alebo na strane agenta. A preto keď prídu na rad aplikácie, môžu pre seba určiť, aké systémové prvky, sú zodpovedné za dotazovanie. Všetci však nakoniec musia vyslať svoje monitorované dáta do procesu systémového monitora.

Toto je užitočné najmä pri nastavovaní monitorovacej infraštruktúry po prvýkrát kde nie všetky kontrolné mechanizmy boli implementované. Monitorovací systém môže robiť všetky dotazovania (*polling*) v akýchkoľvek jednoduchých prostriedkoch ktoré sú k dispozícii. Časom keď sa agenti stávajú múdrejší, môžu prijať väčšiu časť zaťaženia.

## SNMP Konfigurácia na ASA FW 5520 cez Management int.

Cisco ASA FW umožňuje použitie SNMP len s platnou licenciou (DES alebo voliteľná 3DES/AES) a v našom prípade len s verziou SNMPv3 ktorú je oproti SNMPv2 ťažšie nastaviť a nakonfigurovať.

### Nastavenie management (spravovacieho) portu na ASA FW 5520

#interface Management 0/0

#speed 100

#nameif MGMT

#bridge-group 1

#security-level 0

#ip address 192.168.1.1 255.255.255.0

#no shutdown

### Nastavenie SNMP na ASA FW 5520

Povolenie SNMP servera na ASA

#snmp-server enable

Vytvorenie skupiny s názvom projekt2, verziou SNMP a autentifikáciou

#snmp-server group projekt2 v3 priv

Vytvorenie užívateľa s heslom a pridanie do skupiny projekt2 (pri testovaní funkčnosti cez snmpwalk pýtalo minimálne 8-miestne heslo)

#snmp-server user kasala projekt2 v3 auth md5 qwerty1212 priv des qwerty1212

Špecifikovanie príjemcu (NMS alebo SNMP Manager) SNMP informácií (trapov) spolu s verziou SNMP a užívateľom ktorý bude mať ku nim prístup

#snmp-server host MGMT 192.168.1.10 version 3 kasala

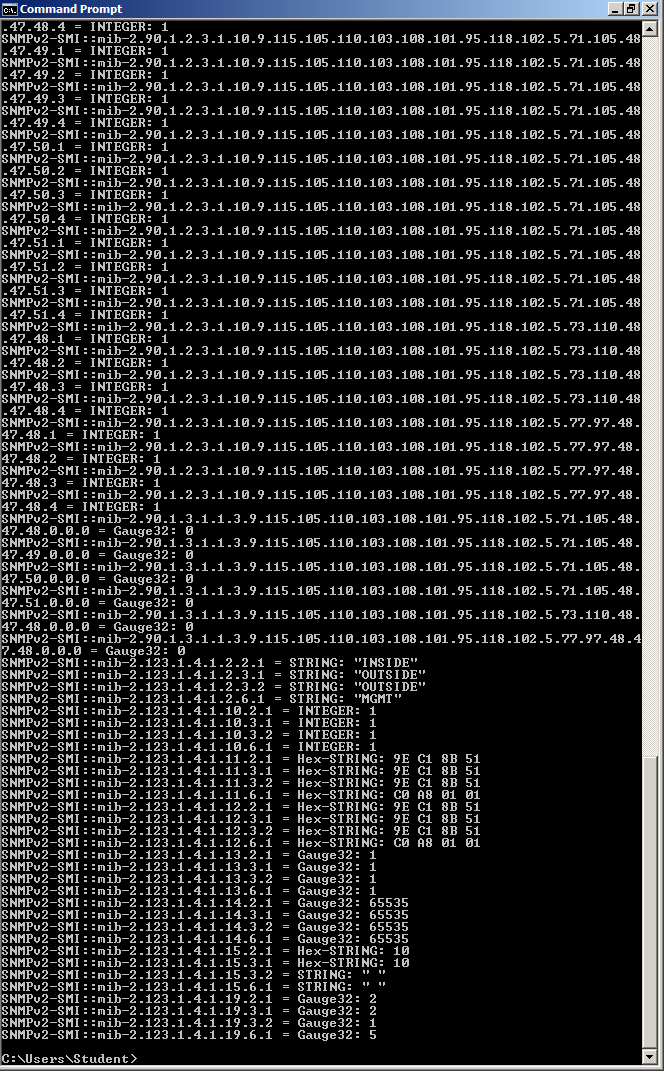
Príkaz ktorý povolí zasielanie trap (oznámení)

#snmp-server enable traps all

### Otestovanie funkčnosti

V príkazovom riadku na počítači s IPv4 adresou 192.168.1.10 zadáme príkaz

|  |
| --- |
| snmpwalk –v3 –l AuthPriv -u kasala –a MD5 –A qwerty1212 –x DES –X qwerty1212 192.168.1.1 |



Obrázok . – Výpis snmpwalk

Pozitívny výsledok funkčnosti bude spočívať vo výstupe v podobe veľkého počtu riadkov.

V Prípade nefunkčnosti nejaká z chýb typu zlé meno/heslo, Timeout , No Response (ak SNMP nepracuje správne alebo nie je zabezpečená konektivita) a podobne.

## Porovnanie 5 najlepších nástrojov

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Nagios** | **PRTG** | **Zabbix** | **SolarWinds NPM** | **HP IMC** |
| **História** | áno | áno | áno | áno | áno |
| **Notifikácia** | e-mail, pager, vlastné | e-mail, SMS, vlastné | e-mail, SMS,  vlastné | vlastné | e-mail |
| **SNMP** | cez plugin | áno | áno | áno | áno |
| **Syslog** | cez plugin | áno | áno | áno | áno |
| **IPv6** | áno | áno | áno | áno | áno |
| **SLA** | cez plugin | áno | áno | áno | áno |
| **Mapy** | áno | áno | áno | áno | áno |
| **Virtualizácia** | áno | áno | áno | áno | áno |
| **Cena** | nelimitovaný počet senzorov 6495$ | nelimitovaný počet senzorov 12 000€ | Open source | 2000 zariadení a ročná údrţba stojí 15675 dolárov | nezistená |
| **Operačný systém** | všetky | Windows | všetky | Windows | Windows, Red Hat Linux |
| **Automatické zisťovanie** | cez plugin | áno | áno | áno | áno |
| **Pracovná plocha/rozhranie** | Web GUI | Web GUI,  Windows GUI | Web GUI | Web GUI,  vlastné | Web GUI |
| **Agentless** | áno | áno | áno | partial | áno |
| **Distribuované monitorovanie** | áno | áno | áno | áno | áno |
| **Logické vytváranie skupín** | áno | áno | áno | áno | áno |
| **Trendy** | áno | áno | áno | áno | áno |
| **Bezdrôtové body** | áno | áno | ? | áno | áno |

Tabuľka 7.13 - Zhrnutie najdôležitejších funkcií a vlastností piatich najlepších nástrojov

Zdroj: Bc. práca 2015 máj - Monitorovanie lokálnych počítačových sietí - Králiková Lucia

## Výber monitorovacieho nástroja - PRTG Network Monitor

### Základné funkcie monitorovacieho nástroja:

* monitorovanie šírky pásma, využitie, aktivity, doby prevádzky a SLA, QoS
* monitorovanie niekoľkých sietí / umiestnenie na jednu licenciu,
* česká verzia nástroja,
* monitorovanie 24/7,
* podporuje aj monitorovanie bez agentov,
* podpora IPv6,
* konfiguračný manažment,
* vhodné pre všetky typy sietí, monitorovanie LAN, WAN, WLAN, VPN.

