CARNet

HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Arbor Networks Peakflow X

NCERT-LAB-PUBDOC-2011-00-003

Nacionalni CERT

Sadržaj

1 Uvod

Današnjim tvrtkama su neophodne pouzdanost, brzina i sigurnost njihove mrežne infrastrukture. Mrežni sustavi su sve veći i složeniji, a dobro je poznato kako je upravo složenost jedan od najvećih neprijatelja sigurnosti. Stoga, naglasak više nije samo u zaštiti resursa nego kvalitetnom praćenju rada sustava te, što je još važnije, pravodobnom dobivanju ključnih informacija. Važno je imati globalni prikaz mreže i jednostavan nadzor nad sigurnosnom politikom. Tako nešto moguće je ostvariti pomoću uređaja koji je u stanju iz ogromne količine podataka, koji svakodnevno prolaze kroz mreže unutar tvrtki, izdvojiti pojedinačne prijetnje sigurnosti. Takav uređaj također mora otkrivati prijetnje u stvarnom vremenu i imati mogućnost praćenja rada pojedinih korisnika.

Jedna od metoda za postizanje navedenih ciljeva je praćenje rada mreže na takav način da uređaj koji nadgleda „uči" kakav promet i kakvo ponašanje unutar mreže je normalno. Takav pristup koristi NBA (Network Behavioral Analysis) tehnologija koju implementira Peakflow X uređaj tvrtke Arbor Networks.

2 Arbor Networks Peakflow X

2.1 Arbor Networks

Tvrtka Arbor Networks jedan je od vodećih svjetskih proizvođača rješenja za nadzor i zaštitu računalnih mreža. Njezini uređaji štite od sigurnosnih prijetnji kao što su distribuirani napadi uskraćivanjem usluge (DDoS) i napadi putem botnet mreža. Također služe sa osiguranje pouzdanosti i kvalitete usluge. Arborovi klijenti su velike svjetske tvrtke i pružatelji Internet usluga (ISP-ovi).

U Arboru su posebno ponosni na svoja rješenja koja omogućuju nadzor MPLS (Multiprotocol Label Switching) mreža i implementaciju sigurnosti temeljenoj na obrani od distribuiranih napada uskraćivanjem usluge (DDoS). Svojim korisnicima tvrtka nudi pravodobne informacije o sigurnosti i Internet prometu na globalnoj razini. To je ostvareno putem jedinstvenog sustava ATLAS (Active Threat Level Analysis System) koji nadzire promet iz 300 svjetskih pružatelja Internet usluga i mrežnih operatora. Te tvrtke anonimno dijele svoj mrežni promet na bazi jednog sata, a podaci iz njega se agregiraju i analiziraju s podacima prikupljenim s Arborovih senzora, kao i od trećih strana. Cilj je tvrtkama omogućiti donošenje ključnih odluka u vezi mrežne sigurnosti, ali i analize tržišta, trendova i mogućih partnera za prijenos prometa. Naravno, sustav donosi podatke i o prijetnjama poput malvera, exploita, phishinga i botnet mreža.

2.2 Peakflow X

Pomoću svojeg uvida u mrežni promet i mogućnosti detekcije sigurnosnih prijetnji u stvarnom vremenu, Arbor Peakflow X rješenje optimizira performanse i sigurnost mreža unutar velikih tvrtki. Uređaj automatski i samostalno „uči" ponašanje radnih stanica unutar mreže, odnosno tko s kim komunicira i kako. To omogućuje bavljenje različitim unutarnjim i vanjskim sigurnosnim prijetnjama, uz zadržavanje normalnog poslovanja. Uređaj se sastoji od dvije vrste komponenti - kolektora i kontrolera (upravljača). Kolektori su zaduženi za prikupljanje prometa kojeg onda šalju kontroleru. Korisnici pristupaju web sučelju

kontrolera kako bi imali uvid u statistiku i kako bi mogli obaviti sve ostale potrebne operacije.
Uz navedeno, Peakflow X integrira i podatke prikupljene s Arborovog globalnog sustava ATLAS. Uređaj analizira mrežni Flow (Netflow i sl.) promet u potrazi za anomalijama koje otkriva zahvaljujući svojoj NBA tehnologiji. Time je moguće otkriti napad prije nego što su za njega dostupni potpisi (definicije). Neke od mogućnosti uređaja su:

- rješavanje prijetnji i nadzor nad mrežom na drugom sloju uz mogućnost jednostavnog otklanjana iz mreže problematičnih radnih stanica, bez utjecanja na rad ostalih čvorova u mreži
- procjena rizika u stvarnom vremenu, odnosno brzo određivanje koje prijetnje unutar mreže imaju najveći faktor rizika (kojeg uređaj automatski izračunava) te koja računala i koji korisnici su uključeni u rizične aktivnosti
- fleksibilno praćenje identiteta te bilježenje aktivnosti korisnika (login / logoff) i njihovih IP adresa

U Arboru također ističu kako uređaj može zamijeniti postojeća rješenja za nadzor VPN prometa i rješenja temeljena na sigurnosti CPE (customer premises equipment) uređaja uz dodavanje novih mogućnosti.

Arbor je Peakflow X zamislio kao uređaj koji objedinjuje upravljanje sigurnošću i operativnošću mreže. S aspekta sigurnosti, uređaj omogućuje:

- detekciju distribuiranih napada uskraćivanjem usluge (DDoS), obranu od virusa, botnet mreža, crva i drugih aktualnih prijetnji
- otkrivanje i otklanjanje phishing napada
- podešavanje mreže u svrhu sprječavanja budućih napada
- upravljanje korisničkim pristupom i otklanjanje mogućnosti napada iznutra

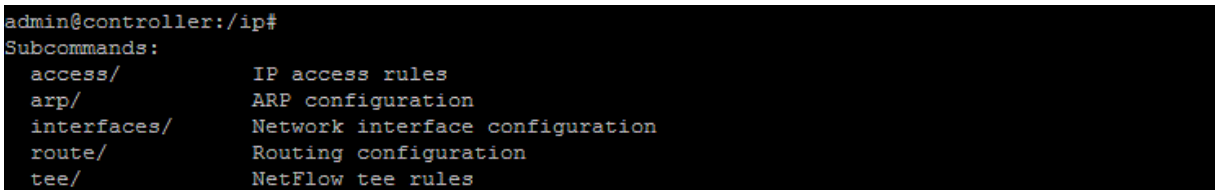
Uređaj je i osmišljen i kako bi tvrtkama pojednostavio implementaciju sigurnosnih politika i standarda kao što su PCI DSS, ITIL, ISO 17799 i dr. Uz fizički uređaj, Arbor je razvio Peakflow X i kao virtualizirano rješenje namijenjeno virtualnim sustavima VMware ESX i ESXi. Upravo takvo rješenje je korišteno u našem testu. Virtualizirano rješenje nudi iste mogućnosti kao i fizički uređaj, naravno uz povoljniju cijenu.

3 Sučelje uređaja

Sustav Peakflow X ima naredbeno (CLI) i Web sučelje. Osnovne postavke kao što su mreža, izvori flow podataka, te povezanost kolektora i kontrolera kod Peakflow X virtualnog sustava se konfiguriraju u CLI sučelju. Nakon pokretanja servisa može se koristiti i Web sučelje.

3.1 Naredbeno sučelje (CLI)

Naredbeno sučelje Peakflow X sustava omogućuje uvid u status i mijenjanje postojeće konfiguracije uređaja. Pristup CLI-u je moguć putem SSH-a, Telnet-a ili izravno putem konzole. Sučelje omogućuje kretanje kroz izbornike i unošenje naredbi. Naredbe su raspoređene hijerarhijski, slično kao u datotečnom sustavu. Korijenski izbornik je označen znakom „/“. Kretanje kroz izbornike je slično kretanju kroz datotečni sustav. Unutar svakog možemo izvršiti određene naredbe karakteristične za taj izbornik.

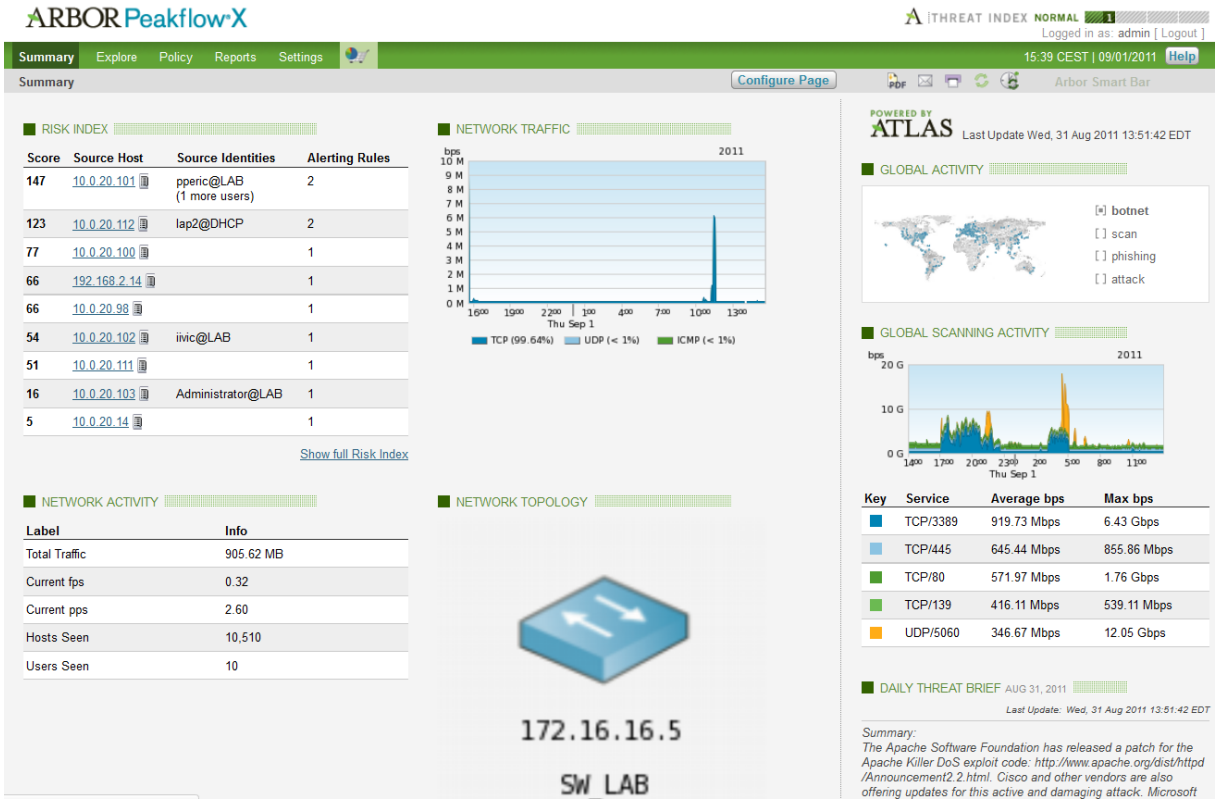


3.1: izgled CLI sučelja

Komandna ljuska može raditi u dva načina rada: „Edit“ koji je označen sa znakom „#“ i „Disabled“ označen sa znakom „>“. Edit omogućava sve konfiguracijske promjene. Ukoliko se korisnik prijavi kao administrator sustav automatski pokreće „edit“ način rada. Disabled način rada omogućuje minimalne konfiguracijske izmjene i uglavnom se svodi na čitanje konfiguracijskih postavki. Korisnik bez administratorskih ovlasti mora ući u Edit mod naredbom **edit** kako bi izmijenio konfiguraciju. Komandna ljuska sadržava i osnovne funkcije drugih CLI sustava kao što su automatsko završavanje naredbe tipkom „TAB“, pregled mogućnosti tipkom „?“, naredba help i sl. Konfiguracija se sprema na disk naredbom **config write**.

