CENTRALIZOVANI SISTEM ZA FILTRIRANJE WEB SAOBRAĆAJA

CENTRALIZED SYSTEM FOR WEB TRAFFIC FILTERING

Ivan Ivanović[1], Jovana Palibrk[2], Miloš Kukoleča[2]
[1]Računarski Centar Univerziteta u Beogradu
[2]Akademska Mreža Srbije

Sadržaj *- U ovom radu je opisano tehničko rešenje implementacije centralizovanog firewall sistema u okviru kampus okruženja. Pored dizajna i pozicioniranja sistema u okviru kampusa, dokument obuhvata i druge bitne preporuke kao što su mehanizmi za ravnomernu distribuciju web saobraćaja. U radu su obrazložene prednosti i mane korišćenja Ironport centralizovanog sigurnosnog sistema. Iako je u dokumentu opisan rad sa specijalizovanom Cisco Ironport opremom, pojedine ideje i tehnologije se mogu primeniti i na opremi bilo kojeg drugog proizvođača. Ideja za ovaj rad je nastala tokom rada na Na3T4-Campus Best Practice tasku koji predstavlja jednu od aktivnosti Akademske mreže Republike Srbije (AMRES) na Géant projektu.*

Abstract *- This paper presents a technical solution for implementation of centralized firewall system in a campus environment. Beside recommendations regarding the design and position of the system in a campus environment, the paper also includes additional important recommendations such as web traffic load balancing mechanisms. This paper also covers the advantages and disadvantages of Ironport centralized security system. Although the paper presents results of the work on the specialized Cisco Ironport equipment, most of ideas and technologies can be applied to any other equipment manufacturers. The idea for this paper was born during the work on the Na3T4-Campus Best Practice task, which presents one of the Academic Network of Republic of Serbia (AMRES) activities on Géant project.*

1. Uvod

Usled povećanja aktivnosti korisnika na Internetu i razvoja sofisticiranih malicioznih softvera za napad javila se potreba za povećanjem nivoa sigurnosti korisnika u okviru AMRES mreže. Dosadašnje metode koje su se koristile za filtriranje Internet saobraćaja i zaštitu korisnika u okviru AMRES mreže su se mahom oslanjale na pristupne liste koje su postavljane na postojećim ruterskim platformama. Ovakav način filtriranja *web* saobraćaja ima ograničenja jer omogućava filtriranje samo na osnovu informacije o protokolu, portovima i IP adresama u okviru paketa.
U pojedinim institucijama AMRES-a, gde je korišćen proksi server, blokiranje saobraćaja ka neželjenim *web* sajtovima se obavljalo na samom proksi serveru institucije, ali bez mogućnosti detaljnog skeniranja sadržaja paketa. Filtriranje saobraćaja iznad L4 sloja *OSI* modela nije bilo moguće usled nedostatka specijalizovane opreme. Kako veći broj institucija koje su povezane na AMRES ima skroman budžet, javila se ideja da se napravi centralizovani *firewall* sistem koji bi omogućio svakoj instituciji da sama definiše pravila filtriranja *web* saobraćaja za svoje korisnike na jednom centralnom uređaju.

2. Arhitektura Ironport sigurnosnog sistema

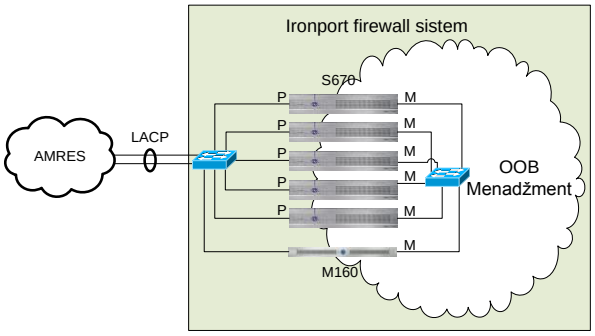
Usled velike količine saobraćaja ka Internetu i svakodnevnog trenda povećanja saobraćaja u AMRES mreži, izvršena je nabavka šest Ironport S670 *firewall* uređaja. Pored Ironport uređaja nabavljena je i oprema koja bi omogućila, ne samo pouzdanost rada sistema, već i praćenje neregularne aktivnosti krajnjih radnih stanica i mogućnost centralizovanog menadžmenta. Dodatni *UPS* uređaji su omogućili nesmetani rad sistema u slučaju nestanka električne energije a dodatna serverska oprema u okviru ovog sistema se koristi za skladištenje i analizu prikupljenih podataka o regularnoj i malicioznoj aktivnosti računara kranjih korisnika AMRES-a.