### Senzory a protokoly:

* viac ako 80 typov senzorov (Ping, HTTP, WMI, SMTP, POP3, DNS a mnoho ďalších),
* prenos v sieti a analýza správania pomocou SNMP, Syslog, NetFlow, sFlow, jFlow, packet sniffing a sledovanie paketov,
* chytré senzory (napr. Automatické rozpoznávanie a monitorovanie viacprocesorových systémov),
* vopred nakonfigurované šablóny zariadení pre routery Cisco, servery SQL, sieťové tlačiarne a pod.,
* senzory pre monitorovanie virtuálneho prostredia (VMware, Xen, HyperV pod.),
* programovateľné triggery a senzory podľa výberu.

### Zobrazenie:

* elegantné, rýchle a výkonné webové rozhranie,
* integrácia aplikácie Google Maps,
* voliteľné grafické rozhranie Windows GUI,
* rozhranie pre mobilné zariadenia iPhone App a Mini-HTML,
* hierarchické zobrazenie (sondy, skupiny, zariadenia, senzory, kanály),
* zoznam senzorov (abecedný, najrýchlejší, najpomalší, podľa označenia / typu atď.)
* prepracované grafy (pre senzory, zariadenia, skupiny a sondy) zobrazujúci dáta monitorovanie za posledné 2 hodiny, posledných 48 hodín, posledných 30 dní a posledných 365 dní,
* mapy s možnosťou vlastného nastavenia, ktoré prepájajú stav monitorovania, grafy a tabuľky, a umožňujú individuálne rozloženie,
* Enterprise konzola: Windows aplikácia predovšetkým pre veľké inštalácie. Podporuje prezeranie dát, monitorovanie niekoľkých PRTG zariadení v jednej aplikácií,
* všetky užívateľské rozhrania umožňujú SSL - zabezpečený a vzdialený prístup a môžu byť použité súčasne.
* súkromné a verejné monitorovacie panely: napr. obrazovky pre sieť operačných stredísk alebo mapy s informáciami pre ostatných zamestnancov,
* interaktívna mapa s viac ako 300 rôznymi mapovými objektmi (ikony siete, stavové ikony, dopravné schémy, top 10 zoznamy, atď.).

### Upozornenia a hlásenia:

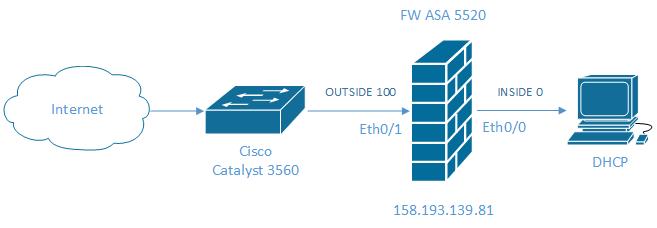
* upozornenie podľa individuálne nakonfigurovaných kritérií,
* rôzne spôsoby oznamovania (e-mail, SMS, správa na pager, žiadosť HTTP, syslog pod., SNMP trap)
* periodické hlásenie s možnosťou vlastného nastavenia (HTML, PDF),
* hlásenie a súbory denníka (podrobné protokoly všetkých činností a výsledkov),
* zvukové alarmy,
* požiadavky na systém a úložisko dát,
* malý objem dát na stiahnutie, jednoduchá inštalácia.

### Hĺbkové správy:

* správy vo formáte HTML alebo vo formáte PDF,
* viac ako 30 šablón správ,
* hlásenie úlohy je možné spustiť ad-hoc alebo plánovane (denne, týždenne, mesačne),
* historické údaje z monitorovania sa môžu exportovať ako HTML, XML, CSV,
* podrobné grafy a tabuľky dát pre jeden alebo viacero senzorov,
* Top 100 využitie šírky pásma, Top 100 využitie CPU, Top 100 Ping Times, Top 100 miesta na disku.

## Sledovanie ASA 5520 pomocou PRTG Network Monitor prostredníctvom SNMP

### Konfigurácia na ASA 5520



Obrázok . - Testovacia topológia

### Nastavenie firewallu do transparentného módu a vytvorenie Bridge-Groupy

|  |
| --- |
| #firewall transparent  #interface BVI 1  #ip address 158.193.139.81 255.255.255.0  #no shutdown |

### Konfigurácia Interfacov G0/0 a G0/1

**speed** [number] – udáva rýchlosť linky ktorá je unás 100Mbit/s

**nameif** [name] – pomenovanie interfacu

**bridge-group** [number] – [0-100] pridelenie do groupy ktorú sme vytvorili vyššie,

**security-level** [number] – [0-100] zabezpečenie prístupu do siete (defaultne je povolený prístup z väčšieho do menšieho)

|  |  |
| --- | --- |
| #interface gigabitEthernet 0/0  #speed 100  #nameif INSIDE  #bridge-group 1  #security-level 0  #no shutdown | #interface gigabitEthernet 0/1  #speed 100  #nameif OUTSIDE  #bridge-group 1  #security-level 100  #no shutdown |

### Nastavenie SNMP, vytvorenie skupiny a užívateľa.

#snmp-server enable

#snmp-server group projekt2 v3 priv

#snmp-server user kasala projekt2 v3 auth md5 qwerty1212 priv des qwerty1212

#snmp-server host INSIDE 158.193.139.179 version 3 kasala

#snmp-server enable traps all

## Inštalácia PRTG Network Monitor

Na webe <https://shop.paessler.com/shop/free_license/?showkey=1&download=1> stiahneme software ktorý je zadarmo. Po dobu 30 dní umožňuje neobmedzený počet senzorov. Po uplynutí 30tich dní len 100 senzor čo je stále veľmi dostačujúce. Počas inštalácie program bude pýtať licenčný kľuč ktorý je zobrazený tiež na webstránke priloženej vyššie.