3.2 Web sučelje

Početna stranica web sučelja je „**Summary**“ koja sadrži pregled trenutnog stanja u mreži, dok s desne strane nudi određene informacije koje se prikupljaju iz sustava ATLAS. Na slici prikazan je izgled navedene stranice. Stranicu je moguće konfigurirati, tako da prikazuje samo željene podatke. Inicijalno, pri vrhu, s lijeve strane se nalaze informacije o najvećim rizicima u mreži poredanih prema indeksu rizika.



3.2: izgled početne ("Summary") stranice web sučelja

Ispod su informacije o ukupnom prometu u mreži, mrežna topologija, a još niže se nalaze upozorenja koja su generirana u posljednja 24 sata. Tu su još i opterećenja prema sučeljima, broj i vrsta generiranih upozorenja, neke osnovne informacije o statusu kontrolera i kolektora, dok se na dnu nalazi log promjena u sustavu (audit trail). Na vrhu se nalazi traka glavnog izbornika koja za odabir nudi pet opcija:

- **Summary** (spomenuta početna stranica)
- **Explore**
- **Policy**
- **Reports**
- **Settings**

Opcija Explore nudi uvid u promet (uključujući statistiku o klijentima, poslužiteljima, servisima s najvećim prometom, grupama, sučeljima, QoS itd.), trenutne konekcije te faktore rizika. Pod Policy je moguće vidjeti aktivnost u mreži prema faktoru ozbiljnosti („**severity**“) određene sigurnosne prijetnje (može iznositi od 1-10). Tu je također moguće definirati svoju sigurnosnu politiku, odnosno pravila („**User-Defined Rules**“) koja kad budu ispunjena će dovesti do generiranja upozorenja. Također je moguće vidjeti listu ugrađenih

pravila ponašanja („**Active Threat Feed**“) koja uključuju pravila vezana uz detekciju malvera, pokušaja iskorištavanja ranjivosti, otkrivanje prometa na društvenim mrežama, IRC-u, anonimizacijskim mrežama itd. Active Threat Feed se redovito nadograđuje novim definicijama sigurnosnih prijetnji. Tu je i pet posebnih ponašanja svrstanih pod „Builtin Behaviours“ koja predstavljaju osnovne tipove prijetnji. To su:

- **Flood** (pretrpavanje TCP, ICMP ili IP paketima, odnosno napad uskraćivanjem usluge)
- **Host Scan** (skeniranje/otkrivanje računala u mreži)
- **Long Lived Sessions** (sesije koje traju dulje od maksimalnog vremena za koje su konfigurirane)
- **Port Scan** (skeniranje portova računala)
- **Worm** (ovdje je moguće definirati servise i portove koji se ignoriraju u slučaju otkrivanja crva unutar mreže)

Reports dio je zadužen za pretragu postojećih izvještaja i generiranje novih. Različite vrste izvještaja moguće je izraditi prema različitim parametrima mreže. Više o njima u kasnijem dijelu dokumenta.
Na posljetku, Settings izbornik je zadužen za upravljanje i uvid u općenite postavke uređaja kao što su definiranje DNS i SMTP poslužitelja koji će se koristiti, uvid u log zapise izvršenih promjena u sustavu (audit trail), sigurnosne kopije, upravljanje ATF i ATLAS nadogradnjama, korisničkim računima (uključujući i one domenske). Na tom se mjestu također mogu konfigurirati osnovne postavke grupa, servisa i vremenskih objekata („Time Objects“).

4 Konfiguracija uređaja

4.1 Osnovne mrežne postavke

Nakon instalacije Peakflow X virtualnih sustava na VMware ESXi poslužitelj potrebno je odraditi konfiguraciju mreže u konzolnom prozoru nakon čega slijedi ostatak konfiguracije kroz CLI.
U konzolnom prozoru konfiguriramo hostname, jedno mrežno sučelje (mgt0) i definiramo mreže iz kojih ćemo administrirati uređajem.

Peakflow X ima 4 virtualna mrežna sučelja:

- **mgt0** služi za administriranje uređaja ili za prihvat flow podataka
- **flow0** predstavlja dodatno sučelje za prihvat flow podataka
- **pcc0** i **pcc1** su sučelja namijenjena za hvatanje paketa (eng. packet capture).

PCC sučelja se koriste za praćenje identiteta korisnika u mreži pomoću DHCP-a ili radiusa. Moraju biti spojeni u lokalnu mrežu jer Peakflow X na osnovu DHCP i RADIUS zahtjeva i odgovora mapira IP adrese s ID-evima korisnika. Identitet se može pratiti i povezivanjem s Microsoftovim AD-om.

```
admin@collector:/# ip interfaces show mgt0
mgt0  Gigabit Ethernet, Interface is UP, mtu 1500
          Hardware: 00:0C:29:7A:3D:E3
          Media: Ethernet autoselect
          Status: 1000Mb/s Full
          Inet: 10.0.14.99 netmask 255.255.255.0 broadcast 10.0.14.255
          Inet6: fe80::20c:29ff:fe7a:3de3 prefixlen 64
          Input: 1062931 pkts, 69643002 bytes, 0 errors
          Output: 1506440 pkts, 1431257361 bytes, 0 errors, 0 collisions
          Interrupts: 2024480
```

4.1: Prikaz mrežnog sučelja mgt0

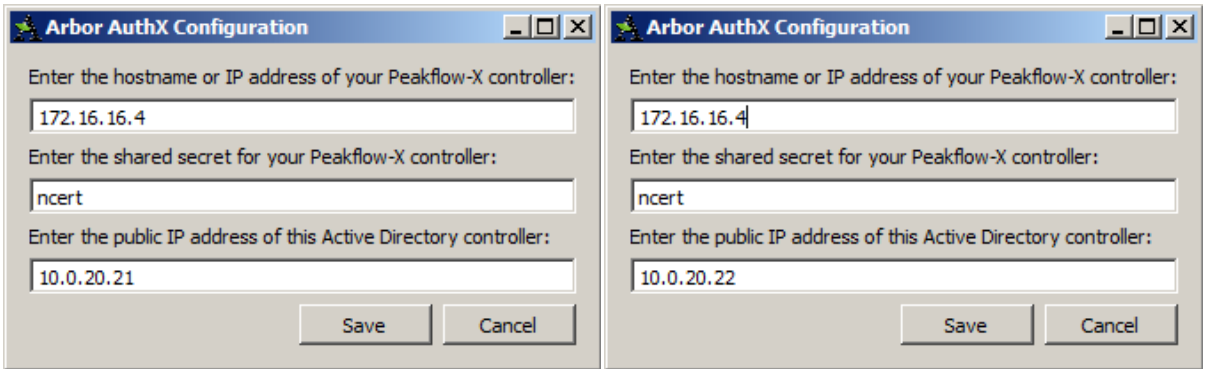
4.2 Konfiguracija izvora netflow podataka

Peakflow X podržava tri tipa „flow" podataka: NetFlow, cflowd i sFlow. Flow podatke možemo slati izravno na kontroler. Kod većih mreža, kolektori služe za prikupljanje podataka i zatim ih šalju kontroleru. Broj flow izvora ovisi o tipu, tj. licenci uređaja koji koristimo. U našem testiranju flow podatke prikupljamo na flow0 sučelje kolektora, te ih prosljeđujemo na flow0 sučelje kontrolera.

Peakflow X podržava i nadzor mrežnih uređaja SNMP protokolom. Na taj način možemo vidjeti stanje pojedinih mrežnih sučelja, a u slučaju korištenja SNMP-a s pravima čitanja i pisanja, kroz Web sučelje možemo ugasiti problematično mrežno sučelje.
Nakon dodavanja, Peakflow X prikazuje hostname i IP adresu uređaja kroz Web sučelje.

4.3 Instalacija „Identity tracking" softvera

Arbor PX podržava identifikaciju korisnika korištenjem nekoliko različitih tehnologija kao što su DHCP, Radius, Microsoft Active Directory i Novell eDirectory. U našem testnom okruženju korišten je Microsoft Active Directory.
Identifikacija korisnika radi na principu mapiranja korisničkog ID-a sa IP adresom.
U slučaju korištenja Microsoft AD-a, na svaki domenski kontroler potrebno je instalirati **AuthX** agent koji HTTPS protokolom šalje informacije prema Arbor kontroleru.
Sama instalacija programa je vrlo jednostavna, a od konfiguracijskih podataka potrebno je unijeti IP adrese Arbor i AD kontrolera te zajednički ključ.



4.2: AuthX konfiguracijski dijalog na poslužiteljima AD i AD2

Valja napomenuti da dotični softver ne podržava višekorisnički rad na terminal serverima gdje je aktivno više korisnika na istoj IP adresi.

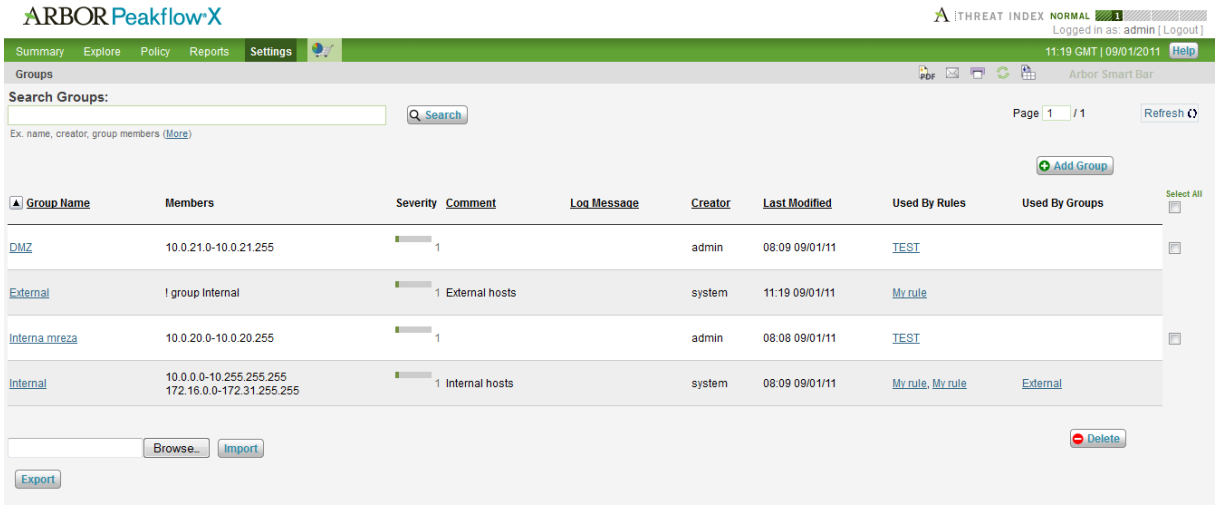
4.4 Konfiguracija objekata

4.4.1 Grupe

Kao i kod drugih uređaja slične namjene, PeakFlow X (pod *Settings* -> *Groups*) nudi jednostavno definiranje grupa računala. Moguće ih je definirati pojedinačno prema IP adresi ili grupno prema rasponu adresa. Za svaku je grupu moguće definirati i faktor ozbiljnosti prijetnje (severity) od 1 do 10 koji je bitan ukoliko se pravodobno želi uočiti upozorenje prilikom napada na najvažnije resurse u mreži. Prilikom editiranja postojeće grupe, sučelje prikazuje i sva pravila sigurnosne politike koji referenciraju dotičnu grupu.