Na slici 1 je prikazana arhitektura sigurnosnog sistema koji se koristi u okviru AMRES-a . Na slici 1 se vidi da je mrežna infrastruktura sigurnosnog sistema razdvojena na dva dela. Prvi deo mrežnog sistema se odnosi na mrežu kroz koju prolazi produkcioni saobraćaj dok drugi deo obuhvata mrežu koja se koristi za menadžment saobraćaj. Kako Ironport uređaji poseduju više mrežnih interfejsa, jedan interfejs je iskorišćen za produkcioni *web* saobraćaj (P interfejs) a drugi za menadžment saobraćaj (M interfejs). M

interfejsi se koriste za menadžment uređaja, odnosno za:

- Pristup i administraciju Ironport uređaja preko *HTTPS* i *SSH* protokola
- Čuvanje logova o aktivnosti korisnika sa svih Ironport sigurnosnih uređaja
- Pristup i administracija produkcionih Ironport uređaja pomoću centralnog Ironport M160 uređaja
- Nadgledanje uređaja putem *SNMP* protokola

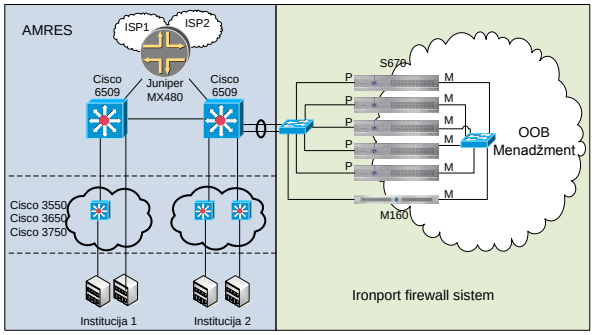
Na ovaj način je izvršeno fizičko razdvajanje produkcionog i menadžment saobraćaja čime se znatno povećava sigurnost rada ovakvog sistema. M i P portovi Ironport uređaja su povezani na ostatak mreže preko svičeva sa gigabitnim interfejsima a ceo sigurnosni sistem je povezan na AMRES mrežu pomoću više gigabitnih linkova. U cilju povećanja kapaciteta veze ka AMRES mreži koristi se *LACP*, kao što je prikazano na slici 1.



Slika 1 – Arhitektura sistema

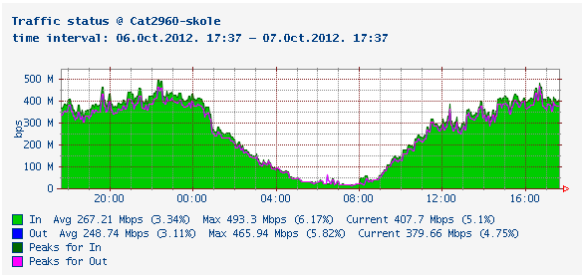
3. Pozicija sistema

Ironport *firewall* sistem za filtriranje *web* saobraćaja je pozicioniran u jezgru mreže. Slika 2 prikazuje poziciju sistema u odnosu na ostale uređaje u mreži.



Slika 2 – Pozicija Ironport *firewall* sistema

Ironport uređaji imaju slučnu funkcionalnost kao proksi serveri, odnosno sav generisani *web* saobraćaj mora prvo da dođe do njih, gde se vrši njegovo filtriranje i skeniranje, a zatim se prosleđuje do krajnje destinacije. Povratni *web* saobraćaj se takođe skenira na osnovu nekoliko parametara pre isporuke ka krajnjim korisnicima. Usled proksiranja saobraćaja dolazi do dupliranja saobraćaja na linkovima, odnosno ulazni i izlazni saobraćaj na portovima Ironport sigurnosnih uređaja je isti. Na slici 3 je dat realan primer dupliranog ulaznog i izlaznog produkcionog saobraćaja ka Ironport sigurnosnom sistemu za period od 24 sata.