**License Name:** prtgtrial

**License Key:** 000014-3BAKFM-8FFMNA-HZZ0Z4-DFURM8-K3XYD2-QHDZMC-J2JY2K-KY6PE1-1J34NP

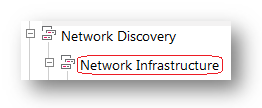
### Nastavenie PRTG

Po prihlásení sa do PRTG pod administrátorským kontom klikneme v hornej lište zobrazovanej stránky na sekciu ***Devices.***



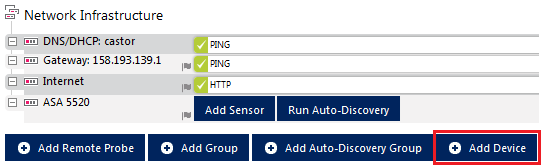
Obrázok . - 1. krok pre nastavenie PRTG

Následne pod ***Network Discovery*** klikneme na ***Network Infrastructure.***



Obrázok . - 2. krok pre nastavenie PRTG

Po načítaní stránky klikneme na tlačidlo **Add Device**.



Obrázok . - 3. krok pre nastavenie PRTG

Klikneme ***Continue***. Následne sa zobrazia informácie o zariadení ktoré treba doplniť. Názov (ľubovoľný) a IP adresa zariadenia 158.193.139.81.

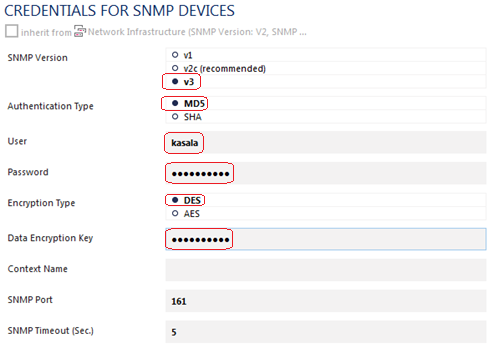


Obrázok . - 4. krok pre nastavenie PRTG

Na tej istej stránke nižšie treba odškrtnúť check box ***inherit from*** pod ***Credentials for SNMP Devices,*** kde treba dopísať informácie ktoré boli nakonfigurované v ASA 5520.

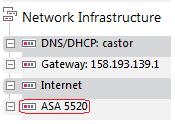
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SNMP Version** | **User** | **Password** | **Auth. a Encry. type** | **data encryption key** |
| v3 | kasala | qwerty1212 | MD5 a DES | qwerty1212 |

Tabuľka 7.14 – Údaje pre Credentials for SNMP



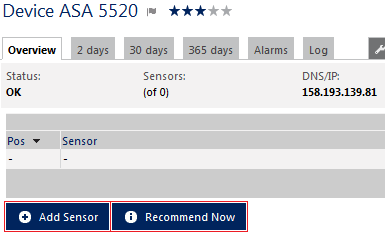
Obrázok . - 5.krok pre nastavenie PRTG - Credentials for SNMP

Klikneme ***Continue*** a následne na nami vytvorené zariadenie s názvom ASA 5520.



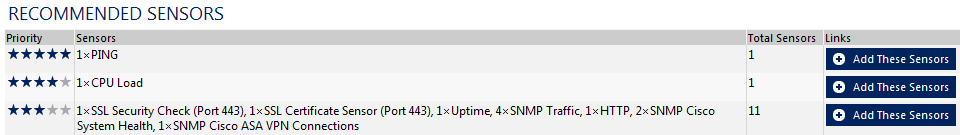
Obrázok . - 6. krok pre nastavenie PRTG

Po načítaní stránky máme na výber 2 možnosti ako pridať senzory. Buď klikneme na ***Recommend Now.***



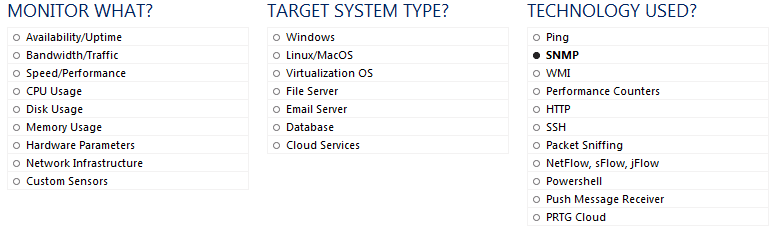
Obrázok . - 7. krok pre nastavenie PRTG

a po spracovaní údajov (trvá asi 15 minút) nám software sám odporučí rôzne SNMP senzory ktoré môžeme pridať jednoduchým stlačením ***Add These Sensors***.



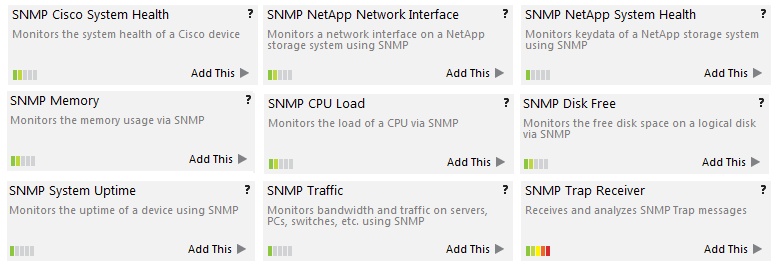
Obrázok . - 8. krok pre nastavenie PRTG

Alebo môžeme pridať senzory ručne po jednom podľa vlastnej potreby. Vtom prípade klikneme na **Add Sensor**. Tu následne vyhľadáme senzor podľa toho čo chcem monitorovať, aký systém alebo akú technológiu použiť.



Obrázok . - 9. krok pre nastavenie PRTG

My sme zvolili technológiu SNMP a následne si môžeme vybrať jeden z ponúkaných senzorov ktorých je vyše 60 avšak nie každý má využitie v spojení so zariadením ASA 5520. Na ilustráciu zopár z ponúkaných senzorov.



Obrázok . – 10. . krok pre nastavenie PRTG

Na obrázku nižšie môžeme vidieť ako vyzerajú už pridané senzory ktoré napríklad sledujú využitie CPU či pamäte alebo Traffic (prevádzku) na ASA interfacoch pomenovaných INSIDE a OUTSIDE a podobne. Po podrobnejšie informácie a grafy treba kliknúť na jeden zo senzorov.