4.4.2 Servisi

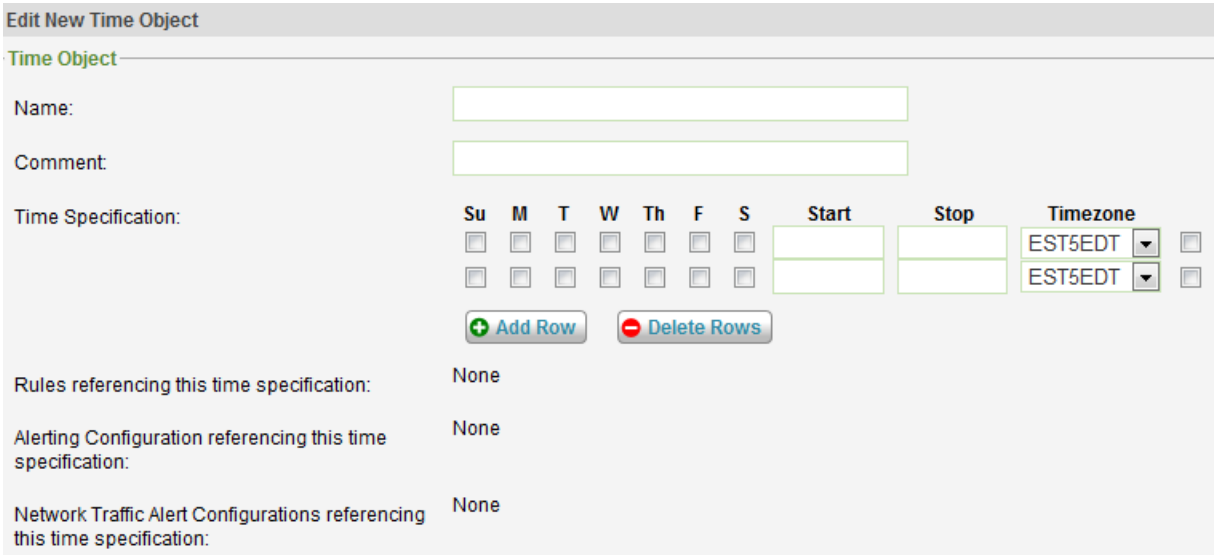
Moguće je i definirati vlastite servise, odnosno skupove servisa. Mogu se definirati prema portu kojeg koriste, kao neki od standardnih servisa ili prema aplikaciji koju je uređaj u stanju otkriti. Za ovaj se objekt također može definirati faktor ozbiljnosti prijetnje.



4.3: definiranje grupa

4.4.3 Time objekti

Peakflow X nudi jednostavnu konfiguraciju vremenskih objekata koje je moguće definirati prema pojedinim danima u tjednu i prema satima (moguće je definirati više različitih kombinacija koje onda istovremeno vrijede).



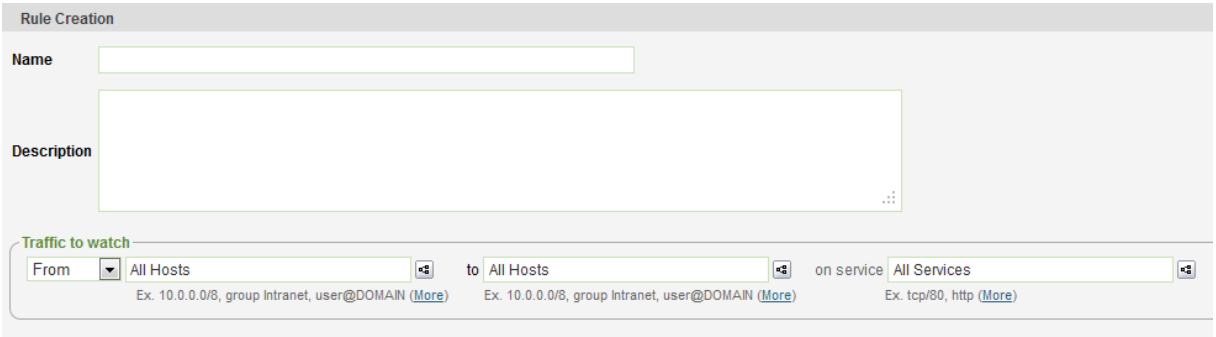
4.4: definiranje vremenskih (time) objekata

4.4.4 Notification objekti

Pomoću Notification objekata se definira kome se šalju obavijesti u slučaju generiranja određenih upozorenja. Peakflow X podržava slanje upozorenja putem elektroničke pošte, SNMP trapa ili sysloga. Sukladno tome, prilikom izrade novog objekta ove vrste, moguće je definirati više različitih adresa elektroničke pošte, do četiri poslužitelja koji će primati SNMP poruke te do četiri poslužitelja koji će primati syslog zapise.

4.5 Definiranje pravila sigurnosne politike

Pod Policy -> Management -> User-Defined Rules definiraju se pravila sigurnosne politike. Potrebno je navesti za koji će promet (rasponi adresa od, do ili između entiteta, odnosno najčešće grupa ili korisnika) vrijediti pravila. Također se definiraju vrste upozorenja koja će pravila generirati, a prilikom izmjene postojećeg pravila moguće je definirati (izabrati ponuđeni promet) i iznimke za koje se neće generirati upozorenja.



4.5: definiranja novog pravila sigurnosne politike

5 Upozorenja i izrada izvještaja

Upozorenja naravno služe kako bi pravodobno upozorila na sigurnosne prijetnje i događaje kao što su, na primjer, rušenje mrežnih čvorova ili neuspješno izvođenje pohrane sigurnosne kopije podataka (backup). U velikim mrežama važno je razlučiti važnost između različitih upozorenja koja moraju biti uočljiva, stoga PeakFlow X nudi jednostavan uvid u događaje koje su izazvali generiranje upozorenja. Takvi događaji su na listi poredani prema faktoru sigurnosnog rizika.

Izvještaji (reports) služe ponajviše tome kako bi se vidio rad mreže kroz nešto duži vremenski period. Često ih koristi menadžment ili odjeli koji nadziru korištenje mrežne infrastrukture. Oni su također velika pomoć pri implementaciji raznih sigurnosnih standarda koje mnoge tvrtke moraju poštovati.

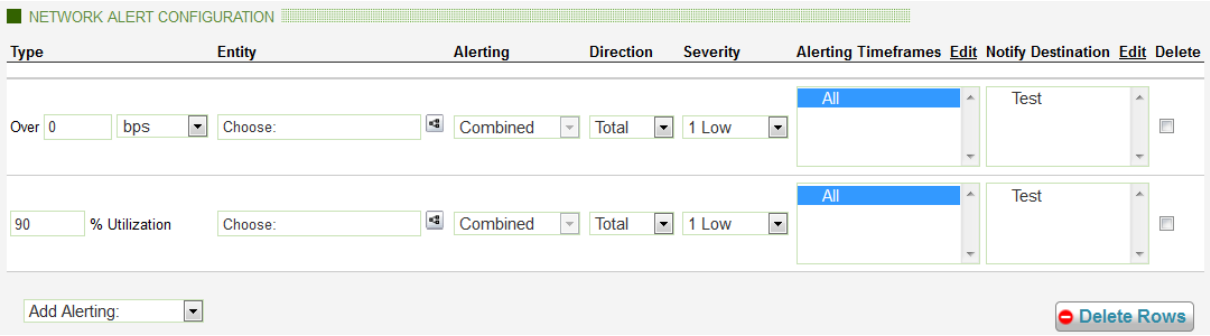
5.1 Upozorenja (Alerting)

Za svako ponašanje u mreži koje PeakFlow X može otkriti, moguće je definirati pri kojem će događaju (ako je unutar objektom definiranog vremenskog intervala i/ili grupe) sustav generirati određenu vrstu upozorenja (Alert Type). Neke od vrsta upozorenja su (svaka je vrsta prikazana zasebnom ikonom unutar sučelja):

- **Client** - generira se prilikom otkrivanja računala koje prethodno nije viđeno unutar određenog mrežnog prometa (grupe)
- **Server** - generira se prilikom otkrivanja novog poslužitelja
- **Connection** - bilo kakva veza koja ne poštuje definiranu sigurnosnu politiku
- **Over / Under Rate** - promet je u periodu dužem od dvije minute iznad, odnosno ispod konfigurirane vrijednosti
- **Over / Under Baseline** - promet je u definiranom periodu iznad, odnosno ispod normalne (baseline[1]) vrijednosti
- **Host Pair** - promet između dva računala koji prethodno nije viđen unutar praćene grupe

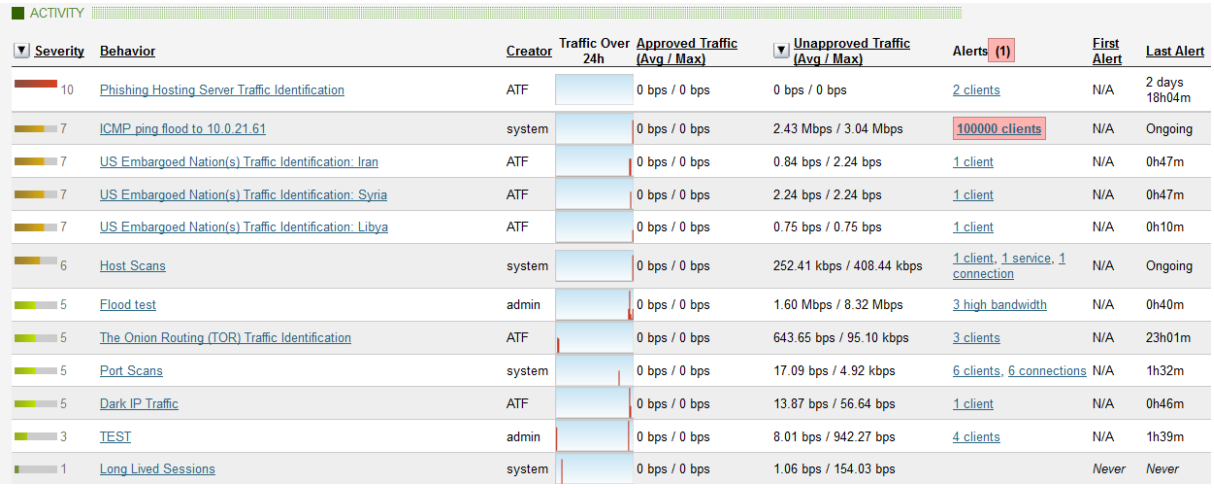
Postoje i posebne vrste upozorenja za sistemske događaje kao što su: pad ili podizanje kolektora, izvora flow podataka itd. Ona se mogu konfigurirati pod *Policy -> Management -> System Events*. Tu su i mrežna upozorenja koja se mogu konfigurirati pod *Policy -> Network Alerts*. Riječ je o upozorenjima koja se koriste za praćenje stanja mrežnog prometa za određene usmjerivače, sučelja i grupe sučelja. Kada je takav promet ispod ili iznad konfigurirane vrijednosti, Peakflow X generira upozorenja. Tu vrijednost je moguće definirati i prema postotku potrošenog maksimuma propusnosti sučelja.