Slika 3 – Primer statistike ulaznog/izlaznog *web* saobraćaja na linku Ironport *firewall* sistema

Usled dupliranja saobraćaja potrebno je da se obrati pažnja na linkove koji povezuju Ironport servere sa ostatkom infrastrukture. Poželjno je koristiti agregaciju linkova (npr. *LACP* protokol) da bi se izbeglo zagušenje na linkovima.

Pozicija sistema u okviru *core* dela se preporučuje obzirom da je u toj situaciji Ironport sigurnosni sistem podjednako udaljen od svih krajnjih korisnika, a i usled agregacije saobraćaja ka *core* delu mreže, ova lokacija predstavlja najoptimalnije mesto za postavljanje sigurnosnog sistema.

4. Redirekcija *web* saobraćaja

Da bi se koristio Ironport sigurnosni sistem potrebno je na neki način preusmeriti *web* saobraćaj krajnjih korisnika ka njemu, gde bi se izvršilo filtriranje i skeniranje. To se može uraditi na više načina i u daljem tekstu je dat primer i preporuka kako se to može uraditi.

Mogući su sledeći scenariji redirekcije *web* saobraćaja:

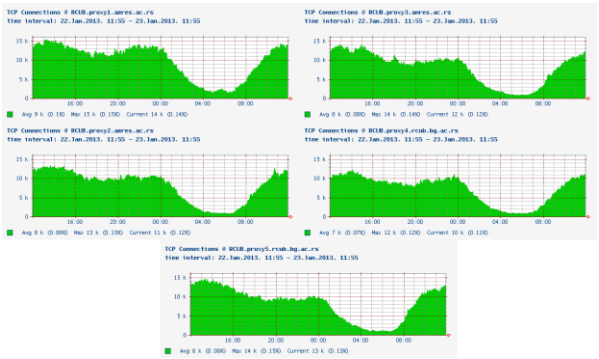
- Preusmeravanje *web* saobraćaja na osnovu proksi konfiguracije u okviru *web* pretraživača
- Preusmeravanje *web* saobraćaja na osnovu *policy-based* rutiranja
- Redirekcija *web* saobraćaja pomoću *WCCP* protokola

U okviru sva tri moguća principa rada akcenat je postavljen na mogućnosti ravnomerne distribucije *web* saobraćaja ka više Ironport sigurnosnih uređaja u cilju njihovog ravnomernog opterećenja.

4.1 Statička konfiguracija proksi servera u okviru *web* pretraživača

Redirekcija saobraćaja se obavlja na osnovu informacije o *IP* adresi ili *DNS* nazivu Ironport uređaja koju korisnik mora sam da unese u okviru proxy podešavanja svog *web* pretraživača. Preporučuje se da se koristi DNS naziv iz više razloga.

- Promena *IP* adrese sigurnosnog sistema je transparentna za korisnika. U slučaju promene *IP* adrese korisnik ne mora ponovo da podešava Internet pretraživač, obzirom da će *DNS* servis uvek vratiti pravu/izmenjenu *IP* adresu sigurnosnog sistema.
- U slučaju da se koristi više Ironport sigurnosnih uređaja preporučuje se da se podesi *DNS* tako da razrešava *DNS* ime Ironport sistema u *round-robin* režimu, odnosno da korisniku omogući da podjednako koristi *IP* adrese svih Ironport uređaja. Na ovaj način se postiže ravnomerna distribucija *web* saobraćaja ka svim Ironport uređajima. Na slici 4 je prikazan primer raspodele *TCP* konekcija produkcionog *web* saobraćaja pomoću *DNS round-robin* metode.



Slika 4 – Raspodela *TCP* konekcija *web* saobraćaja pomoću *DNS round-robin* metode razrešavanja

Na slici 4 se može primetiti da svih pet Ironport uređaja imaju približno sličan broj uspostavljenih *TCP* konekcija. Raspodela bi bila još više simetrična kada bi svi korisnici AMRES-a koristili *DNS* naziv umesto *IP* adresa Ironport sistema.

4.2 Manuelna konfiguracija lokacije PAC fajla

U ovoj situaciji korisnik mora da unese *url* putanju do *PAC (Proxy Auto Configuration)* fajla u okviru proksi podešavanja svog Internet pretraživača. *PAC* fajl se sastoji od skupa java skript komandi koje sadrže definicije o tome na koji način će Internet pretraživač vršiti proksiranje saobraćaja.