Obrázok . – PRTG senzory

## Tabuľka KIS FRI zariadení podporujúce SNMP

|  |  |  |
| --- | --- | --- |
| **Názov** | **Názov produktu** | **Podpora** |
| Switch - CORE\_A\_KIS | Cisco 3560-E-24TD | ✓ |
| Switch - CORE\_B\_KIS | Cisco 3560-E-24PD | ✓ |
| Firewall | FW ASA 5515X | ✓ |
| Firewall | FW ASA 5520 | ✓ |
| Switch - FRI\_A | Cisco 3560 | ✓ |
| Switch - FRI\_B | Cisco 2960 | ✓ |
| Switch - Cisco 3750 | Cisco 3750 | ✓ |
| Wireless Controller | Cisco 2504 WLC | Unknown |

Tabuľka 7.15 - KIS FRI zariadenia podporujúce SNMP

# RMON - Remote Monitoring Network

Rozšírenie Simple Network Management Protocol (SNMP), ktorý umožňuje detailné sledovanie štatistických údajov o sieti pre Ethernetové siete. Vzdialený monitoring siete (RMON) je definovaná v Request for Comments (RFC) 1757.

RMON umožňuje sledovať prevádzku v sieti na vzdialenom Ethernet segmente z centrálneho miesta v sieti s cieľom odhaliť problémové stavy, ako je traffic congestion, dropped packets a excessive collisions (zahltená prevádzka, zahodené pakety a nadmerné kolízie. V RMON sa dajú nastaviť tzv. network traffic thresholds, ktoré spúšťajú alarmy a tým si môžete opraviť problémy so sieťou skôr, než k nim dôjde. Embedded RMON podporuje Ethernetové switche (prepínače) a umožňuje správcom siete monitorovať „switched Ethernet networks“, ktoré sa nedajú ľahko sledovať pomocou tradičných packet-sniffing sieťových analyzátorov.

Rovnako ako SNMP, RMON je implementovaný ako štandardný Management Information Base (MIB) na RMON-podporujúcich zariadeniach. Tieto zariadenia zahrňujú nasledujúce:

* Stand-alone zariadenia nazývané dedikované RMON sondy („dedicated RMON probes“), ktoré môžu byť dočasne alebo trvalo inštalované tam, kde to vyžaduje sieť.
* Existujúce sieťové zariadenia ako „repeaters, bridges, hubs, routers, alebo Ethernet switches“ ktoré majú RMON sondy vložené do ich obvodov.

RMON sonda sa skladá z SNMP agenta pre zhromažďovanie informácií a komunikácie s aplikáciou pre správu SNMP (ktorej tieto informácie zasiela), a jeden alebo viac RMON MIB definujúce sieťové objekty, ktoré majú byť spravované. Obvykle, SNMP-manažované zariadenia, ako napríklad hub alebo router potrebuje v sebe dodatočný inštalovaný softvér iba na zabezpečenie funkčnosti RMON a premeniť ho na sondu. Iné zariadenie zvané „hosted probes“ sú implementované ako doplnok hardvérových modulov so vstavaným výpočtovým výkonom a pamäťou.

RMON je zvyčajne realizovaná iba na jednom zariadení alebo rozhraní pre TCP / IP podsieť. RMON agent softvér beží na porte routra alebo switcha, čím sleduje a zhromažďuje Ethernetové sieťové štatistiky pre pripojené podsiete. Tieto štatistické údaje sa vzťahujú ku fyzickej vrstve (physical layer - vrstva 1) a linkovej vrstve (data-link layer - vrstva 2) OSI modelu. SNMP konzola pre správu kontaktuje RMON agenta, s cieľom zozbierať štatistické údaje, analyzovať ich a prezentovať ich správcovi siete. RMON agenti môžu tiež zhromažďovať a ukladať štatistiky pre sledovanie trendov v oblasti sieťovej prevádzky.

RMON MIB definovaný v RFC 1757 obsahuje deväť skupín ovládateľných objektov (monitorovacie prvky, RMON) pre rôzne aspekty monitorovania Ethernet prevádzky, v celkovom objeme 204 objektov a 2 udalosti. Tieto skupiny objektov, zvyčajne označované ako RMON1 skupiny, sú nasledujúce:

* **Statistics (1) -** Zaznamenáva štatistiky pre rozhrania Ethernetových sietí (porty), vrátane odoslaných a prijatých paketov, bajtov odoslaných a prijatých, počet každého typu paketu, zahodené pakety, chyby a kolízie.
* **History (2) –** Špecifikuje typy dát odobraté ako vzorky, frekvenciu odoberania a zaznamenáva vzorky dát pre neskoršiu analýzu.
* **Alarm (3) -** Umožňuje nastaviť doby odberu vzoriek a „thresholds“ slúžiace k spúšťaniu alarmov pri prekročení určitej podmienky v sieti.
* **Host (4) –** Zaznamenáva MAC adresy; počet odoslaných a prijatých paketov pre broadcast, unicast a multicast pakety; počet bajtov odoslaných a prijatých; a počet chybných paketov pre všetkých hostov v podsieti.
* **HostTopN (5) -** Umožňuje vypísať hostov podľa rebríčka parametrov, ako je objem vygenerovanej prevádzky alebo počtom vygenerovaných chýb.
* **Matrix (6) –** Zaznamenáva štatistiky pre komunikáciu medzi dvojicami hostov, ako je ich zdrojová a cieľová adresa a počet bajtov a paketov odoslaných a prijatých.
* **Filter (7) -** Ovláda ktoré druhy paketov by mal agent zachytiť, ako sú všetky pakety väčšie ako určitá veľkosť, všetky pakety ktoré zodpovedajú konkrétnej bitovej maske, alebo logických kombinácií jednotlivých výrazov.
* **Capture (8) -** Umožňuje zachytiť pakety pre zber štatistických údajov siete a konfigurovať snímanie veľkosti vyrovnávacej pamäte (buffera).
* **Events (9) -** Umožňuje generovanie SNMP traps a log záznamov.

# PACKET CAPTURE s EEM (Embedded Event Manager)

Packet capture je utilita pomocou, ktorej sa dá zachytávať prevádzka prechádzajúca cez Cisco zariadenia.

## Príklad konfigurácie na CISCO ASA cez CLI

capture testcap interface INSIDE circular-buffer buffer 33554432

kde:

**testcap** – názov access listu (my sme žiadny nepoužili, takže sme zachytávali všetky dáta)

**interface INSIDE** – zachytávaná prevádzka na interface INSIDE

**circular-buffer** – dáta sa budú ukladať do súboru stále a po dovŕšení maximálnej veľkosti sa staré dáta vymažú a prepíšu novšími

**buffer 33554432** – veľkosť buffera pre ukladanie prevádzky. Maximálna veľkosť je 33554432 bajtov.

Ďalšie možnosti nastavenia:

**asa\_dataplane** – zachytávanie paketov na ASA backplane, ktoré prechádzajú medzi ASA a modulo využívajúci backplane (ASA CX alebo IPS modul)

**ethernet-type** – výber ethernetových rámcov, ktoré budú odchytávané. Možné typy: 8021Q, ARP, IP, IP6, IPX, LACP, PPPOED, PPPOES, RARP, VLAN.