[1] riječ je o vrijednosti koja značajno odstupa od vrijednosti koju je uređaj „naučio“ u periodu od najmanje tjedan dana tijekom kojih je pratio promet u mreži



5.1: konfiguriranje novog mrežnog upozorenja

Prethodno spomenuta *Activity* stranica sučelja (*Policy -> Activity*) služi za praćenje trenutnog stanja mreže. Stanje je moguće pratiti kroz događaje koji su doveli do generiranja upozorenja, kroz događaje koji ne generiraju upozorenja, kroz upozorenja koje je generirao sustav ATF, prema upozorenjima nastalima kršenjem definiranog pravila sigurnosne politike ili pak kroz upozorenja nastala kršenjem pravila koja je definirao sam korisnik (trenutno ulogiran).

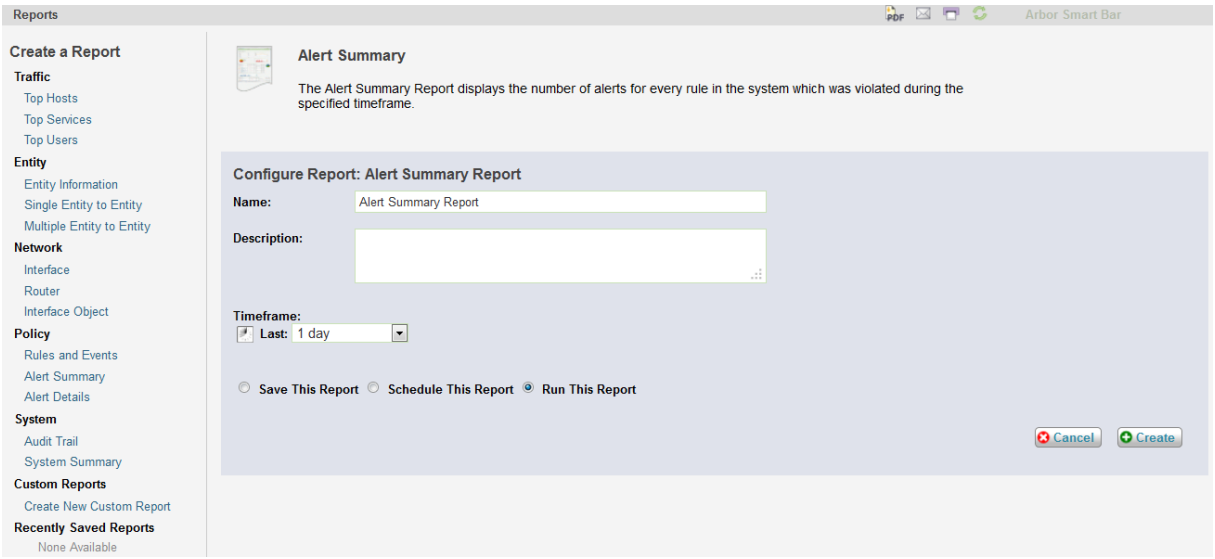


5.2: lista generiranih upozorenja (Activity)

Pomoću manjeg grafičkog prikaza moguće je vidjeti promet u posljednja 24 sata, a uz ostale informacije tu su i količine odobrenog prometa (putem definiranih iznimki u pravilima) i prometa koji nije odobren.

5.2 Izvještaji (Reports)

Kako bi se pratio način na koji se koristi mrežna infrastruktura, Peakflow X omogućuje izradu izvještaja iz podataka koje uređaj neprestano prikuplja. U glavnom izborniku web sučelja nalazi se posebni dio namijenjen tome, pod karticom „*Reports*“.

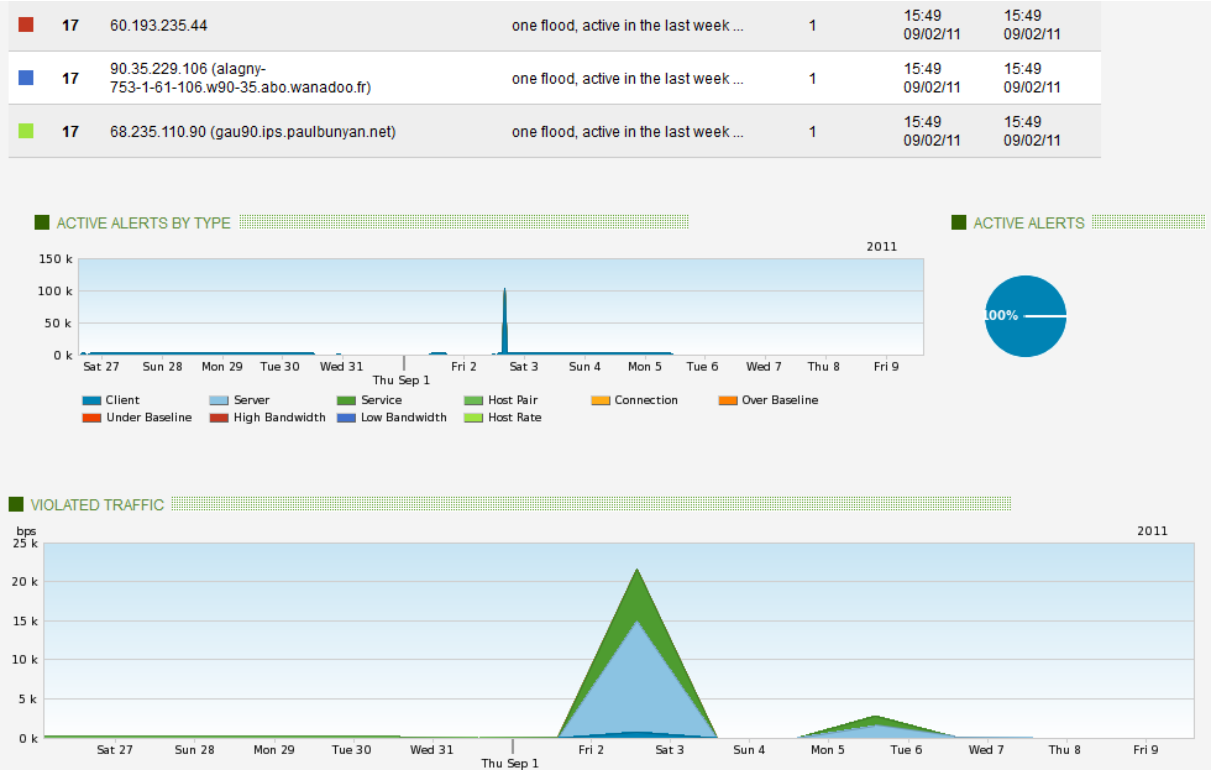


5.3: izrada novog izvještaja

Moguće je izraditi različite vrste izvještaja (što je vidljivo na izborniku na slici lijevo): prema računalima, servisima, poslužiteljima, entitetima (to može biti računalo, korisnik, poslužitelj, servis itd.), web prometu, posjećenim URL-ovima, sučeljima, usmjerivačima, kršenjima sigurnosnih pravila, generiranim upozorenjima itd. Za sve spomenute vrste izvještaja, potrebno je definirati vremenski okvir koji će se uzeti u obzir. Kod definiranja entiteta, uređaj traži promet prema sljedećem redoslijedu:

1. IP adrese
2. CIDR blokove IP adresa
3. imena računala
4. imena grupa

Izvještaje je moguće trenutačno generirati, unaprijed konfigurirati (pa kasnije izraditi) ili namjestiti njihovu automatsku, vremenski predodređenu izradu („*Scheduled Reports*“). Ukoliko se koristi posljednja opcija, izvještaje je moguće automatski, putem elektroničke pošte proslijediti definiranim primateljima (navedenih unutar notifikacijskog objekta koji se odabere). Moguće ih je izraditi u tri različita formata: PDF, XLS ili CSV. Obični korisnici mogu pregledavati sve izvještaje, ali brisati samo one koje su sami izradili. Sustav izvještaje čuva godinu dana, a nakon tog perioda ih briše. Ukoliko želimo pronaći jedan od postojećih izvještaja, tu je opcija, odnosno polje „*Search Recent Reports*“. Izvještaje je moguće pretraživati prema ID-u, naslovu ili imenu korisnika koji ga dao izraditi.



5.4: isječak iz primjera izvještaja

Kao što je vidljivo, proizvođač je izvještajima posvetio posebnu pozornost, što i nije iznenađujuće s obzirom na njihovu višestruku korist u nekoj tvrtki.