AMRES *PAC* fajl je definisan tako da sav lokalni saobraćaj u okviru AMRES mreže Internet pretraživač ne šalje na skeniranje i filtriranje. Sav ostali saobraćaj ka Internetu mora da se šalje ka Ironport *firewall* sistemu. I u ovom slučaju se koristi *DNS* naziv Ironport sistema u cilju što ravnomernije distribucije *web* saobraćaja.

4.3 Dinamička autokonfiguracije

Dinamička autokonfiguracija pomoću *WPAD (*Web *Proxy Auto-Discovery*) protokola se pokreće u okviru *web* pretraživača tako što se selektuje polje za autodetekciju proksi servera. *WPAD* protokol funkcioniše tako što proverava u kom domenu se nalazi korisnički računar a zatim pokušava da pronađe *wpad.dat* fajl u tom domenu. U slučaju da pretraživač ne pronađe *wpad.dat* fajl u tom domenu (npr. http://test.example.com/wpad.dat) pretraga se nastavlja u domenu roditelja (npr. http://example.com/wpad.dat) Sintaksa *wpad.dat* fajla je ista kao i za *PAC* fajl, odnosno u pitanju je java skript.
I u ovom slučaju preporuka je da se koristiti *DNS round-robin* režim rada da bi se omogućila ravnomerna distribucija *web* saobraćaja ka Ironport sigrnosnim uređajima.

4.4 Redirekcija na osnovu policy-based rutiranja

Redirekcija se može obaviti i pomoću *policy-based* rutiranja odnosno na samim ruterskim platformama u jezgru mreže. Potrebno je izdvojiti željeni *web* saobraćaj i zatim preusmeriti na Ironport sigurnosne uređaje. Problem sa ovakvim pristupom je što se ne mogu optimalno iskoristiti svi Ironport uređaji obzirom da je nemoguće ostvariti ravnomernu raspodelu saobraćaja pomoću *policy-based* rutiranja. Ovakvo rešenje ne zahteva konfiguraciju na strani korisnika ali zahteva da se Ironport uređaji pokrenu u transparentnom režimu rada. Na slici 5 je dat primer konfiguracije na Cisco 6500 uređaju. Sav *TCP* saobraćaj koji se generiše iz mreže 10.20.30.0/24 ka bilo kojoj *IP* adresi sa odredišnim portom 80 ili 443 će biti preusmeren ka 172.16.0.1 Ironport uređaju. Ovaj princip ima smisla koristiti kada postoji samo jedan Ironport uređaj ka kome treba proslediti sav *web* saobraćaj.

```
ip access-list extended WEB
permit tcp 10.20.30.0 0.0.0.255 any eq 80
permit tcp 10.20.30.0 0.0.0.255 any eq 443
!
route-map RED2IRONP permit 10
match ip address WEB
set ip next-hop 172.16.0.1
!
interface GigabitEthernet0/0
ip policy route-map RED2IRONP
```

Slika 5 – Primer konfiguracije *policy-based* rutiranja na Cisco 6500 uređaju

4.5 Redirekcija pomoću *WCCP* protokola

WCCP (Web Cache Communication Protocol) je protokol koji je razvijen od strane Cisco kompanije i danas je podržan i kod drugih proizvođača mrežne i serverske opreme. Trenutno postoje dve verzije protokola, V1 i V2. Preporučuje se korišćenje verzije 2 zato što donosi nove funkcionalnosti kao što su, podrška i za druge servise osim *HTTP*, grupisanje *WCCP* rutera u klastere, *MD5* autentifikaciju i ravnomernu distribuciju saobraćaja. Za razliku od *policy-based* rutiranja *WCCP* protokol ima mogućnost ravnomerne distribucije saobraćaja i zbog toga se preporučuje da se koristi u situacijama gde postoji više Ironport uređaja i gde je neophodno ravnomerno rasporediti saobraćaj ka svakom od njih. *WCCP* se može konfigurisati na dva načina u zavisnosti od topologije mreže i veze između mrežnih uređaja. Preporučuje se da se Ironport uređaji povežu sa ruterima u jezgru mreže direktno na L2 nivou i u tom slučaju je moguće vršiti direktno prosleđivanje *web* saobraćaja. U suprotnom, ako su Ironport uređaji u nekom posebnom odvojenom L3 segmentu *WCCP* će koristiti *GRE* protokol da bi izvršio tunelovanje preusmerenog saobraćaja.