**real-time** – dáta, ktoré sú zachytené sa v reálnom čase zobrazujú na termináli (vypnutie sa vykoná pomocou CTRL + C)

**trace** – zobrazenie zachytených dát iným spôsobom

Samozrejme je možné pomocou access listov filtrovať prevádzku, ktorú chceme zachytávať. Ak nechceme používať access listy, môže sa využiť aj **match**, v ktorom sa dá nastaviť napríklad typ protokolu (ip, gre, icmp, ...), zdrojová a cieľová IP adresa alebo porty. Napríklad:

capture testcap interface INSIDE match ip host 1.1.1.1 host 2.2.2.2

Kde sa zachytáva prevádzka od 1.1.1.1 smerujúca na 2.2.2.2.

Pre ukončenie zachytávania sa použije príkaz

no capture testcap

Zobrazenie samotných dát sa dá realizovať dvoma spôsobmi:

* Zobrazenie na samotnej ASA v príkazovom riadku:

show capture testcap

zobrazené dáta sú vo formáte:

HH:MM:SS.ms [ether-hdr] src-addr.src-port dest-addr.dst-port: tcp-flags [header-check] [checksum-info] sequence-number ack-number tcp-window urgent-info tcp-options

* Stiahnutie .pcap súboru:

Stiahnuť dáta z ASA sa dá cez webový prehliadač:

https://IP\_ASA/admin/capture/NAZOV\_CAPTURE/pcap

stiahne sa .pcap súbor pre ďalšiu analýzu napr. vo wiresharku.

Defaultné hodnoty pre packet capture na ASA sú:

dáta: raw-data

buffer size: 512 KB

Ethernet type: IP packets

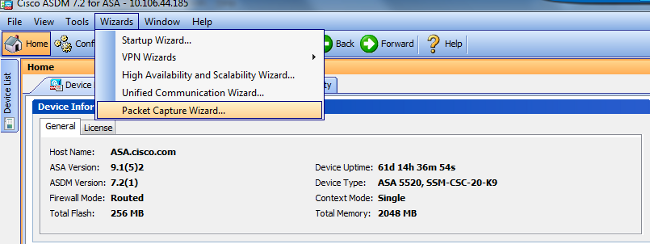
Packet-length 1 518 bytes

Problémom tejto technológie je, že maximálna veľkosť súboru môže byť 33 MB. Navrhované riešenie tohto problému je, že by sa týchto 33 MB (čo je cca 40 000 paketov) posielalo na server, kde by sa po určitom čase tieto 33 MB súbory spojili dokopy.

Tento problém sme sa pokúsili vyriešiť pomocou technológie EEM (Embedded Event Manager). Lenže táto technológia je podporovaná na ASA od verzie 9.2(1) a my sme mali k dispozícii verziu 9.1(6).

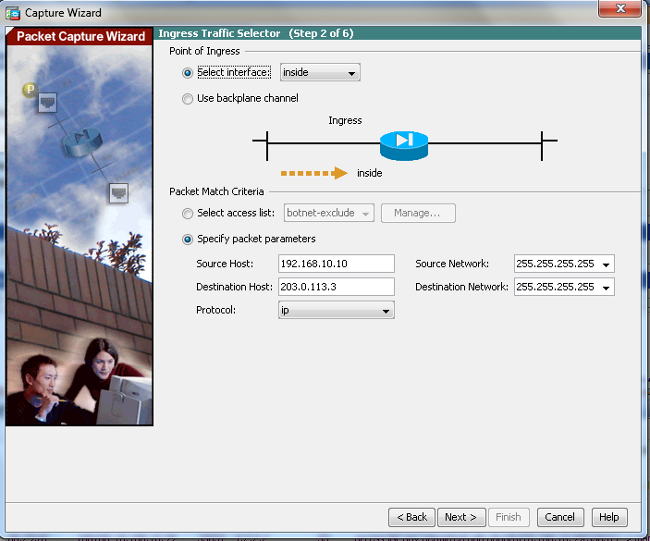
## Príklad konfigurácie na CISCO ASA cez CLI cez ASDM

V ASDM treba najprv vojsť do **Wizard > Packet Capture Wizard**



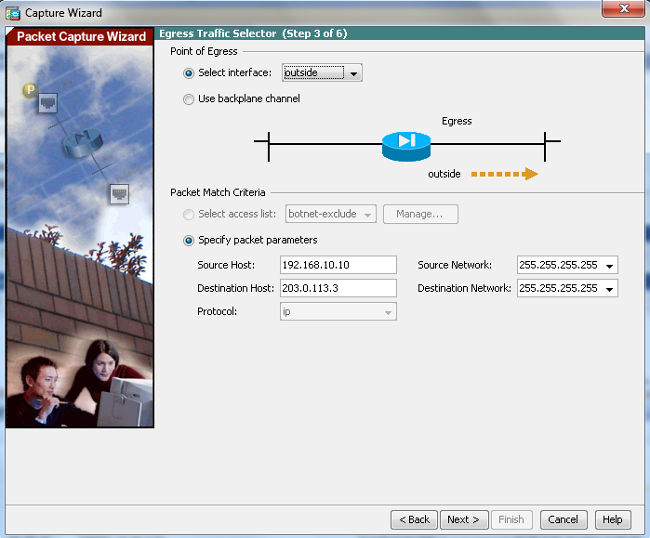
Obrázok . - Začiatok konfigurácie v ASDM

V ďalšom okne klikneme Next. V novom okne sa nastavujú veci pre vstupný interface ako: z ktorého portu sa budú odchytávať dáta, filtrovanie dát a pod.



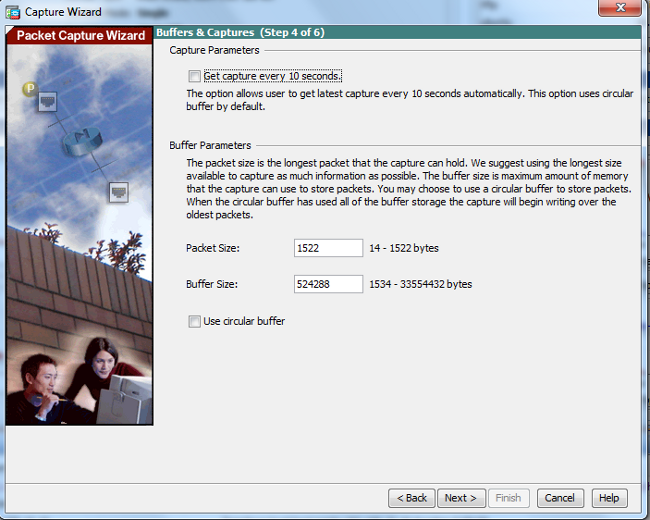
Obrázok . Nastavenie pre vstupný interface

V nasledujúcom okne sa nastavujú totožné veci pre výstupný interface.