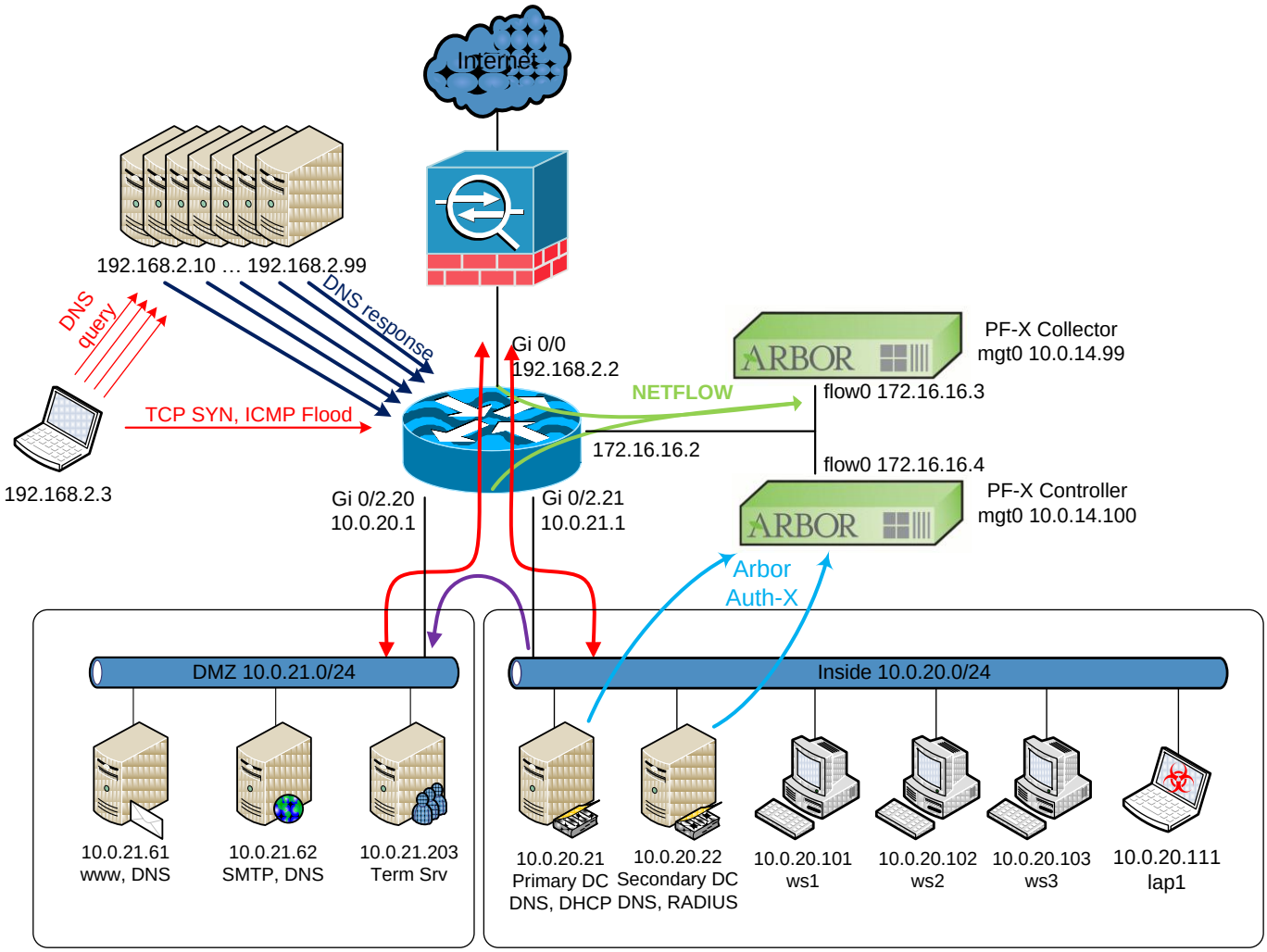
6 Testiranje

U vezi testiranja uređaja Arbor Peakflow X, bitno je naglasiti kako je fokus ovog testa bio na testiranju mogućnosti uređaja s aspekta sigurnosti, a ne praćenja operabilnosti računalne mreže.

6.1 Testna mreža i konfiguracija

Na slici 6.1 prikazana je topologija mreže korištene prilikom testiranja uređaja. Konfigurirane su dvije mreže: interna s rasponom IP adresa 10.0.21.0/24 te DMZ s rasponom 10.0.20.0/24. U internu mrežu smještene su radne stanice i dva Microsoft Active Directory poslužitelja (AD1 i AD2), a u DMZ web i mail poslužitelji te Terminal Server.
Za provedbu testa korišten je Cisco 2911 usmjerivač koji šalje NetFlow podatke inačice 5. Peakflow X inače podržava NetFlow inačica 1, 5, 7 i 9. Usmjerivač je konfiguriran tako da prikuplja Netflow sa sučelja Gi 0/2.20, Gi 0/2.21 i Gi 0/0.

Menadžment sučelja na Peakflow X virtualnim uređajima (mgt0) su konfigurirana prema dokumentaciji te su im dodijeljene IP adrese 10.0.14.99 (kolektor) i 10.0.14.100 (kontroler). Sučelja za Netflow promet (flow0) spojena su u zasebnu mrežu. Kolektor prihvaća Netflow promet s usmjerivača (IP 172.16.16.2) na IP adresi 172.16.16.3 te nakon obrade i konverzije u Arborflow format, šalje kontroleru na IP 172.16.16.4.



6.1: topologija mreže korištene prilikom testiranja

Na oba domenska kontrolera instaliran je Arbor PF-X klijentski softver koji kontroleru šalje korisnička imena ulogirana na pojedinim računalima, odnosno IP adresama. Time je omogućeno praćenje aktivnosti pojedinih korisnika bez obzira na kojem računalu su ulogirani.

6.2 Simulacija korisnika u internoj mreži

Za potrebe ovog testa kreirano je nekoliko korisničkih računa na domenskom kontroleru. Korisničke radne stanicu u testu su simulirale uobičajen uredski promet, odnosno korištene su za pregledavanje web portala, preuzimanje datoteka putem HTTP-a i FTP-a itd.

6.3 Otkrivanje aplikacija

Pod *Policy -> Management* nalazi se popis predefiniranih pravila sigurnosne politike. Među njima se nalaze i pravila koja omogućuju detekciju pojedinih aplikacija. Testirali smo detekciju Bittorent prometa i Facebook aplikacija.

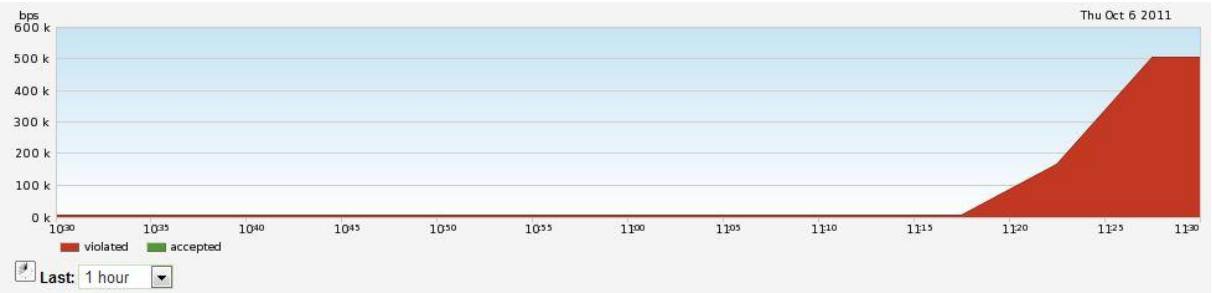
6.3.1 BitTorrent

Prema navodima u opisu pravila, uređaj prepoznaje poznate BitTorrent portove (TCP 6881-6889). Zatim detektira "peer" računala kao klijente, poslužitelje ili oboje.
Prilikom testa, uređaj je uspješno prepoznao računalo koje koristi bittorrent i sastavio listu peer/seed računala s kojima je bila uspostavljena BitTorrent komunikacija.

Severity	Client	Client Interface	Num Servers	Num Service
5	10.0.20.112	arbor-test (172.16.16.2): arborPX - interna mreza Gi0/2.20 GigabitEthernet0/2.20	713	564
5	173.255.125.116 (116.125.255.173.bc.googleusercontent.com)	arbor-test (172.16.16.2): up-link Gi0/0 GigabitEthernet0/0	1	1
5	85.60.124.237 (237.pool85-60-124.dynamic.orange.es)	arbor-test (172.16.16.2): up-link Gi0/0 GigabitEthernet0/0	1	6
5	208.64.36.69	arbor-test (172.16.16.2): up-link Gi0/0 GigabitEthernet0/0	1	3
5	195.222.89.198 (ppp-195-222-89-198.pe1-dynamic.solo.hv)	arbor-test (172.16.16.2): up-link	1	2

6.2: računalo u lokalnoj mreži i druga peer računala

Kao i za druga pravila moguće je definirati vremenske okvire kad je korištenje omogućeno (pauza, izvan radnog vremena) te definirati servise i mreže za koje želimo da uređaj generira upozorenja.



6.3: prikaz BitTorrent prometa

6.3.2 Facebook

Uređaj provjerava HTTP i HTTPS promet prema Facebookovim mrežama koje se nalaze iza ASN broja (autonomnog sustava) 32934. U opisu sigurnosne politike dan je i popis IP adresa (mreža) Facebooka ukoliko se promet prema njima želi ručno blokirati na vatrozidu ili sl.

Trigger

This policy looks for HTTP and HTTPS traffic destined to the Facebook network in ASN 32934.

Affected Platforms and Versions

Any computer with a web browser can be used to access the Facebook website.

Remediation

A number of third party products are able to block Facebook access via DNS and other means.

Workaround

We recommend blocking the known Facebook IP address ranges to prevent login and website use. These address ranges are: 66.220.144.0/20,69.63.176.0/20,74.119.76.0/22, and 204.15.20.0/22.

General References

Date	Organization	Author	E-mail Address	Title
2008-07-08	Facebook			Facebook website

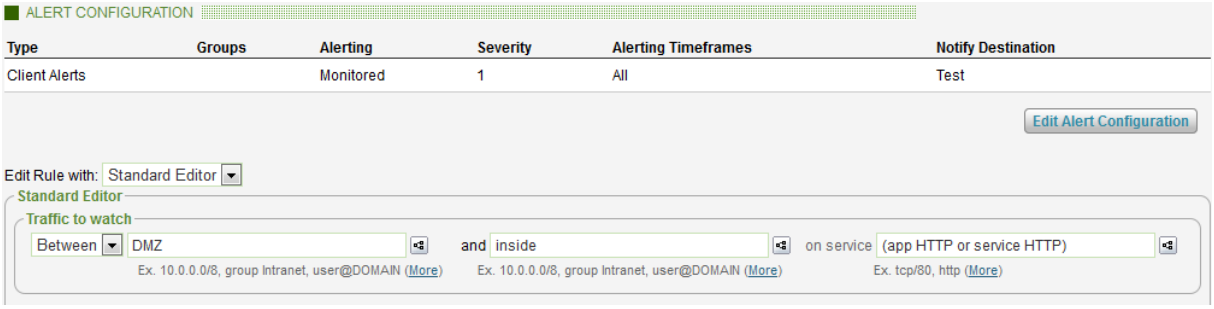
Revision History

5 - Fix spelling typo, add note about Koobface Trojan.
6 - Add support for new Facebook CDN routes in AS32934.
7 - Update BGP routes.