Prilikom konfiguracije *WCCP* protokola potrebno je obratiti pažnju na tip uređaja na kom se *WCCP* protokol pokreće. U zavisnosti od fizičke topologije mreže i konfiguracije *WCCP* protokola može doći do velikog opterećenja resursa *core* uređaja.

U slučaju kada se koristi *WCCP* protokol sav *web* saobraćaj će biti redirektovan ka Ironport uređajima i krajnji korisnici neće morati da izvrše podešavanje u svojim *web* pretraživačima. U slučaju da se koristi više Ironport uređaja *WCCP* proces na *core* uređaju će koristiti *load-balancing* metodu u cilju što ravnomernije raspodele *web* saobraćaja koji se preusmerava ka Ironport uređajima. Iako je *WCCP* protokol razvijen od strane Cisco kompanije, može se pronaći i kod drugih komercijalnih vendora kao što je BlueCoat a i kod *opensource* rešenja kao što je Squid proksi platforma.

5. Centalizovani menadžment

Centralizovani menadžment sistema omogućuje da se izmena konfiguracije vrši na jednom centralnom specijalizovanom Ironport uređaju, pomoću *web* pretraživača, a zatim da se konfiguracija primeni na svim ostalim Ironport uređajima. Na ovaj način se izbegava ponavljanje istog posla na više uređaja i samim tim se smanjuje mogućnost greške u konfiguraciji. Ironport M160 uređaj takođe poseduje mogućnost prikupljanja i obrade log informacija, međutim ovakvo rešenje zahteva kupovinu dodatne licence. U slučaju rešenja koje je primenjeno u okviru AMRES mreže prikupljanje log informacija je rešeno na drugi način. Sve log informacije sa Ironport uređaja se šalju na centralni Linux server gde se obrađuju pomoću posebnih skripti. Nakon toga se fajlovi šalju na obradu do Sawmill aplikacije i potom čuvaju na posebnom storidž sistemu.

Na slici 1 je prikazan princip *OOB (Out-of-Band)* menadžmenta gde se koristi zasebna fizička infrastruktura za menadžment Ironport uređaja. U okviru *OOB* opsega se koristi privatni adresni opseg koje se ne oglašavaju kroz ostatak mreže i na taj način se uvodi dodatni nivo sigurnosti u ceo sistem. Menadžment uređaj poseduje dva porta, jedan port sa javnom *IP* adresom pomoću koga se prilazi opcijama za konfigurisanje i drugi *OOB* port koji je izolovan u okviru *OOB* dela mreže. Mogućnost centralizovanog menadžmenta i opcija da se centralizovani uređaj poveže sa *LDAP* bazom podataka je omogućilo da administratori AMRES mreže razviju *firewall cloud* servis za administratore AMRES članica.

6. Ironport *cloud* servis

U cilju autentifikacije pojedinih korisnika Ironport *cloud* servisa menadžment uređaj za konfigurisanje je podešen tako da komunicira sa *LDAP* serverom u kome se nalazi grupa administratora koja ima prava da vrši izmene na Ironport sigurnosnom sistemu. Svakom od administratora je dodeljeno pravo menadžmenta polise koja definiše opcije za skeniranje i filtriranje *web* saobraćaja koji potiče iz matične institucije tog administratora. Da bi to bilo moguće polisa se vezuje za *IP* adresni opseg institucije administratora. U slučaju da administrator ne želi da administrira svoju polisu sav njegov saobraćaj će biti obuhvaćen krajnjom polisom koja je primenjena za sve AMRES članice.