Obrázok . Nastavenie pre výstupný interface

Následne sa nastavujú možnosti buffera, jeho veľkosť a pod.



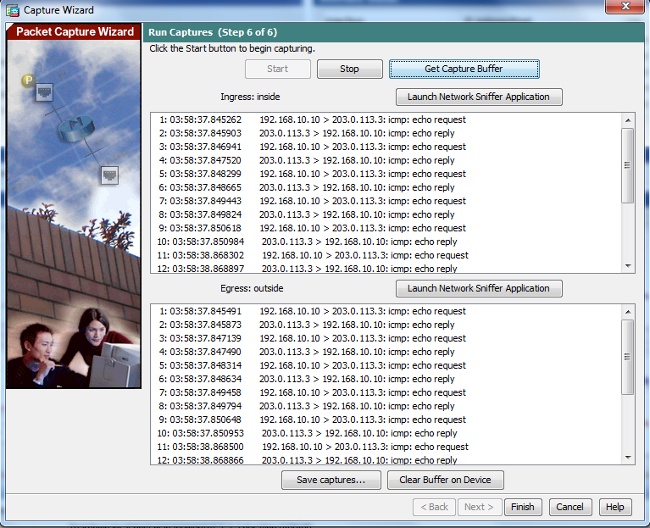
Obrázok . Nastavenie buffera

Potom sa už len klikne v novom okne na **Next** (v tomto okne je napísané zhrnutie našich nastavení) a v ďalšom okne treba capture zapnúť pomocou **Start**.



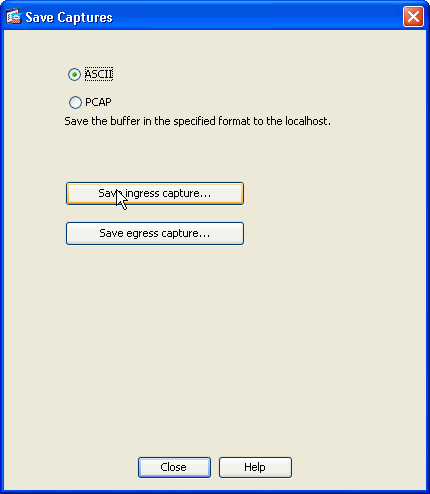
Obrázok . Zapnutie zachytávania paketov

Dáta sa začnú odchytávať a pomocou tlačidla **Get Capture Buffer** vieme zobraziť tieto odchytené dáta.



Obrázok . Zobrazenie odchytených paketov

Cez ASDM samozrejme tieto dáta idú aj stiahnuť. Dole v tomto okne je tlačidlo Save captures... Po kliknutí na toto tlačidlo vybehne okno, kde sa nás pýta či chceme stiahnuť dáta v ASCII alebo PCAP formáte a či chceme dáta zo vstupného alebo výstupného rozhrania.



Obrázok . Export zachytených dát

## Príklad konfigurácie na CISCO IOS

V IOS sa zachytávanie pomocou packet capture uskutočňuje v 4 krokoch:

1. Definovanie si veľkosti buffera
2. Definovanie si „capture point“
3. Asociovať buffer s capture point
4. Export dát a ich analýza

Pre povolenie a konfiguráciu packet capture, treba použiť príkaz *monitor capture* v privilegovanom móde. Znenie celého príkazu je nasledovné:

**monitor** **capture** [ **buffer** **size** size ] [ **circular** | **linear** ] [ **dot1q**] [ **filter** acl-num | exp-acl-num | acl-name ] [ **length** bytes ] { **clear** [ **filter**] | **export** **buffer** location | **schedule** **at** hh **:** mm **:** ss [ date [ month year ] ] | **start** [ **for** number { **seconds** | **packets** } ] | **stop** } **no** **monitor** **capture** [ **buffer** **size** size ] [ **circular** | **linear** ] [ **dot1q**] [ **filter** acl-num | exp-acl-num | acl-name ] [ **length** bytes ] [ **clear** [ **filter**] | **export** **buffer** location | **schedule** **at** hh **:** mm **:** ss [ date [ month year ] ] ]

Vysvetlenie jednotlivých parametrov je možné vyhľadať na [tejto](http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/epc/command/epc-cr-book/epc-cr-m1.html) stránke.

Pre ukážku jednoduchá konfigurácia:

monitor capture buffer buffer-test size 100

definovali sme si veľkosť buffera na 100 Kb. Ďalej treba zadefinovať „capture point“ (nastavený je zber zo všetkých rozhraní a v obidvoch smeroch):

monitor capture point ip cef capture-test all both

V ďalšom kroku treba asociovať vytvorený buffer s capture point:

monitor capture point associate capture-test buffer-test

A už stačí len zachytávanie zapnúť:

monitor capture point start capture-test

pre zastavenie zachytávania sa využije príkaz:

monitor capture point stop capture-test

pre export zachytených raw paketov do .pcap súboru sa využije príkaz:

monitor capture buffer buffer-test export tftp://IP\_ADRESA/subor.pcap

export je možný vykonať pomocou: FTP, http, HTTPS, PRAM, RCP, SCP a TFTP.

pre skontrolovanie nastavených parametrov buffera sa použije príkaz:

show monitor capture buffer NAZOV\_BUFFERA parameters

pre skontrolovanie nastavených parametrov capture point-u:

show monitor capture point NAZOV\_CAPTURE\_POINT

Tu nastáva ale ten istý problém ako na ASA. Keď sa zaplní buffer, tak sa odchytávanie zastaví (pri lineárnom nastavení buffera) alebo sa prepisuje (pri circular nastavení). Ak sa zaplní buffer, zobrazí sa na konzole takáto hláška:

%BUFCAP-5-BUFFER\_FULL: Linear Buffer associated with capture buffer buffer-test is full

Túto hlášku sme následne využili pri nakonfigurovaní EEM.