6.4: dio opisa predefiniranog pravila koje omogućuje otkrivanje Facebook aplikacije

6.4 Otkrivanje novih klijenata u mreži

Konfigurirano je i pravilo za otkrivanje novih korisnika HTTP servisa unutar DMZ mreže:



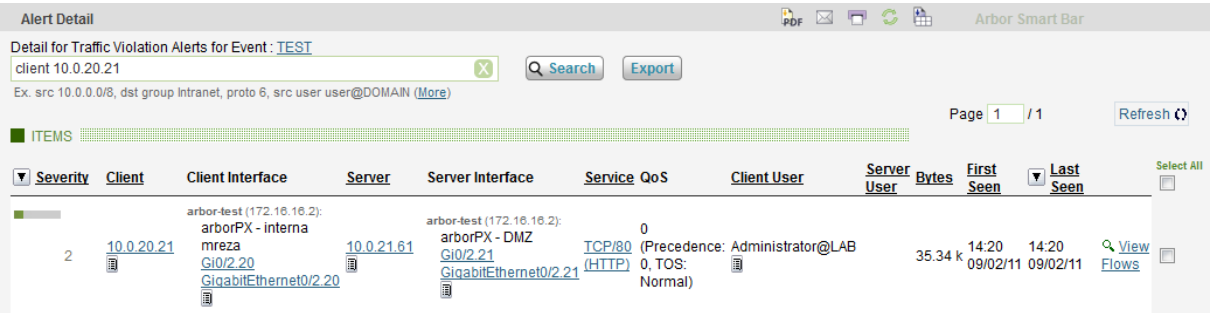
6.5: pravilo za otkrivanje novih korisnika

Svaki put kada se novi korisnik koji se iz interne mreže spoja na neki web poslužitelj, administratori dobivaju e-mail poruku s upozorenjem i linkom na detaljne informacije o incidentu, npr:

Izvadak iz primljene e-mail poruke:

```
------------------------------
Type:     Unapproved Client
Rule:     TEST
URL:       https://controller.lab.cert.hr/event_detail/alertdetail/?type=3&
search_text=client+10.0.20.21&id=233
Severity: 1
Client:   10.0.20.21
Server:   10.0.21.61
Service:  TCP/80
```

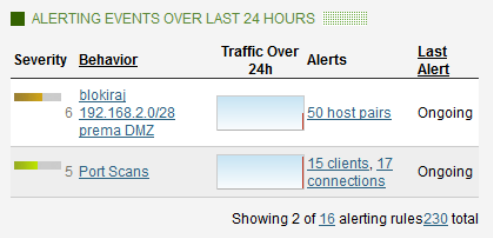
Detaljniji prikaz u web sučelju Peakflow X kontrolera, prikazan je na slici 6.6.:



6.6: upozorenje o novom korisniku u mreži

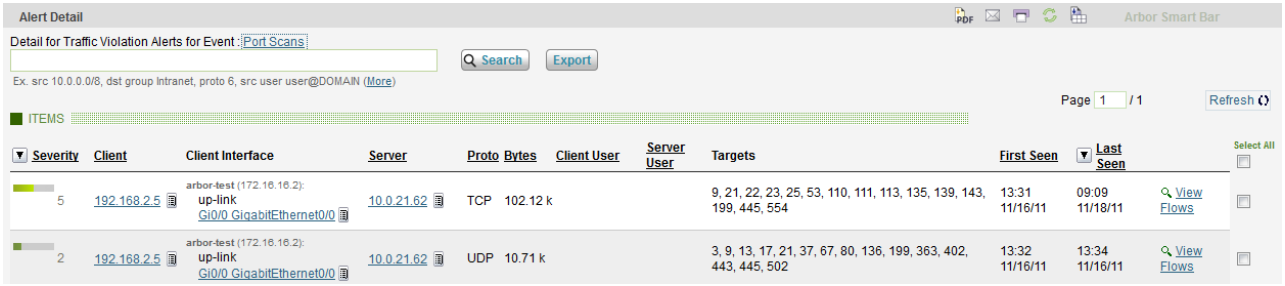
6.5 Skeniranje portova

S računala u vanjskoj mreži pokrenuto je skeniranje portova mail poslužitelja unutar DMZ-a Ubrzo se na web sučelju kontrolera pojavilo upozorenje o zabilježenom skeniranju portova koje je u tijeku.



6.7: upozorenje o skeniranju portova

Detaljniji prikaz zabilježenog skeniranja unutar web sučelja prikazan je na slici ispod:



6.8: detalji o skeniranju portova

6.6 Denial of Service napadi

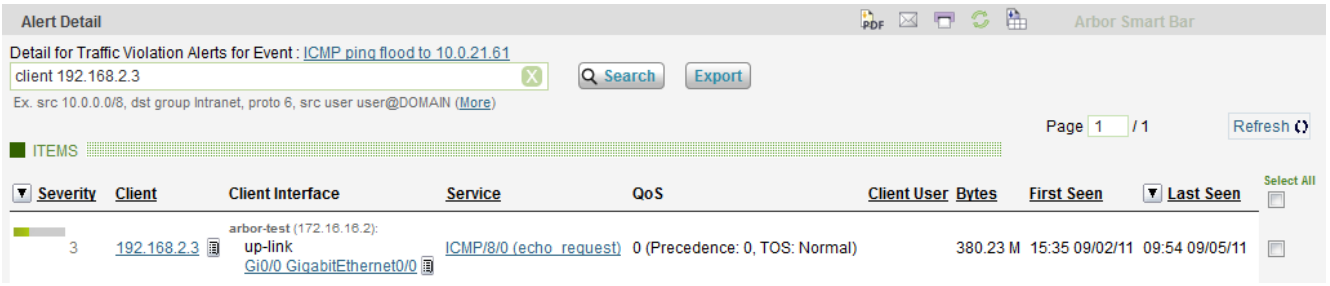
Obzirom da se u daljnjim testovima koriste virusi i krivotvorene (engl. spoofed) izvorišne adrese paketa, testovi su iz sigurnosnih razloga provedeni u potpunosti odvojeno od Interneta. U suprotnom bi postojala mogućnost širenja virusa, curenja informacija ili slanja neželjenih paketa van mreže, kao odgovor na krivotvorene dolazne pakete.

6.6.1 Ping Flood

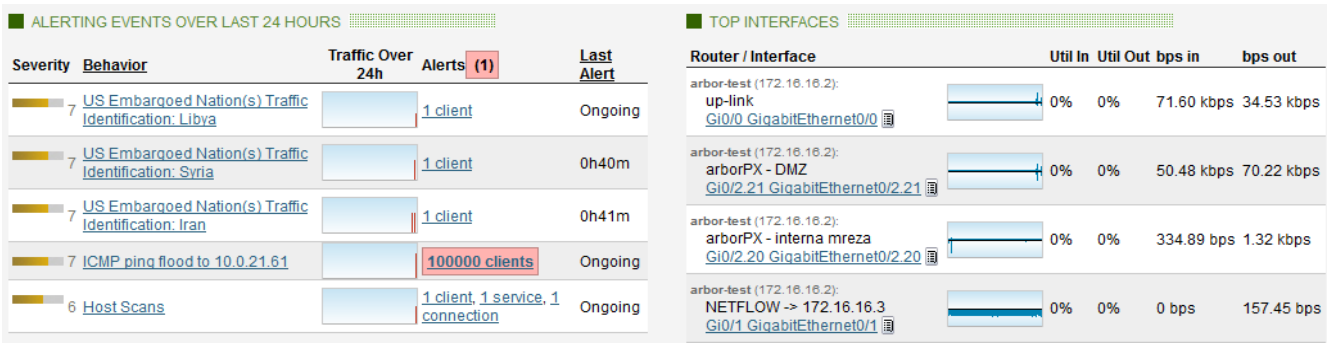
S prijenosnog računala u vanjskoj mreži pokrenut je ICMP flood napad, prvo bez korištenja tehnika prikrivanja, a zatim s krivotvorenim izvorišnim adresama. Neke od nasumično generiranih adresa su spadale u IP prostore zemalja koje su pod sankcijama te su za njih generirana posebna upozorenja (slika 6.10).

Izvadak iz primljene e-mail poruke:

```
-----------------------------
Type:      Static High Bandwidth
Rule:      Flood test
URL:        https://controller.lab.cert.hr/event_detail/alertdetail/?id=234&
type=4&units=0
Severity: 5
Expected: 1.00 Mbps
Actual:    4.85 Mbps
```

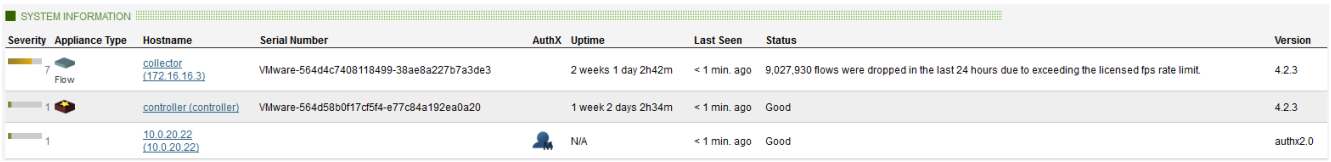


6.9: upozorenje o ICMP Flood napadu



6.10: upozorenje o ICMP Flood napadu s krivotvorenim IP adresama

Kako je napad simuliran preko gigabitnog linka bez limitiranja propusnosti, svake sekunde je generirano približno 25000 ICMP echo zahtjeva. PeakFlow-X Virtual licenca limitira broj netflow zapisa koje može obraditi u sekundi na 16000 (HW appliance može obraditi 32000 zapisa u sekundi).



6.11: upozorenje o zanemarenom Netflow prometu

6.6.2 „DNS Amplification“ napad

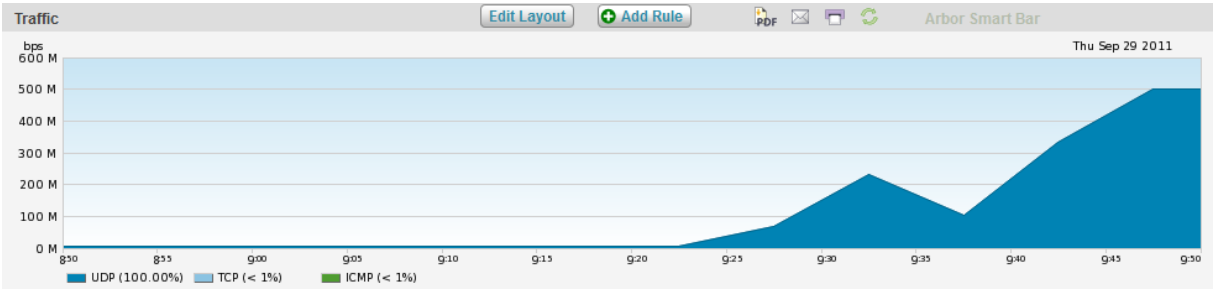
S računala u vanjskoj mreži generiran je velik broj DNS upita prema otvorenim DNS poslužiteljima. Pri tome je izvorna adresa krivotvorena kako bi se svi odgovori DNS poslužitelja slali meti napada, u našem slučaju, web poslužitelju na IP adr. 10.0.21.61.
Kako bi se povećao učinak napada, postavljani su upiti za domenu s velikim tekstualnim (TXT) zapisima čime se višestruko povećava veličina svakog pojedinog odgovora.

Dolazni promet na poslužitelju 10.0.21.61:

No.	Time	Source	Destination	Protocol	Info
15	1.872734	192.168.2.24	10.0.21.61	DNS	Standard query response TXT TXT TXT TXT
16	1.872737	192.168.2.25	10.0.21.61	DNS	Standard query response TXT TXT TXT TXT
17	1.872740	192.168.2.26	10.0.21.61	DNS	Standard query response TXT TXT TXT TXT
18	1.872744	192.168.2.27	10.0.21.61	DNS	Standard query response TXT TXT TXT TXT
19	1.872840	192.168.2.28	10.0.21.61	DNS	Standard query response TXT TXT TXT TXT

6.12: dolazni paketi na web serveru

Pregled prometa na poslužitelju 10.0.21.61:

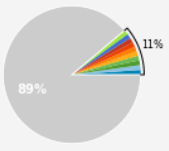


6.13: pregled količine prometa na vanjskom sučelju usmjerivača

Pregled "*Top Connections*" daje detaljniji prikaz 10 konekcija s najvećim prometom.
Kako promet dolazi sa 90 DNS poslužitelja, svaki poslužitelj generira približno 1.1% ukupnog prometa.