Obavezna pravila filtriranja i skeniranja za sve AMRES članice su definisana na sledeći način:

- *URL* filtriranje

Ovom opcijom se definiše skup kategorija kojima je dozvoljen *web* pristup. Cisco kompanija periodično dopunjuje baze podataka na Ironport uređajima u kojima se vrši kategorizacija *web* sajtova i povremeno dodaje nove kategorije. U trenutku pisanja dokumenta bilo je dostupno 78 različitih kategorija sajtova. U okviru Ironport *URL* sistema za filtriranje postoji mogućnost da pojedini sajtovi budu pogrešno svrstani u neku kategoriju, stoga je napravljena posebna *URL* kategorija koja eksplicitno pušta pristup sajtovima koji su u okviru nje definisani. Na taj način se rešava problem pogrešno kategorizovanih sajtova sve dok se na naprave globalne izmene u Cisco bazi kategorija.

Sav saobraćaj koji prolazi kroz Ironport uređaje mora da bude obrađen u okviru neke od definisanih polisa. Poslednja u nizu polisa je *default* polisa koja će obraditi sav saobraćaj koji nije obuhvaćen prethodnim polisama. Poslednja, *dfault* polisa, blokira sledeće *web* kategorije za sve korisnike AMRES-a:

- *Child Abuse Content*
- *Filter Avoidance*
- *Gambling*
- *Hate Speech*
- *Illegal Drugs*
- *Pornography*

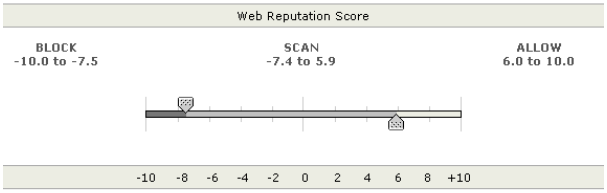
Dodatne kategorije se mogu posebno uključiti za pojedine polise AMRES institucija na zahtev administratora, ili ih sami administratori mogu uključiti ako već imaju kontrolu nad svojom polisom.

- *WBRS-web* reputacija

WBRS (Web Reputation Score) opcijom se definiše način na koji će se vršiti skeniranje *malware* [1] malicioznog softvera pomoću *Webroot* skenera. Postoje tri dostupne opcije u zavisnosti od reputacije *web* stranice:

- Blokiranje
- Skeniranje
- Dozvoljen pristup

Na slici 6 je prikazano *WBRS* podešavanje za globalnu AMRES polisu. Na slici 6 se vidi da će svim *web* stranicama, koje imaju *WBRS* manji od -7.5, biti zabranjen pristup. *Web* stranicama koje imaju *WBRS* između -7.5 i +6 će biti dozvoljen pristup ali uz dodatno skeniranje pomoću *Webroot* skenera. *Web* stranicama koje imaju *WBRS* veći od +6 će biti dozvoljen pristup bez skeniranja.



Slika 6 – Filtriranje i skeniranje na osnovu *web* reputacije

WBRS vrednost se određuje na osnovu velikog broja parametara koje Cisco kompanija čuva u svojoj bazi podataka za veliki broj sajtova.

7. Zaključak

Iako je Ironport sigurnosni sistem dizajniran tako da zadovolji veći broj potreba zatvorenih organizacija kao što su banke i preduzeća čiji profil posla zahteva visok nivo sigurnosti, pojedine komponente sistema se mogu veoma dobro iskoristiti i u drugim organizacijama gde nivo sigurnosti organizacije ne mora da bude na veoma visokom nivou, već je akcenat na zaštiti pojedinačnih krajnjih korisnika. Osnovne škole, srednje škole, fakulteti i biblioteke predstavljaju primer ovakvih organizacija. Trenutni trendovi razvoja tehnologije pored inovativnosti donose i pojedine loše aspekte kao što su krađa indentiteta, širenje destruktivnih virusa i zloupotrebe anonimnosti koje Internet pruža. Veliki broj parametara ukazuju na to da je potrebno više obratiti pažnju na sigurnost korisnika Interneta, a naručito mlađe populacije. Ovakav sigurnosni sistem ima veliku primenu u zaštiti krajnjih korisnika akademskih institucija i očekuje se njegova sve veća upotreba u skorijoj budućnosti.

Reference:

[1] H. Bos, E. Jonsson, E. Djambazova, K. Dimitrov, S. Ioannidis, E. Kirda, C. Kruegel, "Anticipating Security Threats to a Future Internet"; White Paper, March 2009

[2] http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/white_paper_c11-629052.html

[3] http://www.senderbase.org/