Na testovanom smerovači 1841 s IOS 15.0(1) M4 sme EEM nastavili nasledovne:

event manager applet prenos

event syslog pattern „.\*buffer-test is full“

action 1 cli command „enable“

action 2 cli command „monitor capture buffer buffer-test export tftp://10.0.0.2/subor$\_event\_pub\_sec.pcap“

action 3 cli command „monitor capture buffer buffer-test clear“

action 4 cli command „monitor capture point start capture-test“

action 5 syslog msg „Bol poslany zaznam z packet capture na tftp server“

kde sa hľadá výraz „.\*buffer-test is full“. Ak sa tento výraz nájde v syslogu, vykonajú sa ďalšie akcie:

* Choď do privilegovaného EXEC módu
* Pošli súbor cez TFTP na danú adresu
* Vyčisti buffer
* Zapni buffer pre opätovné zaznamenávanie paketov
* Napíš na obrazovku, že bol poslaný súbor na TFTP server

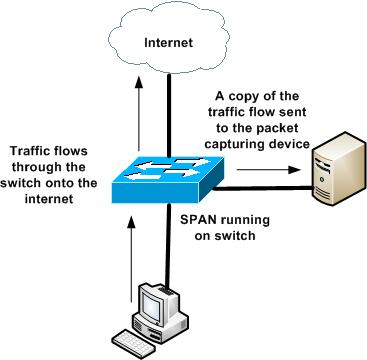
Súbory sa posielajú s názvom *subor* a časom v sekundách aby boli na serveri odlíšené.

# PORT MIRRORING

Ďalšou z možností ako odchytávať celú prevádzku je tzv. zrkadlenie alebo Port Mirroring. Cisco nám ponúka nasledovne možnosti. Local SPAN (Switched Port Analyzer) pre zrkadlenie prevádzky v rámci jedného prepínača a Remote SPAN pre zrkadlenie z viacerých prepínačov. Túto možnosť podporujú prakticky všetky prepínače CISCO. Nie je podporovaná na Firewall ASA.

### PORT MIRRORING – Local SPAN

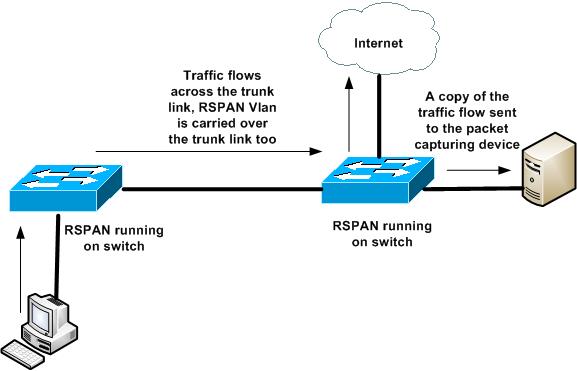
Zber v rámci jedného prepínača:



Obrázok . Local SPAN

### PORT MIRRORING – Remote SPAN

Zber z viacerých prepínačov (budeme mať prístup?):



Obrázok . Remote SPAN

### Konfigurácia

#### SPAN

Switch(config)# monitor session 1 source interface fastEthernet0/1

Switch(config)# monitor session 1 destination interface fastEthernet0/10

Switch# show monitor session 1

#### RSPAN

#### Zdrojový prepínač

SwitchA(config)#vlan 999

SwitchA(config-vlan)#remote-span

SwitchA(config-vlan)#name SPAN\_VLAN

SwitchA(config-vlan)#exit

SwitchA(config)#monitor session 1 source interface fa0/1

SwitchA(config)#monitor session 1 destination remote vlan 999

#### Cieľový prepínač

SwitchB(config)#vlan 999

SwitchB(config-vlan)#remote-span

SwitchB(config-vlan)#name SPAN\_VLAN

SwitchB(config-vlan)#exit

SwitchB(config)#monitor session 1 source remote vlan 999

SwitchB(config)#monitor session 1 destination interface fa 0/2

# Problémy

Prvý problém sa vyskytol hneď na začiatku kedy sme nepoznali meno a heslo pre prístup na firewall ASA 5510. Riešením bola obnova hesla, ktorá prebiehala nasledovne:

**Stiahnutie ASA softwaru z druhého firewallu pomocou TFTP.**

* vytvorenie tftp servera pomocou programu Tftpd64
* pre kopírovanie si musíme nastaviť ip adresu na porte,
* port musí mať nastavený security-level väčší ako ostatné (security-level 100), lebo z menšieho na väčšie nekomunikuje
* ďalej musí mať nastavené meno interface-u (nameif <meno>)
* stiahnuť ASA software - *copy flash:/asa821-k8.bin tftp:<ip address tftp servera>*

**Vymazanie flash na ASA (s neznámym passwordom)**

Počas bootovania stlačiť ESC to interrupt boot (podľa niektorých návodov sa spustí ROMMON), zobrazila sa výzva na vymazanie flash (erase disk0 a disk1).

**Nahranie ASA software pomocou ROMMON režimu**

Po vymazaní sme sa dostali do režimu ROMMON, v ktorom sme zadali nasledovné

rommon #0> ADDRESS=<ip adresa portu>

rommon #1> SERVER=<ip adresa tftp servera>

rommon #2> GATEWAY=<ip adresa brany - tftp servera>

rommon #3> IMAGE=asa821-k8.bin

rommon #4> PORT=Ethernet0/2

rommon #5> set

rommon #6> tftp

* po nabootovaní systému musíme nový ASA software skopírovať do flash pre budúce bootovanie
* k tomu tiež potrebujeme konfiguráciu portu rovnako ako v prvom kroku

copy tftp flash

boot system disk0:/asa821-k8.bin

write memory

reload

Druhým problémom bolo, že ASA 5510 pri konfigurácií stále padala, crashovala s výslednou chybou DISPATCH UNIT. Riešením bolo nahratie nového Cisco Appliance Software podobne ako pri probléme 1.

# Záver

Cieľom projektu bolo nasadenie Firewallu ASA 5510 do živej siete laboratória B303 KIS FRI UNIZA s cieľom získavať dáta a monitorovať prevádzku siete pomocou rôznych nástrojov. Výsledkom je funkčné zapojenie Firewallu ASA 5510 v transparentnom móde s bežiacim NetFlow exporterom, ktorý odosiela informácie na server, tzv. Netflow kolektor. Tu sa jedná o Linux server Debian, na ktorom beží NetFlow kolektor NtopNG.

Ďalšou prácou bolo preskúmanie týchto nástrojov a viacerých technológií pre zber dát okrem Netflow a NTOP aj napríklad SNMP, Port mirroring, Packet capture, Event Objects, RMON a ďalších a tiež iných nástrojov a možností ktoré Firewall ASA poskytuje pre zber dát. Výsledkom je prakticky tento report v ktorom sú zhrnuté ako aj základné informácie o každej technológií, tak aj ukážka jej inštalácie a konfigurácie.

V neposlednom rade bolo cieľom zistiť stav a topológiu nie len našej katedry KIS ale aj celej fakulty FRI. Výsledkom je obrázok topológie (Príloha 2 – Topológia FRI-KIS) a taktiež zoznam zariadení v sieti (Príloha 3 – Zariadenia FRI-KIS).