TOP CONNECTIONS

Key	Client	Server	Service	Bytes	bps	% total bps	Packets	pps	Flows	fps
	192.168.2.73	10.0.21.61	UDP/53 (DNS)	300.67 M	3.08 Mbps	1.1%	593.04 k	760.30	11	0.01
	192.168.2.63	10.0.21.61	UDP/53 (DNS)	300.67 M	3.08 Mbps	1.1%	593.03 k	760.29	11	0.01
	192.168.2.15	10.0.21.61	UDP/53 (DNS)	300.66 M	3.08 Mbps	1.1%	593.02 k	760.28	11	0.01
	192.168.2.84	10.0.21.61	UDP/53 (DNS)	300.66 M	3.08 Mbps	1.1%	593.02 k	760.28	11	0.01
	192.168.2.36	10.0.21.61	UDP/53 (DNS)	300.66 M	3.08 Mbps	1.1%	593.02 k	760.28	11	0.01
	192.168.2.19	10.0.21.61	UDP/53 (DNS)	300.66 M	3.08 Mbps	1.1%	593.02 k	760.28	11	0.01



6.14: pregled konekcija sa najvećim prometom

6.7 Pojava i širenje malvera u internoj mreži

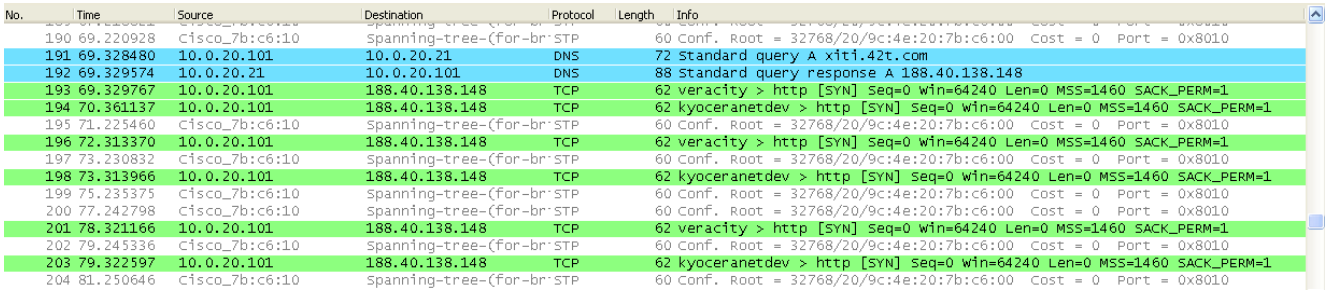
Peakflow X ima predefinirana pravila sigurnosne politike koja bi trebala prepoznati aktivnost malvera i spriječiti daljnje nanošenje štete. Neki od poznatijih malvera za koje postoje pravila su SpyEye, Zeus i Stuxnet. Aktivnost malvera se prepoznaju na temelju komunikacije s kontrolnim (C&C) poslužiteljima i određenim računalima na Internetu. Sljedeći testovi su iz sigurnosnih razloga provedeni odvojeno od Interneta. Budući da

većina malvera prije komunikacije s kontrolnim poslužiteljima provjerava vezu prema Internetu, nismo bili u mogućnosti detaljnije provjeriti ovu funkcionalnost.

Kako bi se dobio što vjerniji prikaz ponašanja malvera, testovi su provedeni u nekoliko iteracija te se u svakoj iteraciji na lokalnim DNS serverima (AD, AD2) ručno dodavalo poslužitelje kojima je malver pokušavao pristupiti (dodavane su stvarne javne IP adrese dobivene iz DNS upita u danom trenutku). Tako je malver uzorcima omogućeno da barem pokušaju uspostaviti konekciju prema Internetu što je vidljivo na usmjerivaču, te u Netflow zapisima.

6.7.1 SpyEye

Krajem 2009. godine uočena je nova vrsta malvera, slična zloglasnom bankarskom trojanskom konju Zeusu. Riječ je o SpyEye-u, malveru posebno dizajniranom za krađu podataka za Internet bankarstvo. Autor malvera, odnosno organizacija koja stoji iza njega na crnom tržištu prodaje toolkit (SpyEye builder) za izradu malvera kojeg onda tehnički manje vješti kriminalci raspačavaju kako bi zarazili što veći broj računala, a time i stekli što veću financijsku korist. Zaraženo računalo postaje dio botnet mreže kojom se upravlja preko kontrolnih poslužitelja. Sukladno tome, nakon što se malver instalira na računalu, prvo šalje DNS upit za neki od svojih kontrolnih poslužitelja kako bi ostvario vezu, odnosno bio spreman za zaprimanje naredbi.
Analizom mrežnog prometa programom Wireshark vidi se slanje DNS upita za server xiti.42t.com te pokušaj spajanja na pripadajuću IP adresu.



No.	Time	Source	Destination	Protocol	Length	Info
190	69.220928	Cisco_7b:c6:10	Spanning-tree-(for-br	STP	60	Conf. Root = 32768/20/9c:4e:20:7b:c6:00 Cost = 0 Port = 0x8010
191	69.328480	10.0.20.101	10.0.20.21	DNS	72	Standard query A xiti.42t.com
192	69.329574	10.0.20.21	10.0.20.101	DNS	88	Standard query response A 188.40.138.148
193	69.329767	10.0.20.101	188.40.138.148	TCP	62	veracity > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
194	70.361137	10.0.20.101	188.40.138.148	TCP	62	kyoceranetdev > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
195	71.225460	Cisco_7b:c6:10	Spanning-tree-(for-br	STP	60	Conf. Root = 32768/20/9c:4e:20:7b:c6:00 Cost = 0 Port = 0x8010
196	72.313370	10.0.20.101	188.40.138.148	TCP	62	veracity > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
197	73.230832	Cisco_7b:c6:10	Spanning-tree-(for-br	STP	60	Conf. Root = 32768/20/9c:4e:20:7b:c6:00 Cost = 0 Port = 0x8010
198	73.313966	10.0.20.101	188.40.138.148	TCP	62	kyoceranetdev > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
199	75.235375	Cisco_7b:c6:10	Spanning-tree-(for-br	STP	60	Conf. Root = 32768/20/9c:4e:20:7b:c6:00 Cost = 0 Port = 0x8010
200	77.242798	Cisco_7b:c6:10	Spanning-tree-(for-br	STP	60	Conf. Root = 32768/20/9c:4e:20:7b:c6:00 Cost = 0 Port = 0x8010
201	78.321166	10.0.20.101	188.40.138.148	TCP	62	veracity > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
202	79.245336	Cisco_7b:c6:10	Spanning-tree-(for-br	STP	60	Conf. Root = 32768/20/9c:4e:20:7b:c6:00 Cost = 0 Port = 0x8010
203	79.322597	10.0.20.101	188.40.138.148	TCP	62	kyoceranetdev > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
204	81.250646	Cisco_7b:c6:10	Spanning-tree-(for-br	STP	60	Conf. Root = 32768/20/9c:4e:20:7b:c6:00 Cost = 0 Port = 0x8010

6.15: pokušaj spajanja na kontrolni poslužitelj [slika iz alata Wireshark]

Na kolektoru se također može uočiti pokušaje spajanja na vanjsku IP adresu 188.40.138

```
admin@collector:/services/x/flow# watch fcap "client 10.0.20.101"
type,source,dest,proto,sport,dport,tcpflags_src,tcpflags_dst,start,stop,pkts_src,pkts_dst,bytes_src,bytes_dst,rtr_a,rtr_b
s,10.0.20.101,188.40.138.148,6,1062,80,2,0,2011-09-19 14:06:27+00,2011-09-19 14:06:36+00,3,0,144,0,172.16.16.2,172.16.16.2
s,10.0.20.101,188.40.138.148,6,1063,80,2,0,2011-09-19 14:06:28+00,2011-09-19 14:06:37+00,3,0,144,0,172.16.16.2,172.16.16.2
s,10.0.20.101,10.0.20.255,17,138,138,0,0,2011-09-19 14:09:12+00,2011-09-19 14:09:12+00,1,0,229,0,172.16.16.2,172.16.16.2
s,10.0.20.101,10.0.20.255,17,137,137,0,0,2011-09-19 14:09:18+00,2011-09-19 14:09:30+00,9,0,702,0,172.16.16.2,172.16.16.2
```

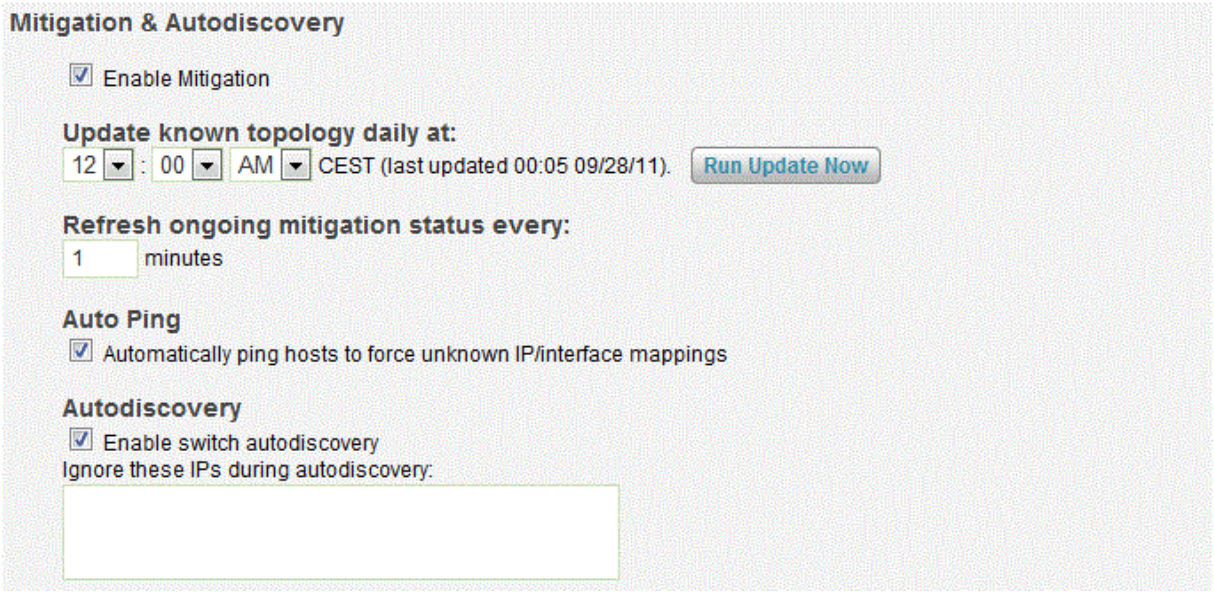
6.16: kolektor također vidi pokušaj spajanja na kontrolni poslužitelj

Kako su testovi provedeni odvojeno od Interneta, konekcija se ne može uspostaviti te PeakFlow u takvim okolnostima ne detektira SpyEye.

6.8 SNMP mitigation

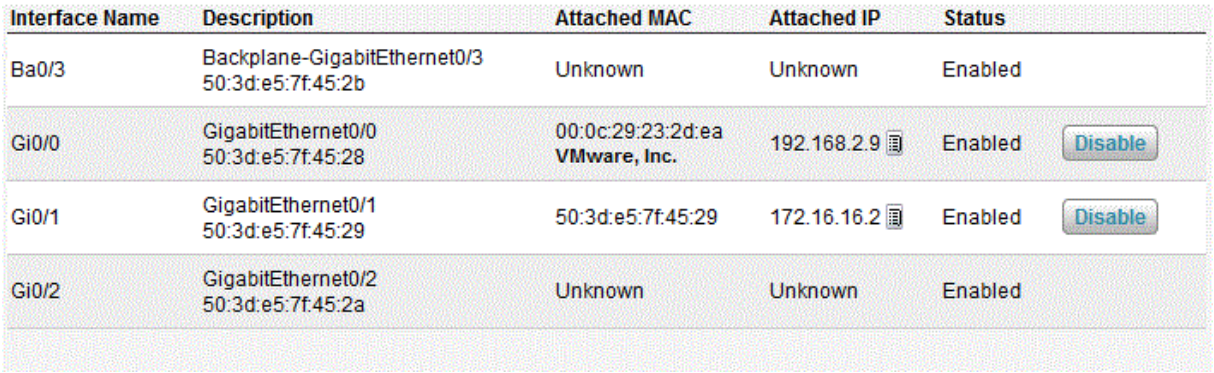
Peakflow X nam omogućuje nadzor i konfiguraciju sučelja mrežnih uređaja putem SNMP protokola. Na taj način se dobija uvid u opterećenje i stanje pojedinih sučelja. Kroz web sučelje je moguće i isključivanje problematičnih sučelja.

Nove uređaje možemo dodati ručno ili pokrenuti funkciju „*Autodiscovery*“ koja uspješno pronalazi sve mrežne uređaje koji imaju ispravno podešene SNMP postavke.



6.17: definiranje automatskog otkrivanja mrežnih uređaja

U testu smo koristili usmjerivač Cisco 2911 i preklopnik Cisco 3560. Jedan smo dodali ručno, dok je drugog uređaj pronašao korištenjem funkcije „autodiscovery“. Za L3 sučelja Arbor PX je u nekoliko testova uspješno prepoznao problematične IP adrese, te ponudio opciju da se isključi sučelje kroz koji prolazi problematični promet.

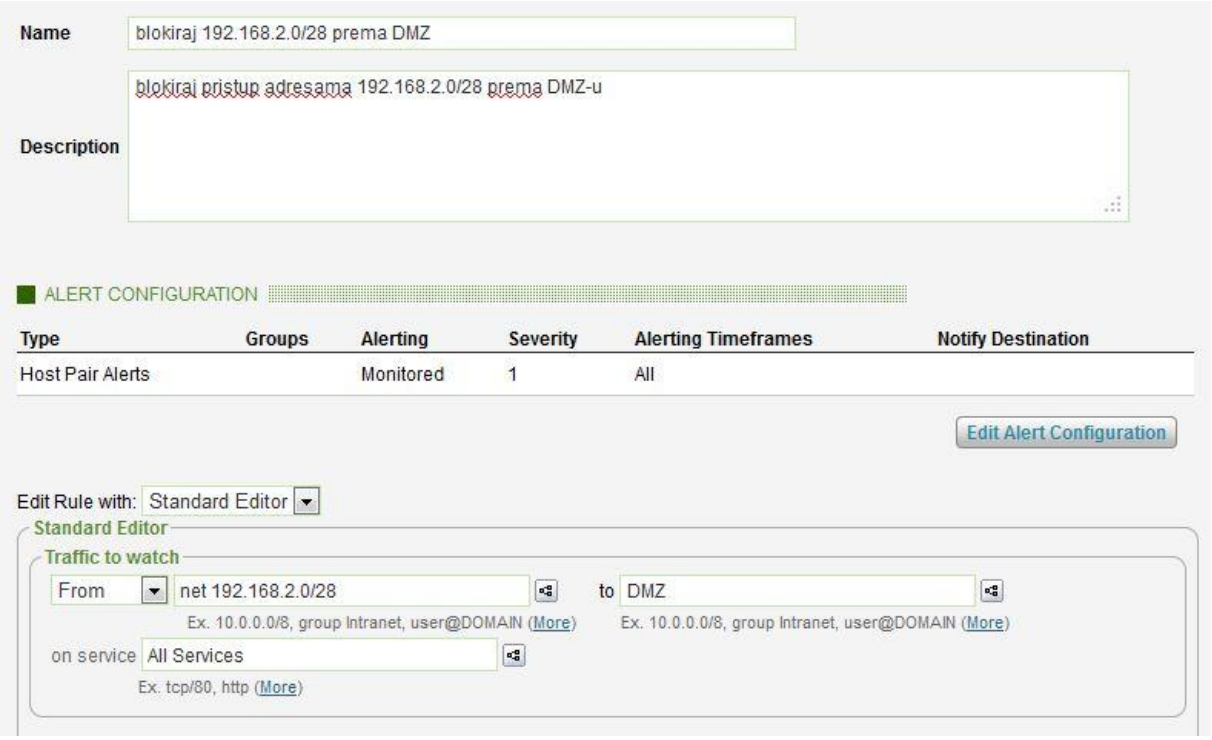


Interface Name	Description	Attached MAC	Attached IP	Status	
Ba0/3	Backplane-GigabitEthernet0/3 50:3d:e5:7f:45:2b	Unknown	Unknown	Enabled	
Gi0/0	GigabitEthernet0/0 50:3d:e5:7f:45:28	00:0c:29:23:2d:ea **VMware, Inc.**	192.168.2.9	Enabled	Disable
Gi0/1	GigabitEthernet0/1 50:3d:e5:7f:45:29	50:3d:e5:7f:45:29	172.16.16.2	Enabled	Disable
Gi0/2	GigabitEthernet0/2 50:3d:e5:7f:45:2a	Unknown	Unknown	Enabled	

6.18: pronađena sučelja na raznim uređajima

6.9 Access Control List (ACL)

Korisna značajka kod uređaja je što automatski kreira pristupne liste (ACL) vezane uz pravila sigurnosne politike. Takve liste administratorima mrežnih uređaja omogućuju jednostavnu provedbu sigurnosne politike „copy-paste" metodom.
U testu smo kreirali novo pravilo kojim želimo mreži 192.168.2.0/28 blokirati pristup DMZ-u.

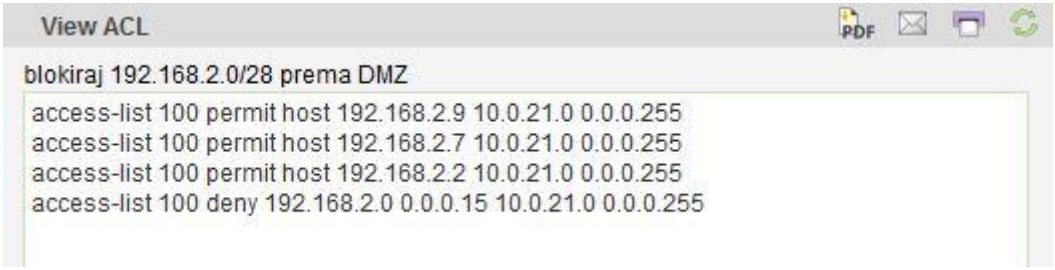


6.19: novo pravilo sigurnosne politike

Nakon definiranja novog pravila izuzet ćemo neka računala iz njega i jedino njihov promet proglasiti legitimnim.

6.20: računala kojima želimo omogućiti pristup mreži

Pristupne liste se kreiraju automatski na osnovu naših definiranih pravila. Možemo je vidjeti klikom na „*View ACL*“. Pristupna lista se može mijenjati dodavanjem i brisanjem računala ili mreža čiji promet želimo proglasiti legitimnim.



6.21: primjer automatski generirane ACL liste

7 Zaključak

Količina mrežnog prometa i broj korištenih servisa unutar velikih poslovnih okruženja je u sve bržem porastu. S druge strane, sigurnosne prijetnje također postaju sve složenije, u toj mjeri da ih je nemoguće precizno definirati bez točnog tehničkog poznavanja okoline. Stoga se, s aspekta informacijske sigurnosti, naglasak s zaštite najvažnijih resursa prebacuje na mogućnost izdvajanja pojedinih i bitnih informacija o prijetnjama. NBA (Network Behavioral Analysis) tehnologija koju implementira Peakflow X nam to upravo i omogućuje. Također, Arbor preko svojeg globalnog sustava ATLAS, svojim korisnicima omogućuje uvid i olakšano provođenje potrebnih zaštitnih mjera za prijetnje koje su se, u tom trenutku, pojavile na drugom kraju svijeta. S obzirom da se današnje sigurnosne prijetnje unutar globalne mreže ne mogu promatrati izolirano, Arbor se s navedenim sustavom drži trenda.

Mogućnosti koje uređaj Peakflow X nudi u pogledu nadzora mreže su zaista velike. Mrežni promet je tako moguće sumarno pratiti prema sučeljima, servisima (aplikacijama i portovima), korisnicima, količini prometa itd. Uređaj generira upozorenja u slučaju povrede predefiniranih ili pravila koje je kreirao sam korisnik. Vrlo je zgodna i mogućnost definiranja faktora ozbiljnosti prijetnje unutar različitih parametara što olakšava otkrivanje zlouporabe, odnosno sigurnosnih prijetnji koje pogađaju neki od važnih resursa u mreži. Nakon dva tjedna korištenja, uređaj je pomoću svojih tehnika za „učenje“ sebi definirao normalne vrijednosti raznih parametara mrežnog prometa kako bi znao izdvojiti neobično ponašanje unutar mreže koju nadzire. Uređaj je na testu pravilno otkrio korištenje aplikacija kao što su Facebook i BitTorrent, također je otkrio nove korisnike unutar mreže te prepoznao različite oblike napada uskraćivanjem usluge (DoS). Putem ugrađenih definicija malvera i svojeg sustava ATLAS, uređaj je u stanju otkriti različite oblike malvera, no to u ovom testu nije bilo moguće u potpunosti provjeriti. Korisne su i mogućnosti nadzora i upravljanja mrežnim uređaja putem protokola SNMP i opcija definiranja ACL lista. Peakflow X omogućuje i automatiziranu izradu (kao i izradu na zahtjev) izvještaja prema zaista širokom spektru parametara.

Peakflow X je pokazao kako se putem jednog mrežnog uređaja može na vrijeme procijeniti sigurnosni rizik za cijelu mrežu i dobiti potrebne informacije za sprječavanje moguće zlouporabe bila ona izvana ili iznutra.