Prikladáme aj tabuľky, ktoré zhrňujú otestované monitorovacie softvéry a softvéry pre zber dát.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Zariadenia/Technológia | NetFlow | SNMP | Packet Capture | EEM | port mirroring |
| Cisco 3560-E-24TD | ✔ | ✔ | ✔ | ✔ | ✔ |
| Cisco 3560-E-24PD | ✔ | ✔ | ✔ | ✔ | ✔ |
| FW ASA 5515X | ✔ | ✔ | ✔ | od ASA 9.2(1) | x |
| FW ASA 5520 | ✔ | ✔ | ✔ | od ASA 9.2(1) | x |
| Cisco 3560 | ✔ | ✔ | ✔ | ✔ | ✔ |
| Cisco 2960 | ✔ | ✔ | ✔ | ✔ | ✔ |
| Cisco 3750 | ✔ | ✔ | ✔ | ✔ | ✔ |
| Cisco 2504 WLC | ✔ | Unknown | x | x | Unknown |

Tabuľka 12.1 - Zhrnutie testovaných technológií

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Kolektory k NETFLOW | Scrutinizer | PRTG | NTOP | NTOPNG |
| Windows | ✔ | ✔ | x | ✔ |
| Linux | x | x | ✔ | ✔ |

Tabuľka 12.2 - Zhrnutie testovaných kolektorov pre NetFlow

# Zdroje

NTOP/NTOPng  
[https://www.lisenet.com/2014/install-ntop-on-debian-and-configure-to-use-netflow-on-mikrotik-routeros/](https://l.facebook.com/l.php?u=https%3A%2F%2Fwww.lisenet.com%2F2014%2Finstall-ntop-on-debian-and-configure-to-use-netflow-on-mikrotik-routeros%2F&h=-AQEizT58)

<http://www.ntop.org/products/traffic-analysis/ntop/> <http://www.ntop.org/products/netflow/nprobe/>

<http://knowledge-db.info/2014/09/21/install-ntopng-on-debian-7-wheezy/>

<http://idroot.net/tutorials/how-to-install-ntopng-on-ubuntu-14-04/>

Pmacct

<http://www.pmacct.net/>

<http://wiki.pmacct.net/OfficialExamples>  
Povolenie ICMP  
[https://www.youtube.com/watch?v=ecgNII0aMhY](https://l.facebook.com/l.php?u=https%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3DecgNII0aMhY&h=-AQEizT58)   
Konfigurácia ASA  
[https://supportforums.cisco.com/discussion/11122946/asa-5510-transparent-mode-issue](https://l.facebook.com/l.php?u=https%3A%2F%2Fsupportforums.cisco.com%2Fdiscussion%2F11122946%2Fasa-5510-transparent-mode-issue&h=-AQEizT58)  
Obnova ASA  
[https://www.youtube.com/watch?v=qySrJPXB3T0](https://l.facebook.com/l.php?u=https%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3DqySrJPXB3T0&h=-AQEizT58)  
Password Recovery  
[http://ezinearticles.com/?Password-Recovery-on-the-Cisco-ASA-Security-Appliance&id=664795](http://l.facebook.com/l.php?u=http%3A%2F%2Fezinearticles.com%2F%3FPassword-Recovery-on-the-Cisco-ASA-Security-Appliance%26id%3D664795&h=-AQEizT58)  
[https://www.youtube.com/watch?v=qySrJPXB3T0](https://l.facebook.com/l.php?u=https%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3DqySrJPXB3T0&h=-AQEizT58)  
[https://www.youtube.com/watch?v=5dCWx3y\_Gbw](https://l.facebook.com/l.php?u=https%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3D5dCWx3y_Gbw&h=-AQEizT58)

Netflow

<http://www.cisco.com/c/en/us/td/docs/ios/fnetflow/configuration/guide/12_2sr/fnf_12_2_sr_book/fnetflow_overview.html>

<http://netflow.caligare.com/index.htm>

<https://en.wikipedia.org/wiki/NetFlow>

<https://www.plixer.com/blog/general/what-is-jflow/>

Konfigurácia NetFlow pomocou ASDM  
[https://supportforums.cisco.com/document/30476/configuring-netflow-asa-asdm](https://l.facebook.com/l.php?u=https%3A%2F%2Fsupportforums.cisco.com%2Fdocument%2F30476%2Fconfiguring-netflow-asa-asdm&h=-AQEizT58)

Packet Capture a EEM

<http://www.tunnelsup.com/packet-captures-on-cisco-asa>

<http://www.techrepublic.com/blog/data-center/easy-packet-captures-straight-from-the-cisco-asa-firewall/>

<http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118097-configure-asa-00.html>

<https://supportforums.cisco.com/document/69281/asa-using-packet-capture-troubleshoot-asa-firewall-configuration-and-scenarios>

<http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/epc/command/epc-cr-book/epc-cr-m1.html>

<https://routerjockey.com/2011/02/14/ios-embedded-packet-capture/>

<https://routerjockey.com/2010/06/14/working-with-the-embedded-event-manager-eem/>

<http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/epc/configuration/12-4t/epc-12-4t-book/nm-packet-capture.html>

SNMP:

<http://www.samuraj-cz.com/clanek/zarizeni-v-siti-pod-kontrolou/>

<http://m-linux.cz/2014/05/snmp-zaciname/>

<http://homel.vsb.cz/~nav79/ps1/snmppopis.html>

<http://www.kiwiki.info/index.php/Mana%C5%BEment_po%C4%8D%C3%ADta%C4%8Dovej_siete>

<https://en.wikipedia.org/wiki/System_monitoring#Mode>

SNMP: Bc. Práce:

[Návrh a realizácia monitorovania počítačovej siete s využitím systému ZABBIX - Diplomová práca - MTF-17392-36089 2011 - Bc, Peter Murín](http://is.stuba.sk/lide/clovek.pl?zalozka=13;id=2860;studium=75038;zp=24052;download_prace=1)

[Monitorovanie lokálnych počítačových sietí - Bakalárska práca - Králiková Lucia](http://is.bivs.sk/th/21932/bisk_b/BP_Kralikova_final.pdf)

SNMP: Konfigurácia SNMP na ASA

<http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/monitor_snmp.html>

RMON:

<http://www.thenetworkencyclopedia.com/entry/remote-network-monitoring-rmon/>

<http://www.svetsiti.cz/clanek.asp?cid=RMON-v-sitovych-zarizenich-1962000>

<http://www.svetsiti.cz/clanek.asp?cid=Principy-RMON-1662000>

<http://www.svetsiti.cz/clanek.asp?cid=RMON-specifikace-1762000>